

THE PREDATOR FILES

**HOW EUROPEAN SPYWARE THREATENS CIVIL
SOCIETY AROUND THE WORLD**

PHOTO: HANNES WIEDEMANN



SECURITY LAB AT AMNESTY INTERNATIONAL

- ▶ A multi-disciplinary team focused on investigating and exposing unlawful surveillance and other digital threats targeting human rights defenders.
 - ▶ Research and investigations
 - ▶ Open source forensic tools
 - ▶ Campaigns and advocacy





DER SPIEGEL

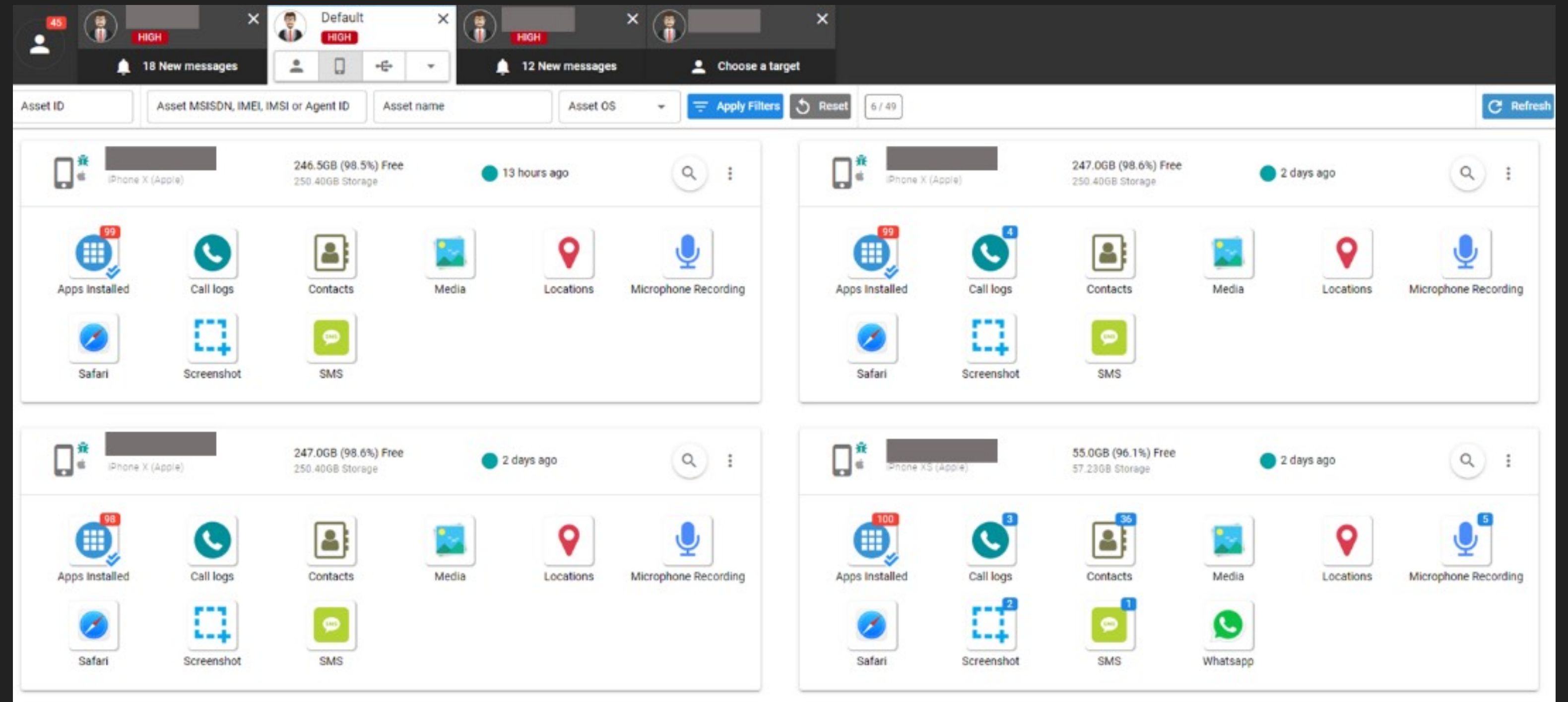


**PREDATOR
FILES**

PREDATOR FILES

INTELLEXA'S PREDATOR SPYWARE

- ▶ A form of highly-invasive spyware that can infect iPhones and Android devices.
- ▶ Uses zero-day exploits to infect even fully patched devices.
- ▶ These exploits can cost millions of euros.



Operator interface for the Predator spyware (source: EIC documents)

INTELLEXA'S PREDATOR SPYWARE

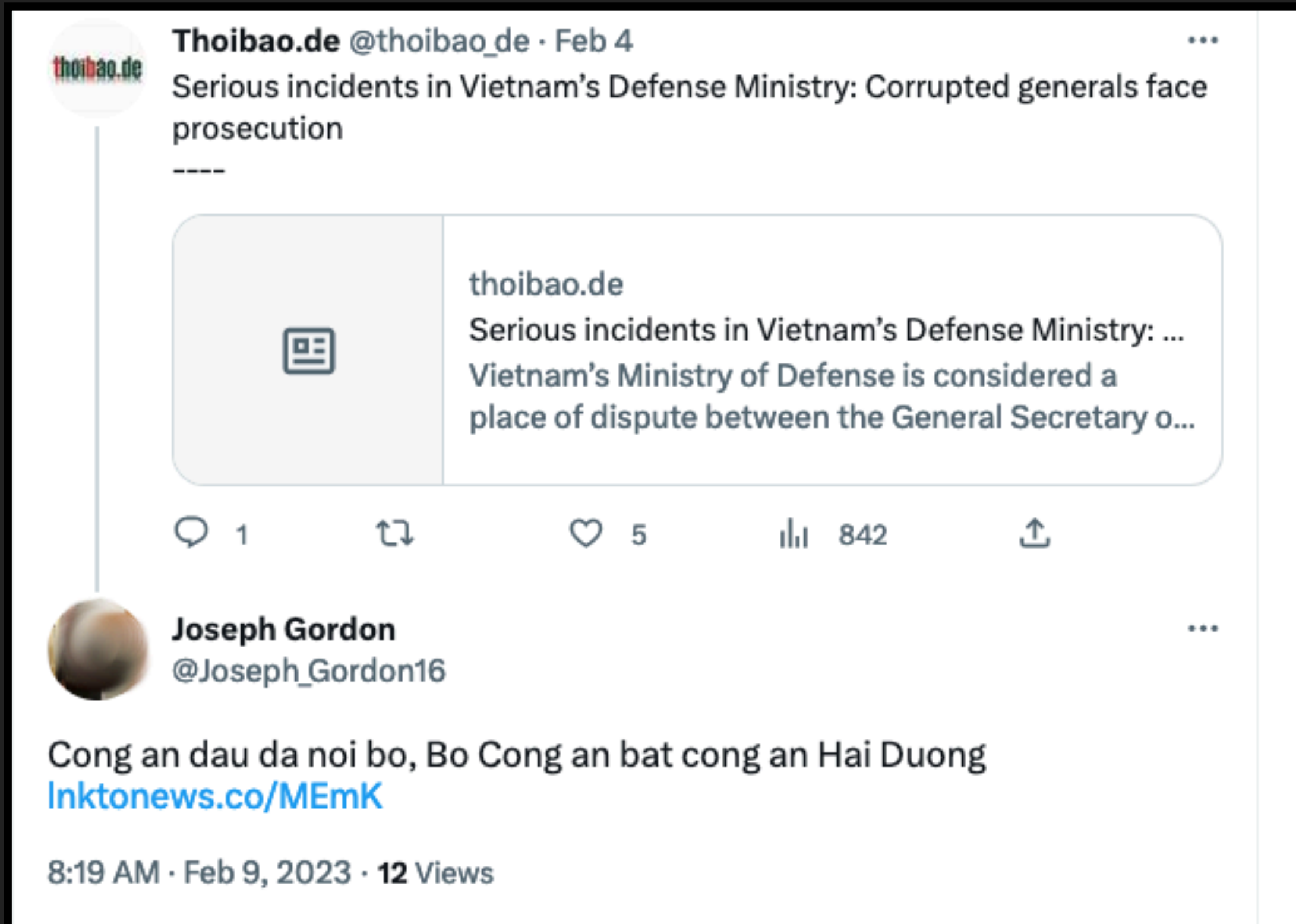
- ▶ Predator is typically delivered as 1-click spyware.
- ▶ The target needs to click on a malicious Predator link to be infected.



Predator first identified in-the-wild targeting an Egyptian journalist in 2021
(Source: Citizen Lab)

THE INVESTIGATION

A TWITTER USER SPREADING SPYWARE INFECTION LINKS



Thoibao.de @thoibao_de · Feb 4
Serious incidents in Vietnam's Defense Ministry: Corrupted generals face prosecution

[Screenshot of a tweet from thoibao.de]
1 1 5 842

Joseph Gordon @Joseph_Gordon16
Cong an dau da noi bo, Bo Cong an bat cong an Hai Duong
Inktonews.co/MEmK
8:19 AM · Feb 9, 2023 · 12 Views



Taiwan-made landing platform dock to enter service in June: Source ...
Taipei, May 15 (CNA) The Taiwan-made Yushan landing platform dock (LPD), a type of naval warship used to transport landing crafts such ...
10 43 157 19.6K

Joseph Gordon @Joseph_Gordon16 · 1h
Replying to @CollinSLKoh
Summit a 'major diplomatic event' to boost China's ties with Central Asian nations amid Ukraine, Afghanistan concerns
southchinapost.net/WzMqB
6



1 47 125 21.5K

Joseph Gordon @Joseph_Gordon16 · Apr 14
Replying to @AsiaMTI and @cnnphilippines
PLA forces tail US warship near disputed Spratly Islands as live-fire drills around Taiwan enter day 3 caavn.org/news/china/mil...

Links sent to Twitter account @Thoibao_de, run by journalist Trung Khoa Lê

PHISHING OR FISHING?



WEBINAR *Asociatividad para el desarrollo y la innovación de la pesca y acuicultura artesanales en América del Sur*

Miércoles 31 de agosto 11:00 horas (Santiago, Chile) [FAO.org/americas](https://www.fao.org/americas)

Joseph Gordon @Joseph_Gordon16 · May 16
Replying to @HugBallesteros and @FAOAmericas
¿Cuál es su solución para deshacerse de la tarjeta amarilla? asean-news.net/HpjXXwRU

Alexandre Marcos @AlexMarcos71 · May 16 View
Replying to @HugBallesteros @UniversidadeUSC and @economia_pesca
Los esfuerzos para eliminar la "tarjeta amarilla" de los productos del mar todavía enfrentan muchas dificultades



Mission Ocean Waters @eumissionocean · 21h
“We have decided to transform how we live on Aran Islands with a population of 1500 on three islands.”
“Individually Inis Mór (large island) has a population of 1000 people, Inis Meáin (middle island) has 200 inhabitants and Inis Oírr (easterly Island) although the smallest... [Show more](#)”



Joseph Gordon @Joseph_Gordon16 · 8h
Replying to @eumissionocean
As more nations oppose China, how seriously does the world take Beijing? southchinapost.net/VuAfn

Attack links referencing the EU Yellow Card system ("Tarjeta amarilla")

SENIOR POLITICIANS AND OFFICIALS TARGETED

Emily Haber @GermanAmbUSA · Mar 7
Noted. No response to the arguments.

J.D. Vance @JDVance1 · Mar 6
“We’ve committed.” “We will spend.” If your policy hadn’t been to depend on Russia for energy and shirk your NATO dues for two decades you wouldn’t be shopping for tanks at Aldi.
twitter.com/GermanAmbUSA/s...

Joseph Gordon @Joseph_Gordon16 · Mar 8
Replying to @GermanAmbUSA
Get rid of the EU and NATO liars inktonews.co/CVqp

Joseph Gordon @Joseph_Gordon16 · 3h
Replying to @EU_Commission
As more nations oppose China, how seriously does the world take Beijing? southchinapost.net/VuAfn

Roberta Metsola @EP_President · 19h
La risposta alla tragica alluvione in Emilia-Romagna ha fatto emergere il meglio delle persone.
A coloro che hanno perso una persona cara, giunga il nostro pensiero più forte.
A chi ha perso la propria casa, siamo con voi e vi aiuteremo a ricostruire



Joseph Gordon @Joseph_Gordon16 · 8h
Replying to @EP_President
As more nations oppose China, how seriously does the world take Beijing? southchinapost.net/VuAfn

THE INVESTIGATION



外交部 Ministry of Foreign Affairs, ROC (Taiwan) @MOFA_Taiwan Apr 14

Welcome to the club, @RepMcCaul! #Beijing's sanction is proof of your achievement in safeguarding freedom, democracy, & status quo across the #Taiwan Strait. JW

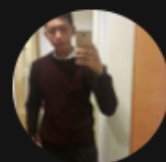


House Foreign Affairs Committee Majority @HouseForeignGOP Apr 13

CHM @RepMcCaul: "Being sanctioned by the Chinese Communist Party is a badge of honor." [reuters.com/world/china-sanc...](https://www.reuters.com/world/china-sanc...)

Show this thread

28 118 11 837



Joseph Gordon @Joseph_Gordon16 Apr 14

[caavn.org/news/china/article...](https://www.caavn.org/news/china/article...)



蔡英文 Tsai Ing-wen @iingwen · May 21

#Taiwan has become a key word across the world. The Taiwan Strait has transcended from a cross-strait, regional issue to become the focal point of global security and international prosperity. The whole world is at stake. As such, we must manage cross-strait issues from a global... [Show more](#)

Peace is the only option across the Taiwan Strait. Maintenance of the status quo is the largest common denominator among all parties and the decisive key to preserving peace.

The global consensus is clear: the Taiwan Strait issue must be resolved peacefully, and war is not an option. Neither side can change the status quo through non-peaceful means.

Since I took office, our position has remained firm, pledging to maintain the status quo, and upholding the "four commitments," in order to safeguard the shared interests and well-being of the 23 million people of Taiwan. We do not provoke, we do not act rashly, and we will absolutely not bow to pressure.

We have endeavored to maintain the status quo, prevent conflict, resolve cross-strait differences through dialogue on equal footing, and promote healthy and orderly exchanges. These are our shared responsibilities across all political parties and across the Taiwan Strait. These are also the common expectations of regional countries and democracies across the globe.

Ing-wen Tsai
May 20, 2023

@iingwen

396 783 3,961 398.9K



Joseph Gordon @Joseph_Gordon16 · 10h

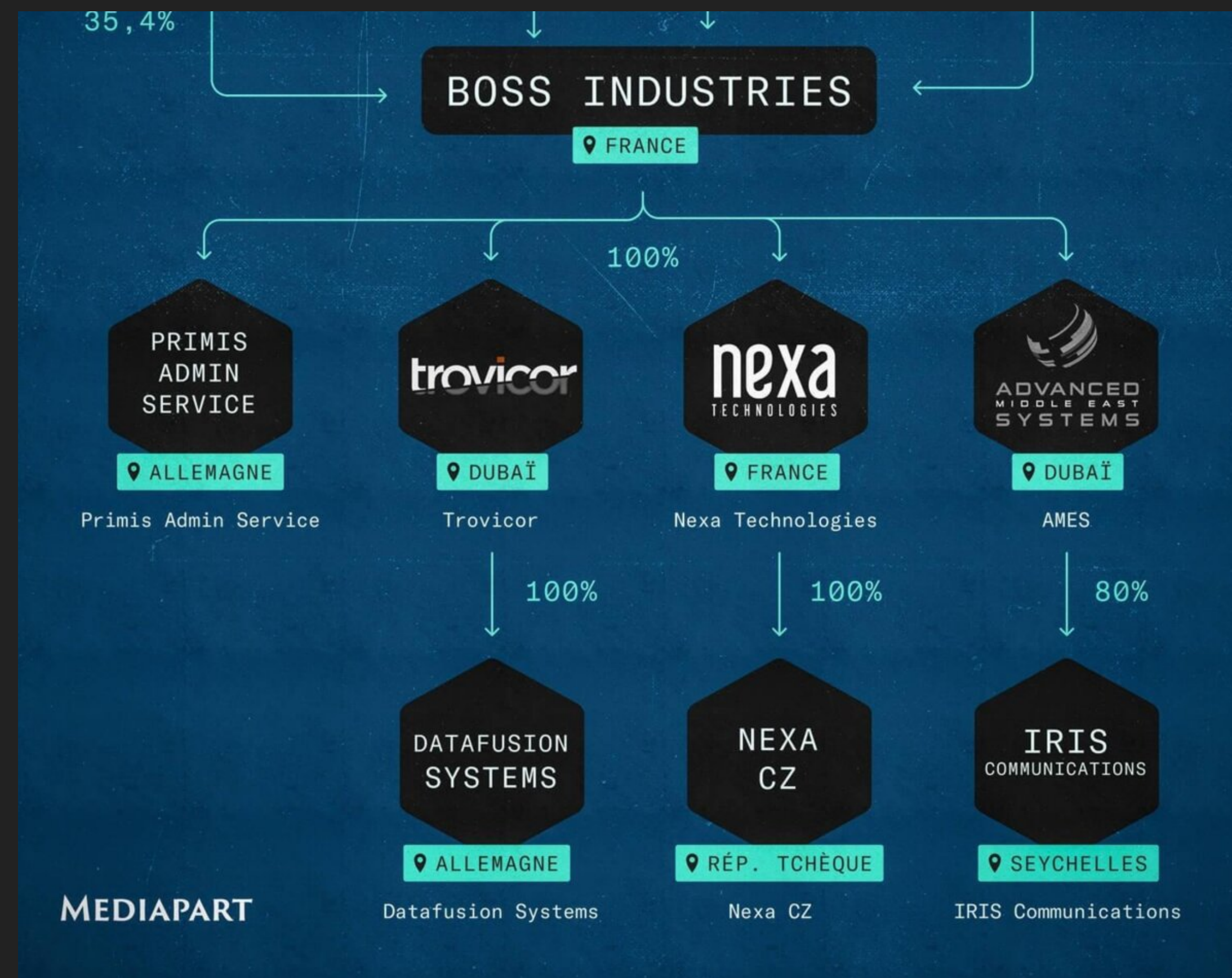
Replying to @iingwen

South China Sea: PLA 'expels ship' near Fiery Cross Reef [southchinapost.net/RtQBG](https://www.southchinapost.net/RtQBG)

UNRAVELING THE ATTACKS

In 2020, Nexa Technologies signed an initial deal for “infection solutions” with Viet Nam's Ministry of Public Security (MOPS) through the Nexa group's UAE-based sales subsidiary **Advanced Middle East Systems**.

The deal was worth 5.6 million Euros.



EUROPEAN
INVESTIGATIVE
COLLABORATIONS



MEDIAPART

DER SPIEGEL

THE INVESTIGATION

UNRAVELING THE ATTACKS

On 19 February 2021, **Advanced Middle East Systems** signed an agreement for spyware solutions with **Delsons Hong Kong Ltd.**

Thank you for your prompt answer by email and for your information.

Our main target is Ministry of Public Security of Vietnam , in your particular field , they have several projects in progress. Customer will also be attending tomorrow some exhibition on the subject done in Hanoi. It is an overall budget which includes not only your project. Time frame : Projects over the 2012-2021

If you are already in touch with end users in Vietnam I do understand and do not want to trouble the same customers. If you can disclose the name of your partner, I can easily check with my customers if they have been approached or not?

If it is possible to cooperate

Best Regards

Alexis Delevaux

Our main target is Ministry of Public Security of Vietnam , in your particular field , they have several projects in progress. Customer will also be attending tomorrow some exhibition on the subject done in Hanoi. It is an overall budget which includes not only your project. Time frame : Projects over the 2012-2021

< 10/13 >

Transaction date	2021/11/01
B/L No.	--
Buyers	Bca Thang Long One Member Limited Company
Supplier	Delsons Hong Kong Ltd.
Import area	Vietnam
Export area	Israel
Product description	MOBILE SMART PHONE MONITORING MODULE BELONGING TO PROFESSIONAL SOFTWARE SYSTEM, MANUFACTURER: AS @ Translate

Product description	MOBILE SMART PHONE MONITORING MODULE BELONGING TO PROFESSIONAL SOFTWARE SYSTEM, MANUFACTURER: AS @ Translate
---------------------	---

POL	--
-----	----

VIET NAM – MINISTRY OF PUBLIC SECURITY

Department of Professional Technology (Cục Kỹ thuật nghiệp vụ)

Technical unit of the Viet Nam Ministry of Public Security (formerly units A70 and A71). Documents suggest Nexa Group has previously worked with this department.



Headquarters in Ho Chi Minh City - 258 Nguyen Trai



HOW DIGITAL THREATS ENABLE PHYSICAL THREATS

Hotel Rwanda activist's daughter placed under Pegasus surveillance

US-Belgian citizen Carine Kanimba has been leading effort to free her father after forced return to Kigali



📷 Carine Kanimba and her father, Paul Rusesabagina. Forensic analysis found that Kanimba's phone had been infiltrated since at least January this year. Composite: AFP/Getty Images/Belga

The Pegasus Project A global investigation

Jamal Khashoggi's wife targeted with spyware before his death

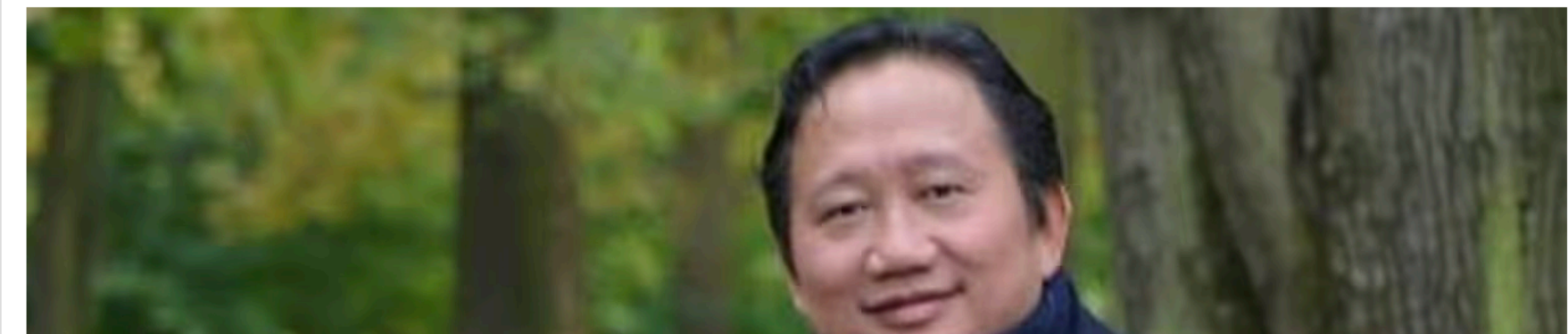
The cellphones of murdered Saudi columnist's fiancée and associate hacked after his murder



A police officer passes a portrait of Jamal Khashoggi near the Saudi Consulate in Istanbul during a ceremony marking the first anniversary of his murder. Several associa

Germany accuses Vietnam of abducting businessman from Berlin

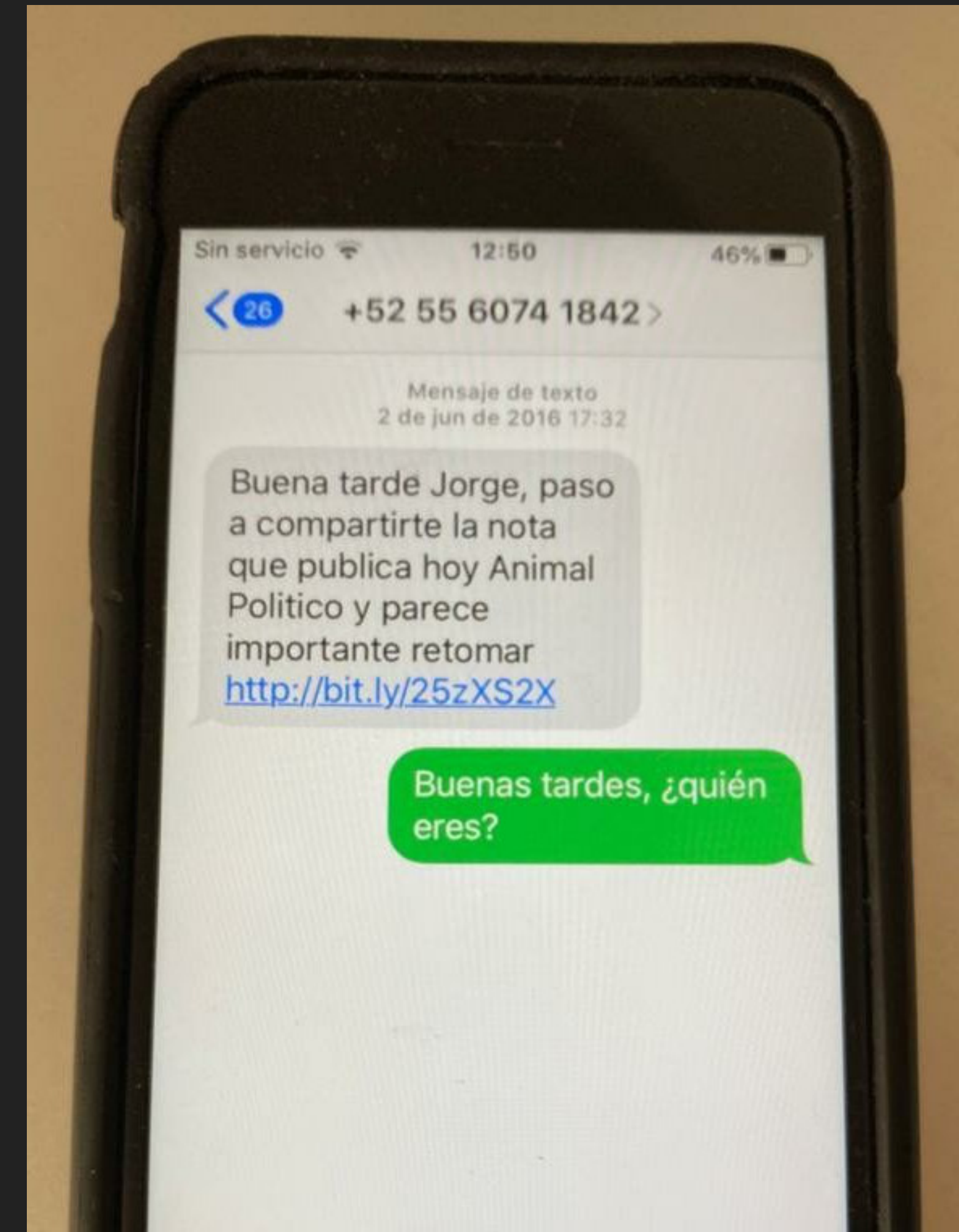
Vietnam's spy chief has been expelled from Germany, which was processing Trinh Xuan Thanh's asylum claim after 3.3bn dong went missing from state oil company



INTELLEXA'S ECOSYSTEM OF PRODUCTS

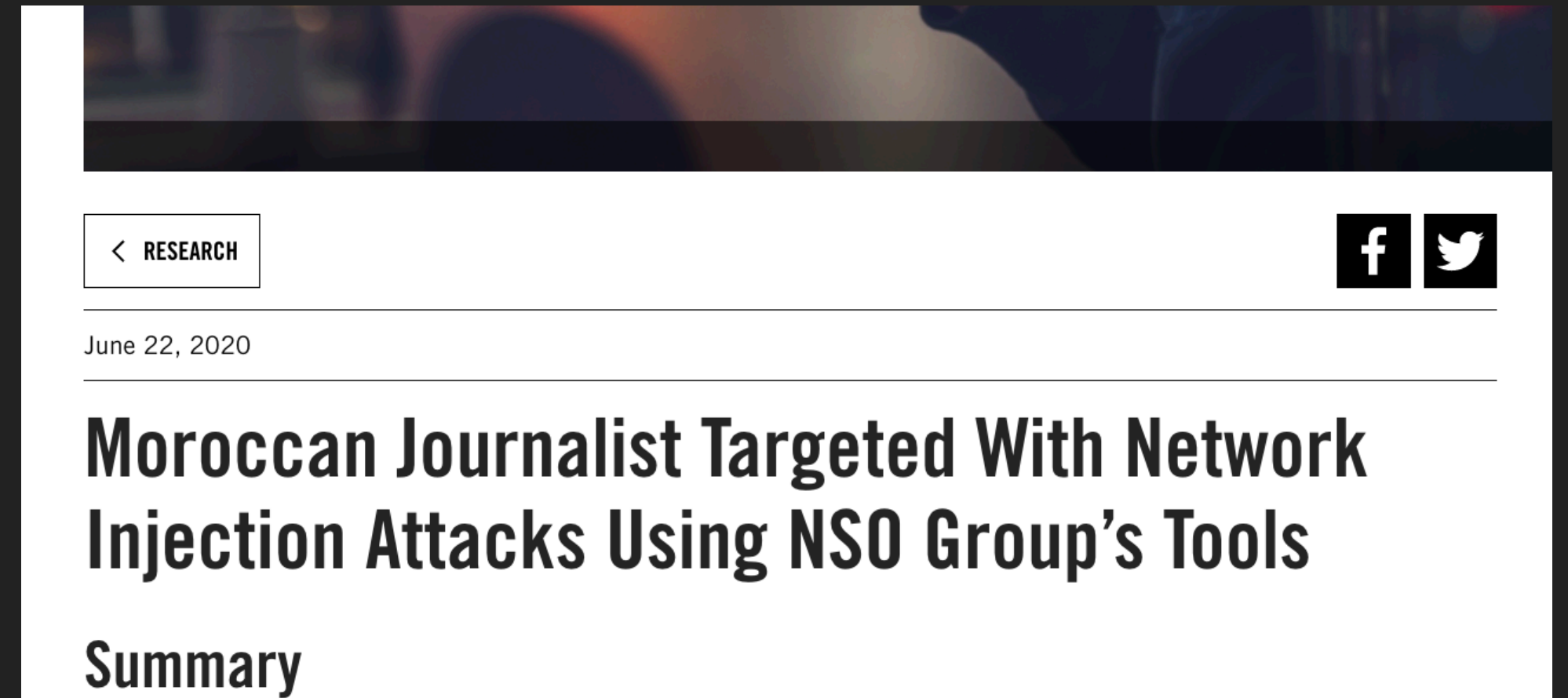
INTELLEXA'S 1-CLICK PREDATOR SPYWARE

- ▶ Predator is typically delivered as 1-click spyware.
- ▶ However, customers want the stealthiness and reliability of zero-click attacks.
- ▶ Zero-clicks can be very expensive
- ▶ Intellexa has some tricks up their sleeves...



NETWORK INJECTION – UPGRADE 1-CLICK TO ZERO-CLICK

- ▶ Enables a standard browser exploit to automatically infect a device without user interaction.
- ▶ A powerful attack, as it can be difficult for an individual to detect that their phone has been silently redirected.



RESEARCH

June 22, 2020

Moroccan Journalist Targeted With Network Injection Attacks Using NSO Group's Tools

Summary

This screenshot shows the top portion of a research article. It features a navigation bar with a 'RESEARCH' label and social media icons for Facebook and Twitter. Below this is the date 'June 22, 2020' and the main title 'Moroccan Journalist Targeted With Network Injection Attacks Using NSO Group's Tools'. A 'Summary' link is visible at the bottom of the header section.



BAD TRAFFIC

Sandvine's PacketLogic Devices Used to Deploy Government Spyware in Turkey and Redirect Egyptian Users to Affiliate Ads?

By Bill Marczak, Jakub Dalek, Sarah McKune, Adam Senft, John Scott-Railton, and Ron Deibert

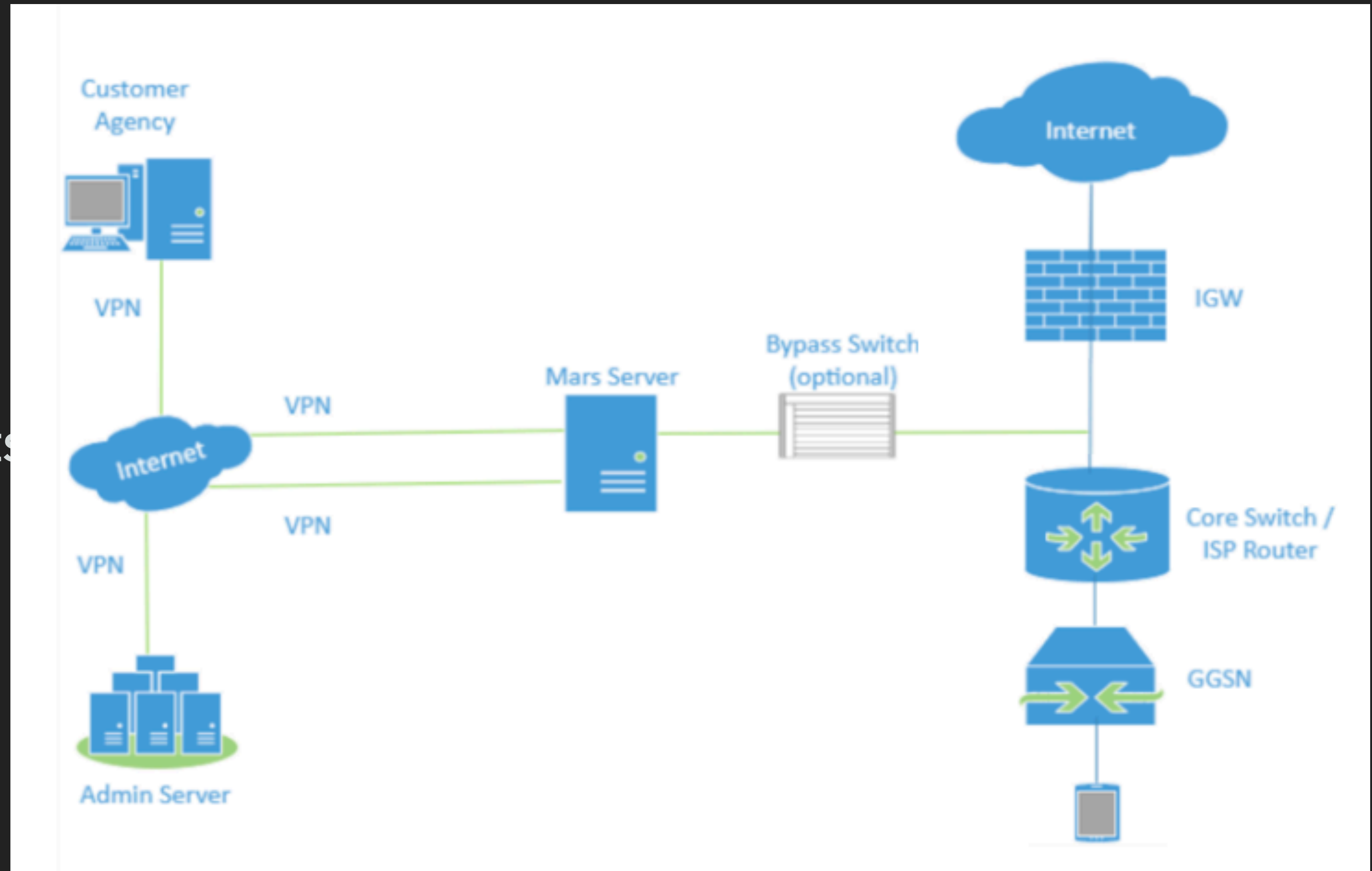
March 9, 2018 [أزمة مروية \(Arabic translation\)](#), [KÖTÜ TRAFİK \(Turkish translation\)](#)

Download this report

This screenshot shows the header of a report titled 'BAD TRAFFIC'. The main title is 'Sandvine's PacketLogic Devices Used to Deploy Government Spyware in Turkey and Redirect Egyptian Users to Affiliate Ads?'. The authors listed are Bill Marczak, Jakub Dalek, Sarah McKune, Adam Senft, John Scott-Railton, and Ron Deibert. The date is March 9, 2018, and there are links to Arabic and Turkish translations. A 'Download this report' button is located at the bottom.

INTELLEXA'S MARS - ISP LEVEL NETWORK INJECTION

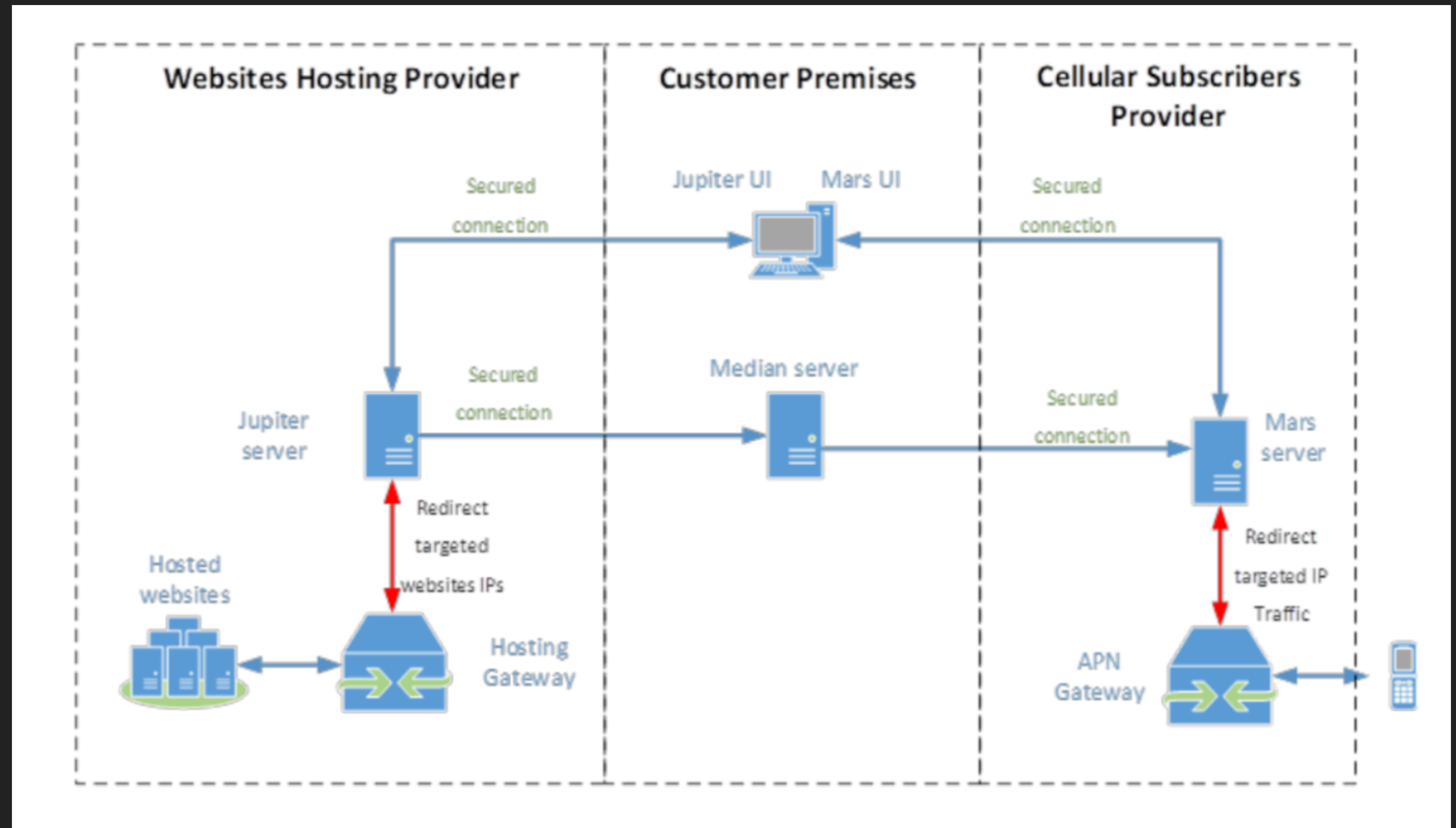
- ▶ Network hardware installed at mobile ISPs enable redirection and infection of targeted mobile devices.
- ▶ Automatically redirect targets to Predator 1-click links.



Intellexa's Mars ISP network injection system

INTELLEXA'S JUPITER - ISP LEVEL NETWORK INJECTION ON ENCRYPTED TRAFFIC

- ▶ "Jupiter" enabled the infection of visitors to HTTPs encrypted websites.
- ▶ Attack requires ability to manipulate traffic to hosting provider of target website.



INTELLEXA ALLIANCE - TACTICAL NETWORK INJECTION



WI-FI AND GSM TACTICAL NETWORK INJECTION

- ▶ Long-range Wi-Fi hardware, drones, and fake base stations can be used to intercept and infect target devices.

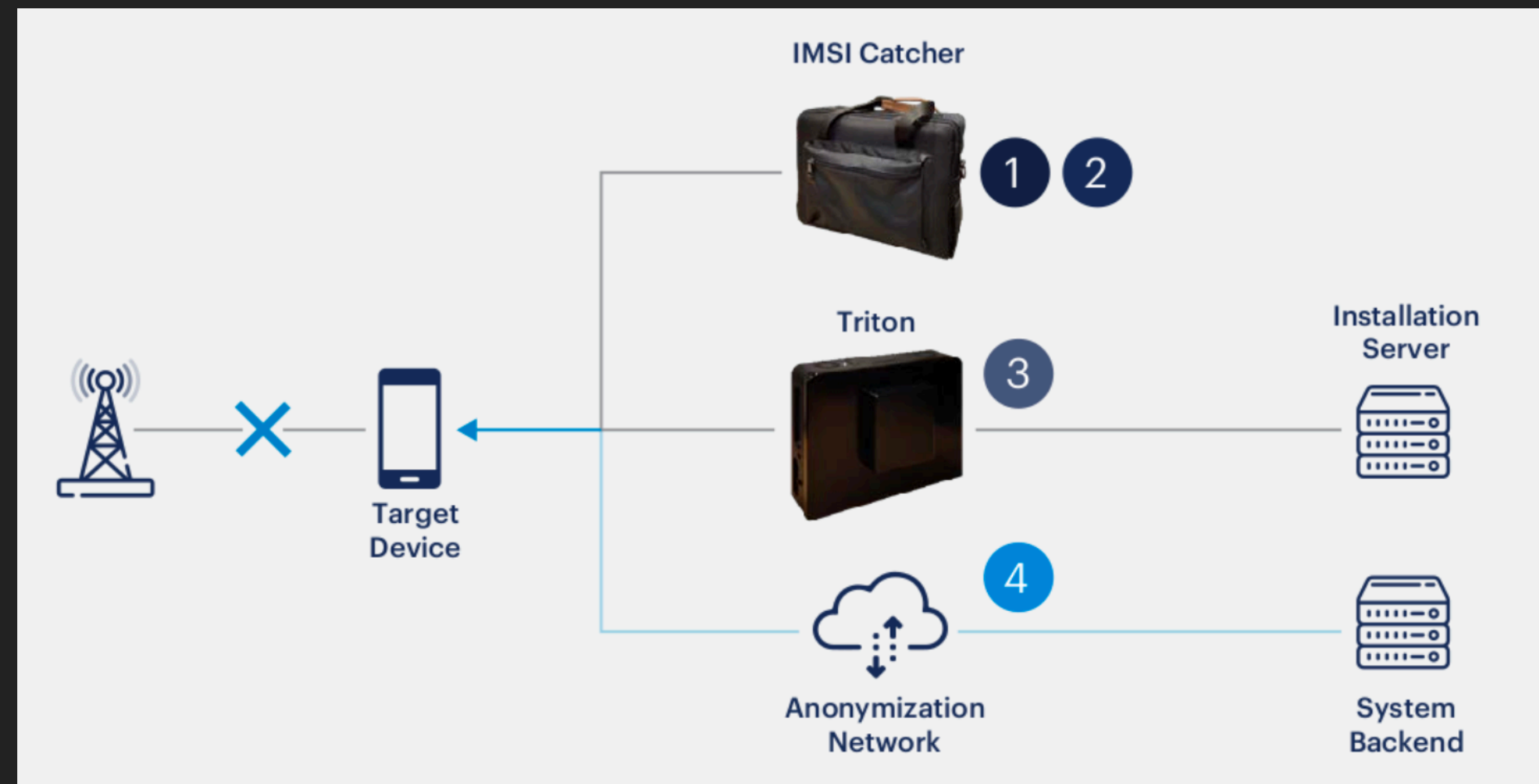


INTELLEXA'S TRITON – TACTICAL BASEBAND ATTACK AGAINST SAMSUNG DEVICES

- ▶ Appears to be a full zero-click attack not relying on a pivot to a browser exploit.
- ▶ May still be a zero-day.

Triton Operational Flow

Triton tactical operation requires the target to be downgraded from 5G/4G/3G to a specific channel, then delivers the agent to the mobile device with a simple click. The downgrading process can be performed with Intellexa's IMSI catcher, or with any IMSI Catcher which can be useful, should the customer already possess one.



THE WIDER PROBLEM

EGASUS
MEXIQUE,
SPIONS

Passé sanitaire: l'exécution
Le projet de loi instituant l'obligation vaccinale pour les soignants et un passe sanitaire pour les citoyens a été présenté en conseil des ministres le 15 juillet.

REVELATIONS SUR UN SYSTEME MONDIAL D'ESPIONNAGE DE TELEPHONES
Hommes politiques, avocats, militants et journalistes sont les premières victimes

LE VISEUR DU MAR

The Guardian For 200 years
Tuesday 20 July 2021
A Guardian special investigation
Exclusive interview Edward Snowden
"If you don't stop this, it's not going to be 50,000 targets. It's going to be 50 million"

Modi accused of spyware complicity
Aides of Mexican president on list
Fears that Apple software vulnerable

PM reveals job certificates will be needed to enter nightclubs

Depuis 2016, des dizaines de milliers de téléphones ont été sélectionnés comme cibles d'un logiciel d'espionnage baptisé « Pegasus », commercialisé par la société israélienne NSO

Six mois d'une enquête internationale réunissant dix-sept médias, dont « Le Monde », montrent que cet outil, officiellement destiné à lutter contre le terrorisme, est massivement utilisé pour surveiller les sociétés civiles

En France, un millier de numéros ont été

Le Parisien 75
Teddy Riner Son grand rendez-vous avec les JO
PAGES 14 ET 15
La Conspiration des Belettes

The Guardian For 200 years
Monday 19 July 2021
From £1.75 for subscribers

led leak uncovers global of spy weapon

It's heinous' Activists and journalists among thousands on list
Jamal Khashoggi Associates targeted after his death

Libération 21 JULLET 2021
Espionnage Macron

Le Monde Mercredi 21 juillet 2021 N° 23915 - 170 €
Spécial Covid L'épidémie s'emballe comme jamais
Espionnage Macron ciblé
Le président de la République et l'ensemble de son gouvernement de 2019 ont été visés par le logiciel d'espionnage qui pirate

zeigt sich, was Armin Laschet kann - und was nicht > Die Seite Drei
Süddeutsche Zeitung
NEUESTE NACHRICHTEN AUS POLITIK, KULTUR, WIRTSCHAFT UND SPORT
Das Streiflicht
Cyberangriff

Le Monde
EMMANUEL MACRON DANS LE VISEUR DU MARC
PROJET PEGASUS
Un des numéros de téléphone du chef de l'Etat a été sélectionné par les services secrets marocains en vue d'une potentielle mise sous surveillance
Seule une analyse technique de l'appareil peut révéler s'il a été infecté par le logiciel de NSO
Edouard Philippe, alors premier ministre du gouvernement, a été ciblé

SPYWARE ABUSES THREATEN ACTIVISTS, JOURNALISTS, AND CRITICS WORLDWIDE

The Washington Post
Democracy Dies in Darkness

Egyptian presidential hopeful targeted by Predator spyware

Rare 'zero-day' exploit used in failed hacking attempt that researchers say was probably conducted by the Egyptian government

By [Evan Hill](#) and [Joseph Menn](#)
September 23, 2023 at 9:30 a.m. EDT

accessnow NEWS & UPDATES TAKE ACTION OUR WORK GET HELP

Spyware in Serbia: civil society under attack

PUBLISHED: 28 NOVEMBER 2023 LAST UPDATED: 21 DECEMBER 2023

In the latest example of how invasive surveillance technology is being used to silence and suppress civil society, Access Now, SHARE Foundation, the Citizen Lab at the Munk School of Global Affairs & Public Policy at the University of Toronto

THE CITIZEN LAB munkschool OF GLOBAL AFFAIRS & PUBLIC POLICY UNIVERSITY OF TORONTO RESEARCH NEWS ABOUT

Research > Targeted Threats

PREDATOR IN THE WIRES

Ahmed Eltantawy Targeted with Predator Spyware After Announcing Presidential Ambitions

By Bill Marczak, John Scott-Railton, Daniel Roethlisberger, Bahr Abdul Razzak, Siena Anstis, and Ron Deibert

Dominican investigative journalist targeted with NSO spyware, report says

Nuria Piera, known for her investigations into corruption, was targeted three times, Amnesty International says

Stephanie Kirchgaessner
in Washington

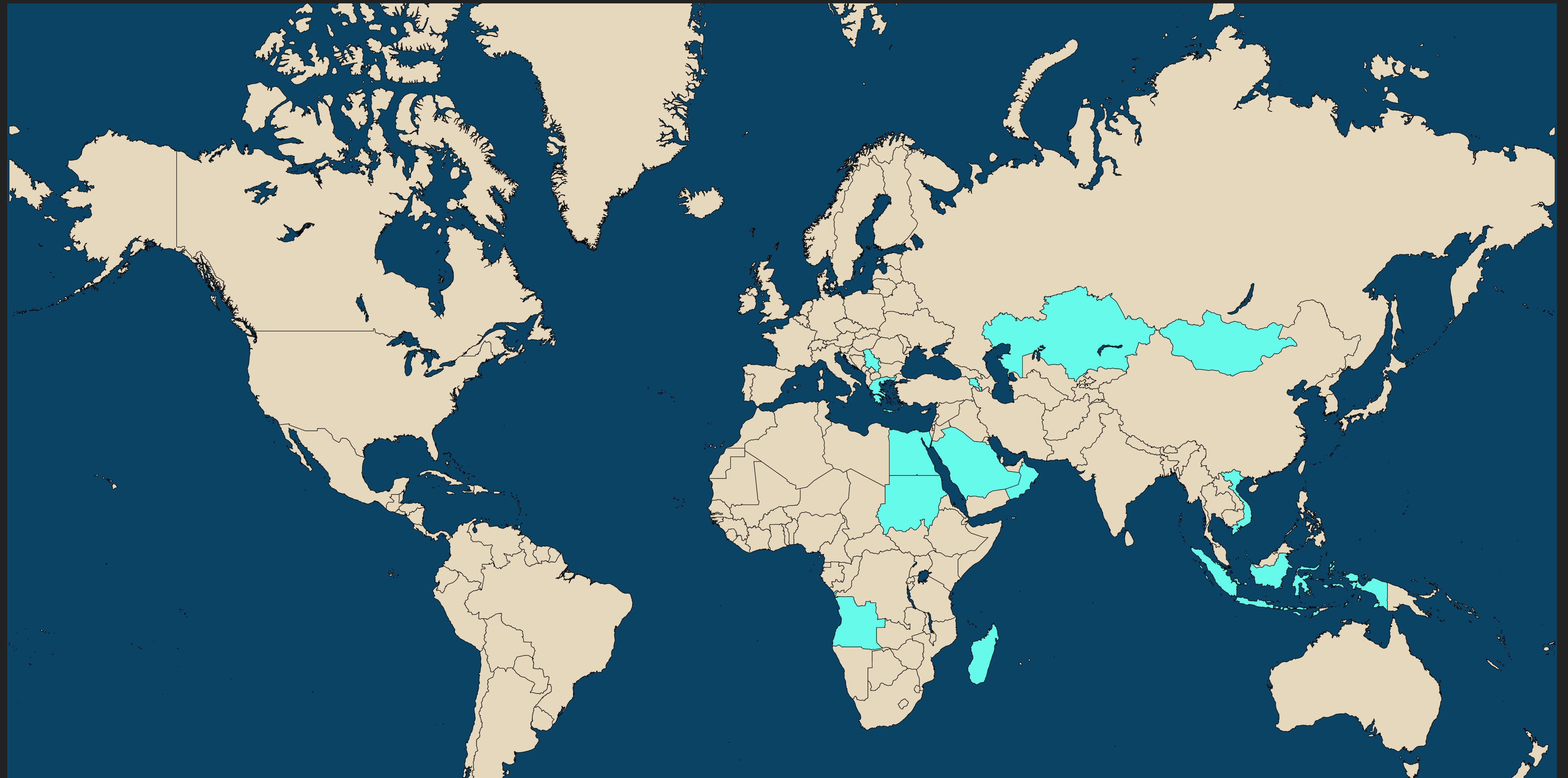
@skirchy
Wed 3 May 2023 00.25 CEST

f t e

INTELLEXA AND COMPETITORS SPREAD SPYWARE WORLDWIDE

Predator customers or targeting activity:

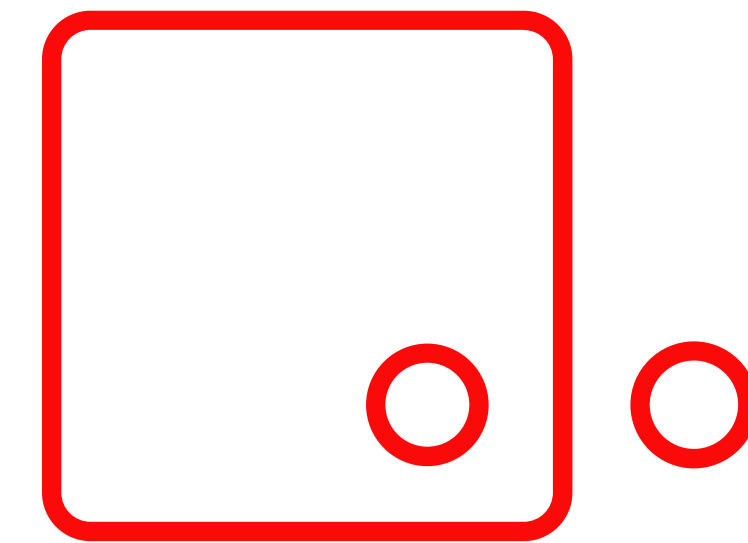
- Angola
- Armenia
- Egypt
- Greece
- Indonesia
- Kazakhstan
- Madagascar
- Mongolia
- Oman
- Saudi Arabia
- Serbia
- Sudan
- Trinidad and Tobago
- Vietnam



EUROPEAN COMPANIES FUEL THE CYBER-SURVEILLANCE INDUSTRY



DSIRF



MEMENTO LABS™
HUNTING IN THE DARK

VARISTON



THE RULE-MAKERS BENEFIT FROM A LACK OF ACCOUNTABILITY

Greece to launch parliamentary inquiry into spy scandal

Move follows revelations that opposition leader was placed under surveillance while serving as MEP



HAARETZ

Flight of the Predator: Jet Linked to Israeli Spyware Tycoon Brings Surveillance Tech From EU to Notorious Sudanese Militia

A cross-continental investigation uncovered a network of firms connected to Tal Dilian, ex-

WHAT TO DO?

DEFENDING AGAINST PREDATOR

- ▶ Enable any enhanced security modes on your devices.
 - ▶ Lockdown Mode for iOS is the gold-standard protection against zero-click and 1-click attacks
 - ▶ Google's Advanced Protection program enables HTTPS-Only mode in Chrome
 - ▶ Firefox and many browsers support opt-in HTTPS-Only mode
- ▶ Consider using an always-on-VPN if you believe you are at risk of targeted network injection attacks.

WHAT CAN YOU DO?

DO NOT work for the mercenary spyware industry

This industry empowers human rights abusers, helps them control their critics and maintain systems of injustice and oppression.

THANK YOU

Email: donncha.ocearbhaill@amnesty.org

PGP: 5AD9 8B48 22EC 24D0 66F1 7D56 DA11 9656 A48F 4954

Keybase: DonnchaC

<https://securitylab.amnesty.org>

Zero-days, exploits, leaks and whistleblowers welcome!