Revealing Europe’s NSO

lighthousereports.nl/investigation/revealing-europes-nso

CREDITS

Crofton Black, Riccardo Coluccini, Gabriel Geiger, Tomas Statius, Max Hoppenstedt, Nikolaj Nielsen, Aiia Timofeeva, Maud Jullien

REPORTED WITH

- DER SPIEGEL
- IRPI
- Domani
- MEDIAPART
- euobserver

TAGS

SURVEILLANCE

FROM THIS INVESTIGATION

Domani

La sorveglianza europea parte da un’azienda italiana

Mentre l’Unione europea fa i conti con lo spyware israeliano Pegasus, intanto anche in Europa c’è chi sfrutta una vulnerabilità[..]

More MEDIAPART

Une société italienne rattrapée par son logiciel espion

Alors que des auditions se déroulent au Parlement européen sur le groupe israélien NSO, une société d’espionnage italienne, Tykelab, propose,[..]

More euobserver

Investigation: NSO surveillance rival operating in EU

The European Union has begun to wake up to the threat posed by an out-of-control surveillance industry, with Israel's notorious[..]

More DER SPIEGEL

»Das ist die einfachste Möglichkeit, jemanden gezielt zu überwachen«

Die EU untersucht die Rolle des israelischen Spionageanbieters NSO. Doch auch in Europa entwickeln Firmen offensive Cyberwaffen: Dokumente zeigen, wie[..]

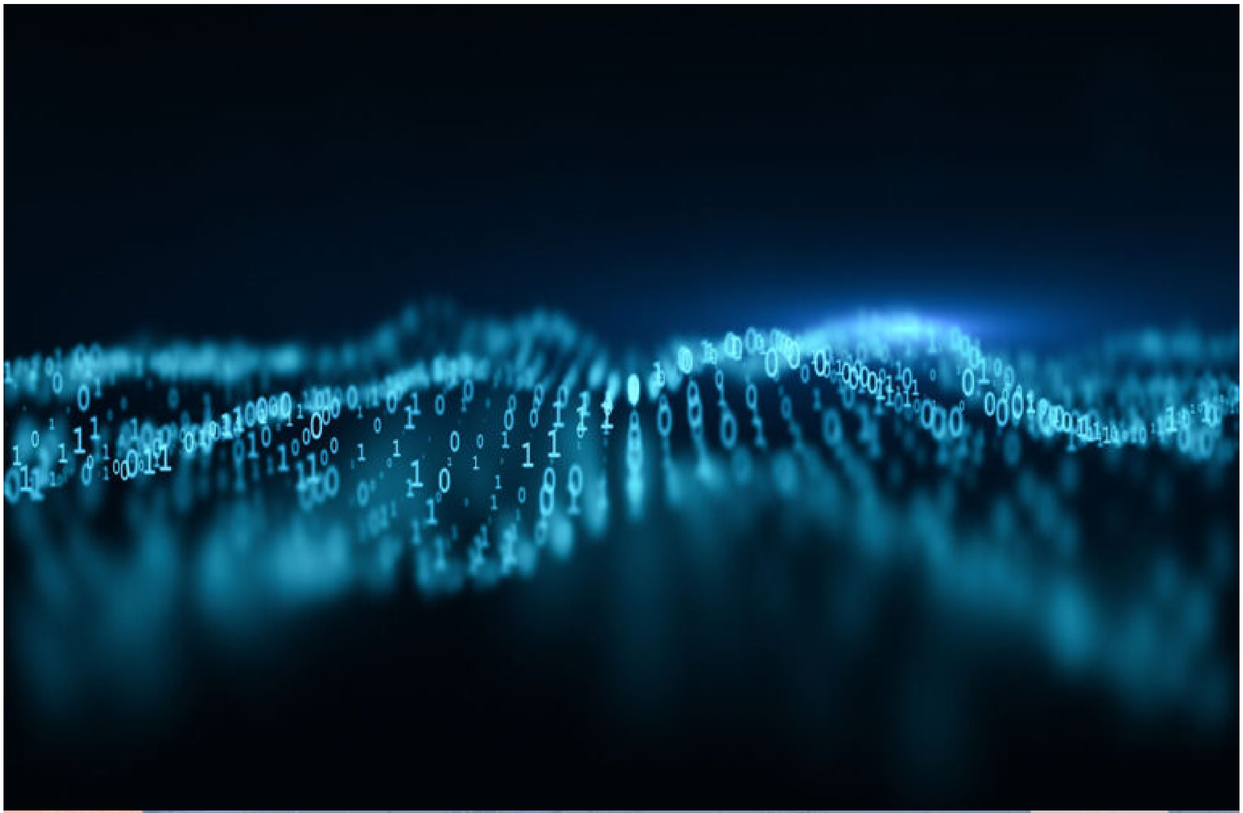
More IRPI

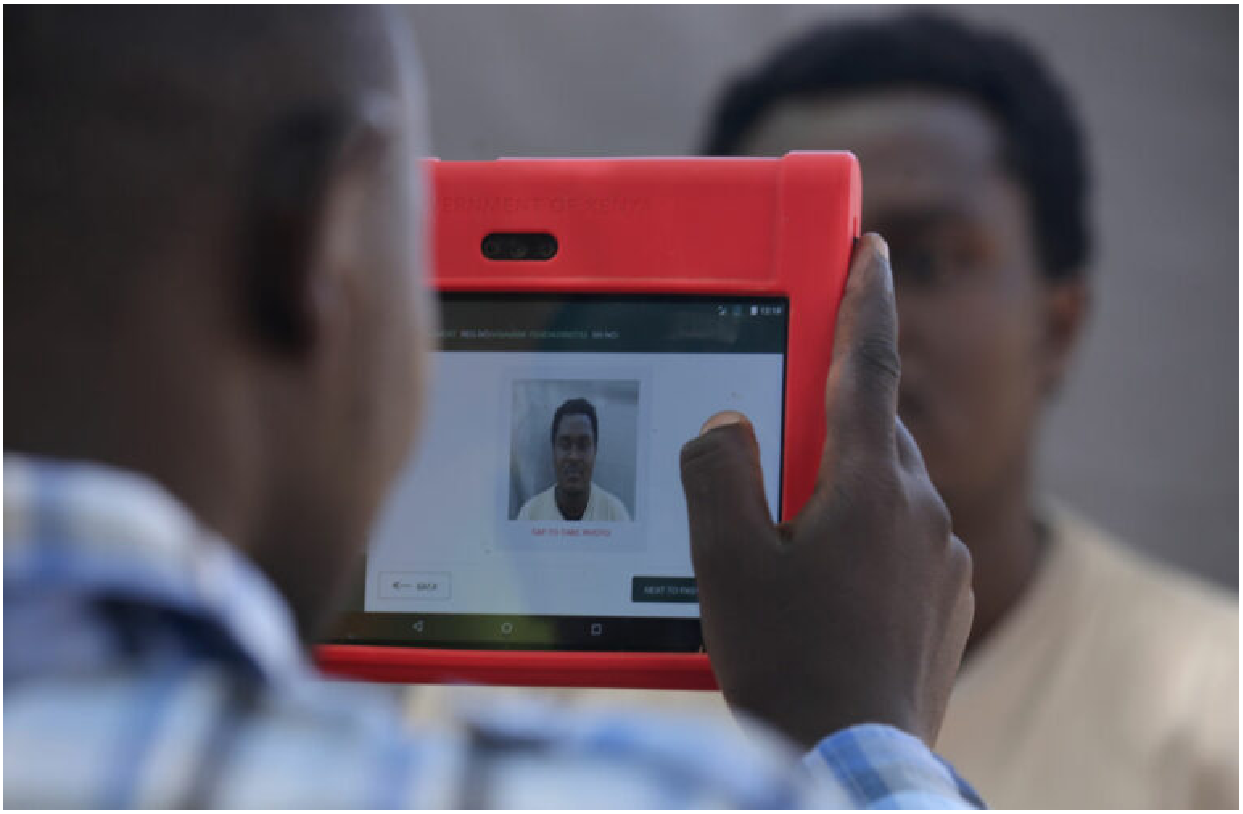
L’azienda italiana che può localizzare una persona in ogni angolo del mondo

Tykelab offre i suoi servizi tramite la ben più nota azienda di intercettazioni RCS. Iinsieme sono state acquisite dal colosso[..]

More

SIMILAR INVESTIGATIONS

- 
-

- 

  ## Biometrics and the Enslavement of African Elections

  Technology has been pushed as a panacea for African democracies. As Kenya faces its third biometric election, a French multinational has made tens of millions from failed systems

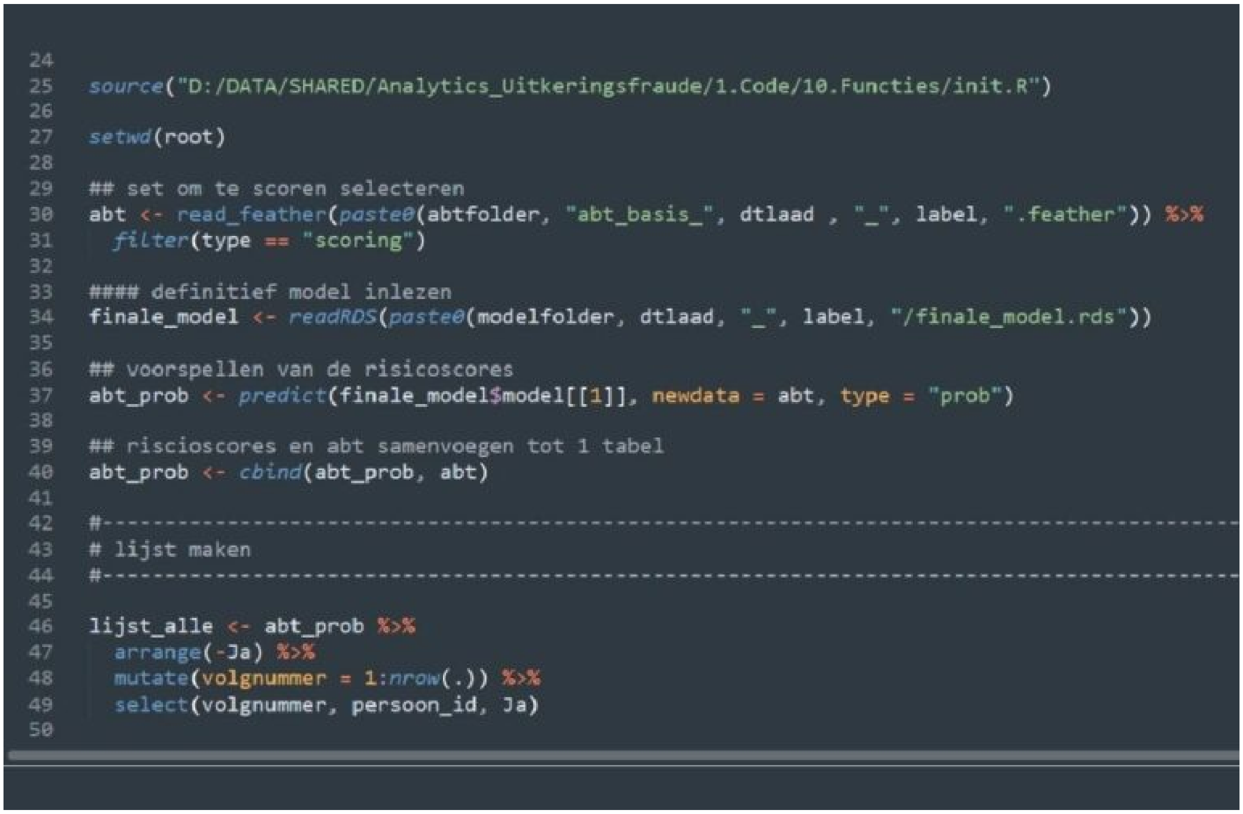
  More

-

Is Europol becoming a European NSA?

The most in-depth investigation to date of the EU police agency uncovers years of unlawful retention of personal data

More

- 

```r

source("D:/DATA/SHARED/Analytics_Uitkeringsfraude/1.Code/10.Functies/init.R")

setwd(root)

## set om te scoren selecteren
abt <- read_feather(paste0(abtfolder, "abt_basis_", dtlaad , "_", label, ".feather")) %>%
  filter(type == "scoring")

#### definitief model inlezen
finale_model <- readRDS(paste0(modelfolder, dtlaad, "_", label, "/finale_model.rds"))

## voorspellen van de risicoscores
abt_prob <- predict(finale_model$model[[1]], newdata = abt, type = "prob")

## riscioscores en abt samenvoegen tot 1 tabel
abt_prob <- cbind(abt_prob, abt)

#---------------------------------------------------------------------------------------------
# lijst maken
#---------------------------------------------------------------------------------------------

lijst_alle <- abt_prob %>%
  arrange(-Ja) %>%
  mutate(volgnummer = 1:nrow(.)) %>%
  select(volgnummer, persoon_id, Ja)

```

-

  EU Spy Tech Serves Myanmar Junta

  While the military coup and deadly crackdown in Myanmar has drawn European condemnation, EU funds and technology have secretly aided the junta in spying on its own population

  More

-

What is Palantir Doing in Europe?

The controversial US tech company is putting down roots in the EU's security, public health and aviation sectors as well as its data infrastructure, raising questions

More

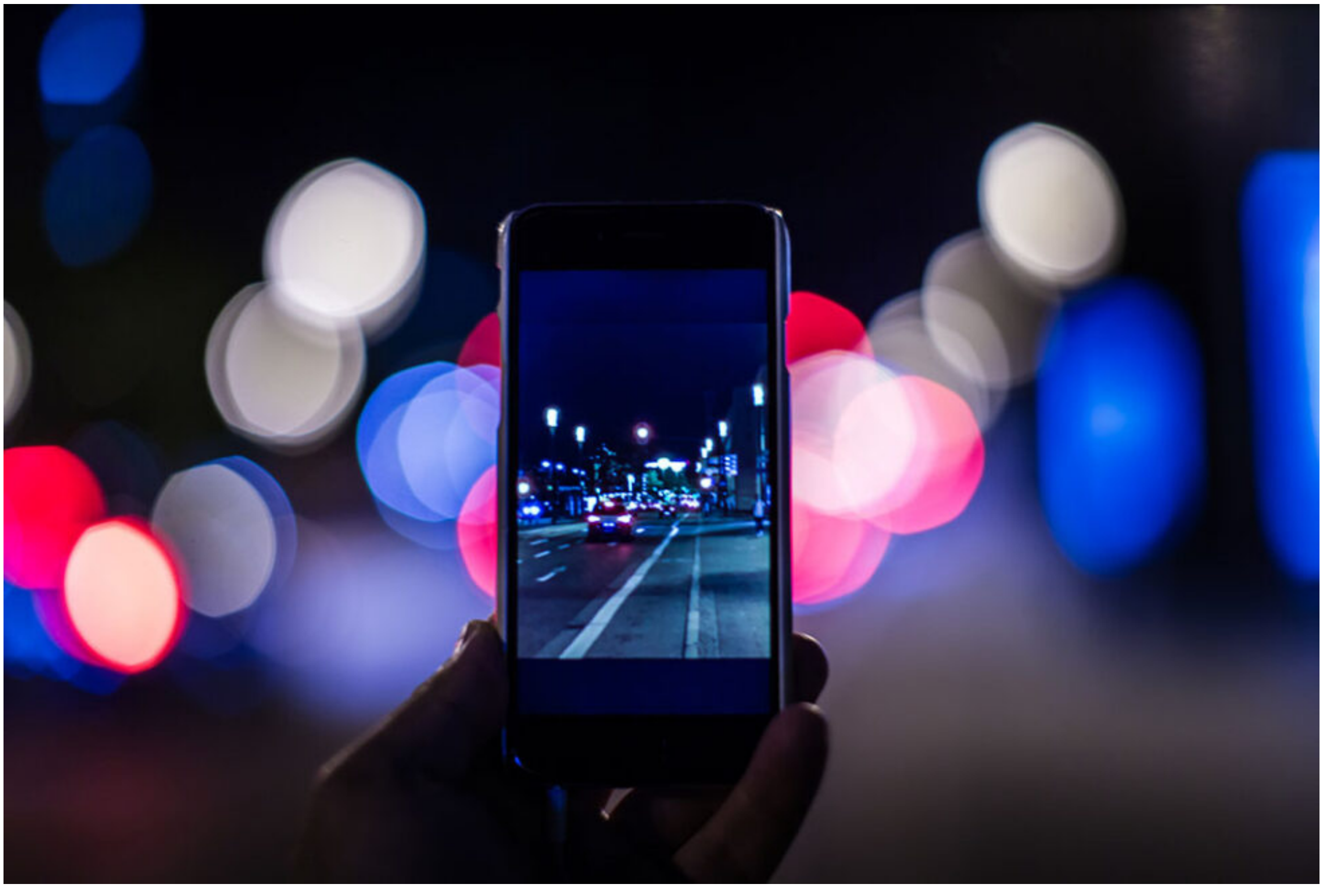
- previous
- next

CONTACT

- info@lighthousereports.nl
- +31 6 40229299

August 28, 2022

Confidential data and sources uncover major surveillance outfit operating from within the European Union



An Italian surveillance company is tracking people all over the world on a grand scale on behalf of its clients – including in countries with a recent history of corruption and human rights abuses. Its powerful spyware was recently found in Kazakhstan and Romania. Europe's parliamentarians voice growing concern about an out-of-control surveillance industry and call for it to be regulated.

Confidential data seen by Lighthouse Reports shows that a little-known company based in Rome, Tykelab, has been using dozens of phone networks, often on remote Pacific islands, to send tens of thousands of secret "tracking packets" around the world, targeting people in countries including Libya, Nicaragua, Malaysia, Costa Rica, Iraq, Mali, Greece and Portugal – as well as in Italy itself.

It's doing this by exploiting longstanding but frequently unfixed vulnerabilities in global phone networks which make it possible for third parties to see phone users' locations, and potentially intercept their calls, without any record of compromise being left on their devices.

At the same time, Tykelab's parent company, RCS Lab, has developed a powerful phone hacking tool, Hermit, which once installed on a victim's device can be used to remotely activate the phone's microphone, as well as record calls, access messages, call logs, contacts, photos and other sensitive data.

Behind the scenes, security professionals have raised the alarm about Tykelab's activities. Analysts with access to confidential telecom data described how the company was "persistently and systematically" attempting to bypass network protections as well as carrying out "blatant and targeted tracking of individuals".

"They are becoming more and more active," one told us. "Since the start of this year, they've been increasing the number of attacks, and now it's constant."

As the European Union wakes up to the threat posed by an out-of-control surveillance industry, with Israel's notorious NSO Group and its Pegasus software in its crosshairs, we reveal the scope and scale of a previously unknown surveillance vendor in the heart of the EU.

METHODS

Our findings originated with two confidential sources in the telecom industry. They had both independently been tracking significant volumes of suspicious traffic sent through a group of phone networks – much of it ostensibly from islands in the South Pacific. Through technical and other data they determined, independently from each other, that this traffic originated in Italy with a company called Tykelab. The company's website says it's an innocuous telecom services provider. Our sources said that its traffic had no legitimate purpose other than surveillance.

We sent samples of the data our sources provided to two independent security experts: Karsten Nohl, from Security Research Labs in Germany, and Jean Gottschalk, from Telecom Defense Ltd in the USA. Both agreed with our sources' analysis. "Someone is spying on a large scale via the phone network," said Nohl.

Through corporate disclosures and financial data, we established that Tykelab is a part of RCS Lab, an Italian company with a long history of interception activities both in Italy and abroad. This fact was undisclosed until a takeover by a third company, Cy4Gate, made it known to shareholders last December. We also established that RCS Lab has another concealed subsidiary, Azienda Informatica Italiana, which builds interception software for Android and iPhone devices.

Tykelab’s office in a suburb of Rome with the company logo clearly visible inside

We obtained unpublished brochures of RCS Lab’s products and services from an invite-only trade fair. These included details of Ubiqo, a tool which can “track the movements of almost anybody who carries a mobile phone, whether they are blocks away or on another continent”, as well as offering more sophisticated behaviour analysis. We used IoT search engines Censys and Shodan to scan RCS Lab’s Italian infrastructure and found a login for a webpage with the slogan “powered by Tykelab”.

During our investigation, cybersecurity specialists at Lookout and Google published details of a previously unknown but sophisticated hacking package called Hermit. They both independently attributed this package to RCS Lab and provided lists of fake internet domains which the company had set up to lure targets to download the software. They included domains masquerading as Apple and Facebook, as well various telecom providers. We analysed this list using the domain database WhoisXML API and found that RCS Lab purchased some of these fake domains as early as 2015, while others were bought in March this year – indicating years of potential hacking operations by the company.

We interviewed Lookout’s Justin Albrecht and Paul Shunk, who confirmed further details of the Hermit spyware, including that they had recently observed it in action in another country, Romania.

STORYLINES

Since 2021 a wave of hacking scandals has engulfed EU countries, with tools supposedly meant for the most serious criminals being turned against politicians and journalists. The European Parliament is holding hearings, focusing particularly on Israel's NSO Group and its flagship Pegasus spyware. But our investigation has thrown the spotlight on the EU itself and Europe's role in the high-risk proliferation of commercial surveillance technology.

Our findings show Tykelab's surveillance traffic reaching all over the world – the Italian company's systems have been targeting people in Libya, Costa Rica, Nicaragua, Pakistan, Malaysia, Iraq and Mali, to give only a few specific examples, as well as in Greece, Macedonia, Portugal and Italy.

MEPs, security specialists and privacy experts, looking at our findings, expressed deep concern at the risks associated with the untransparent trade in powerful spy tech and questioned whether EU member states were doing enough to regulate it.

As Markéta Gregorová, the European Parliament's rapporteur for surveillance technology export controls, told us: "Commercial cyber-surveillance secretly sold to anyone willing to pay is a global security risk for all of us inside and outside the European Union. This service gets human right activists and journalists tortured and killed."

While highlighting problems in Europe's export policies, the investigation also exposes the little-known practice in the telecom industry which enables these types of abuses to flourish – the leasing of phone network access points or "global titles". We spoke to the mobile phone trade association, GSMA, who confirmed to us that "organisations improperly using leased global titles must be stopped". But the association pointed out that phone operators cannot always identify the source and purpose of the traffic that flows through their networks, making it difficult to curtail the surveillance industry.

Security expert Karsten Nohl emphasised that it is now eight years since critical vulnerabilities in how mobile phone networks function were disclosed – the same vulnerabilities which Tykelab and others have weaponised for surveillance purposes. Nohl said: "Firewalls have long been in place so that phone operators can protect their customers — but this research proves that not all worldwide phone providers have set up these basic protections. It is very unfortunate that these vulnerabilities have still not been closed."

To keep up to date with Lighthouse investigations sign up for our monthly newsletter