Spyware for rent

Les Assises de Monaco 2024

Fred Raynal
fraynal@quarkslab.com

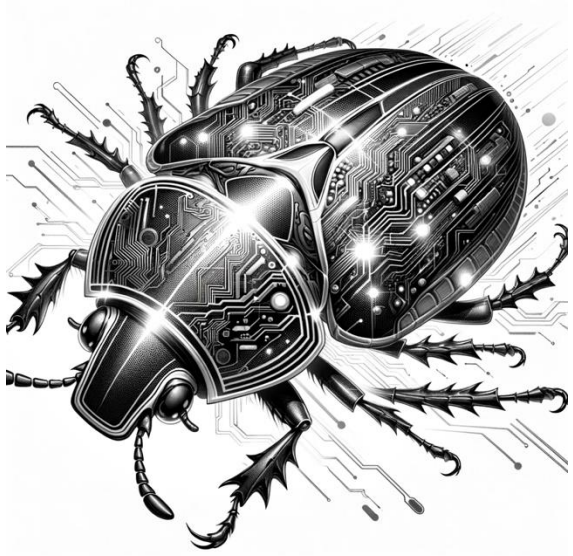
LES ASSISES

Quarkslab

What is spyware?

Quarkslab

Spyware?



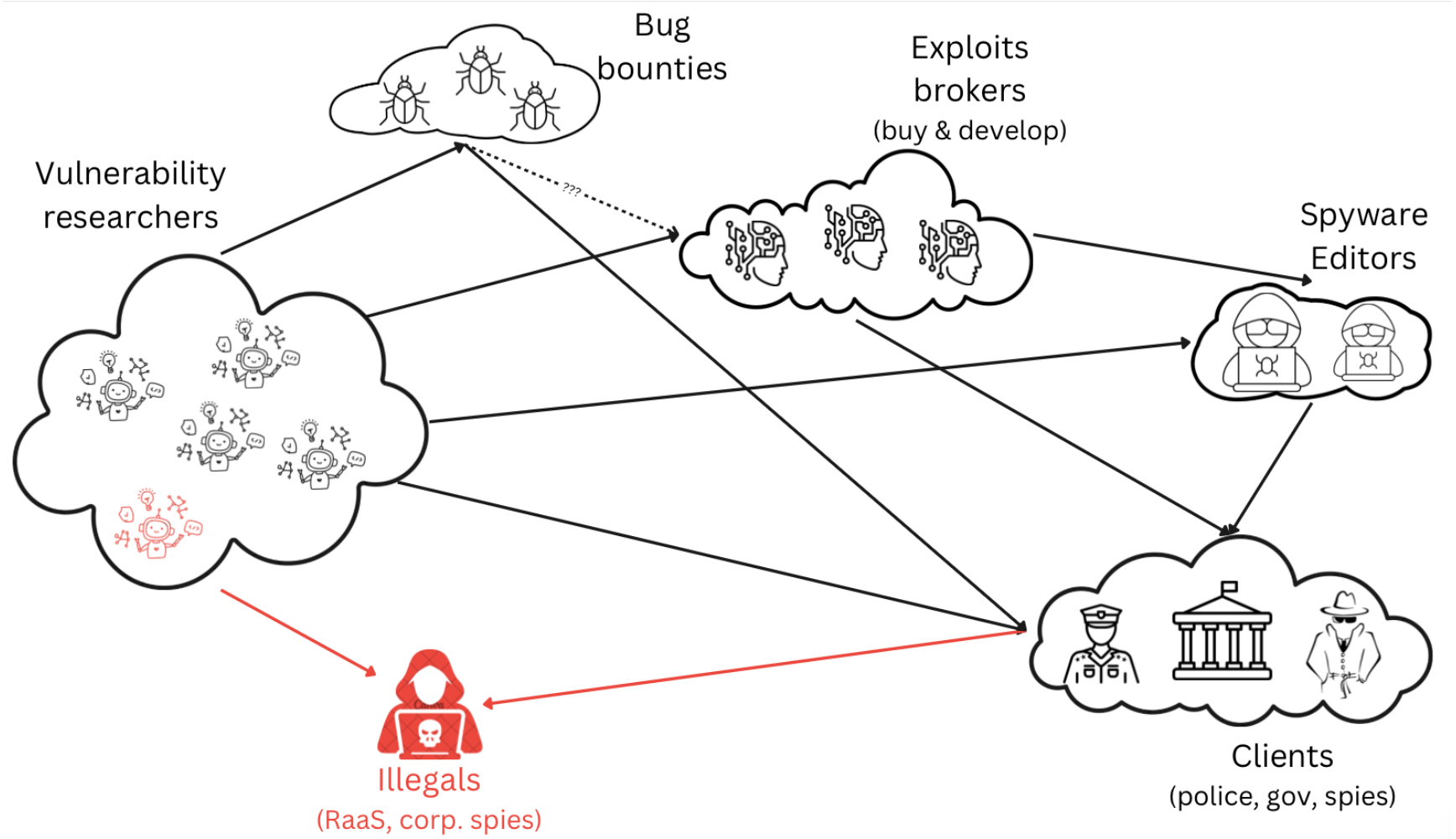
A software that enables a user to obtain covert information about another's computer activities by transmitting data covertly from their system.

Covert information: localization, messages, pictures, voice, passwords…

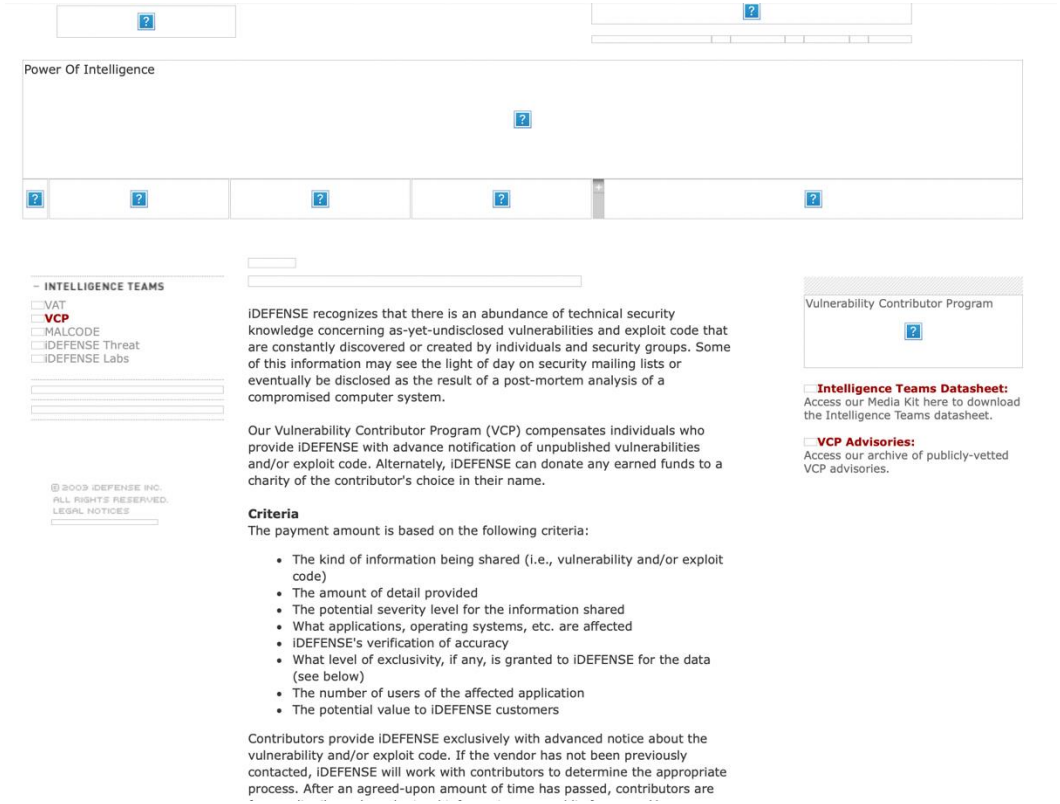
Targets

- **Journalists**: especially in countries where press freedom is not obvious, to identify the sources
- **Human rights activists**: targeted by authoritarian regimes to suppress activism and limit international exposure
- **Politicians and Opposition Figures**: governments spy on opposition members or critics, including foreign officials
- **Lawyers**: when involved in human rights cases or sensitive legal matters, likely to compromise client information
- **Business people**: some high-profile business figures are targeted, possibly for financial or competitive advantages
- **Diplomats**: targeted to gather sensitive information about negotiations or political/economic strategies.

The spyware (under)world



Buying 0-days: iDefense Vulnerability Contributor Program (2003)



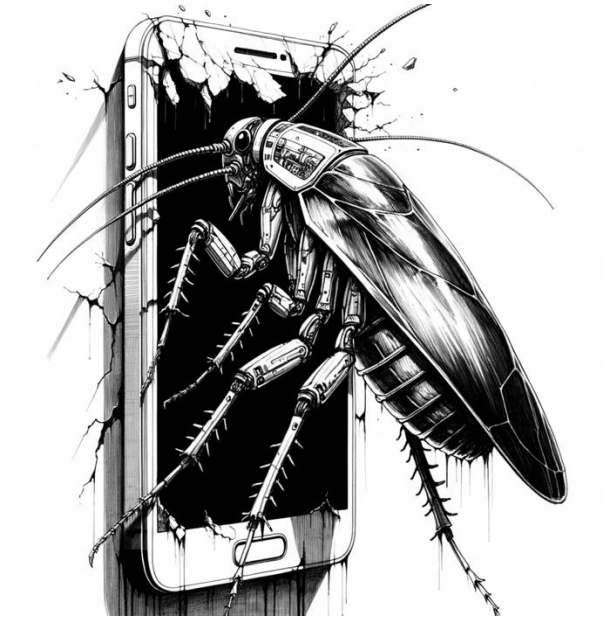
How does payment work?
I am a regular contributor. Is it possible to get a base salary and/or add to it like a bonus plan for each vulnerability report I send in?

Who/what is iDEFENSE?
iDEFENSE Inc. was founded as Infrastructure Forum Inc. in May 1998. The company opened offices in Virginia later that year, and around this time changed its name to Infrastructure Defense Inc. The philosophy driving the change was that information-sharing and detailed analysis of cyber threats were and still are key to protecting any critical information infrastructure. Since then, iDEFENSE has been a comprehensive provider of security intelligence to governments and Fortune 500 organizations. The company's goal is to help customers avoid or mitigate threats to customers' information assets, computers, networks, Internet functions, and proprietary information before a crisis occurs, thereby minimizing potential disruption to network and business operations.

What is the purpose of the VCP?
Our main purpose in creating the VCP is to provide iDEFENSE clients with the most timely security intelligence available. We recognize that there is an abundance of technical security knowledge concerning as-yet-undisclosed vulnerabilities, exploits and malicious code that is constantly discovered and created by individuals and security groups. Some of this information may see the light of day on security mailing lists or are eventually disclosed as the result of a post-mortem analysis of a compromised computer system. We believe that one effective way to capture this data is by going straight to the source, i.e. you the security researcher.

http://idefense.com/poi/teams/vcp.jsp?flashstatus=false (yes, I don't have flash ;-) 10/2003

Initial access: 0-days, 0-days, 0-days



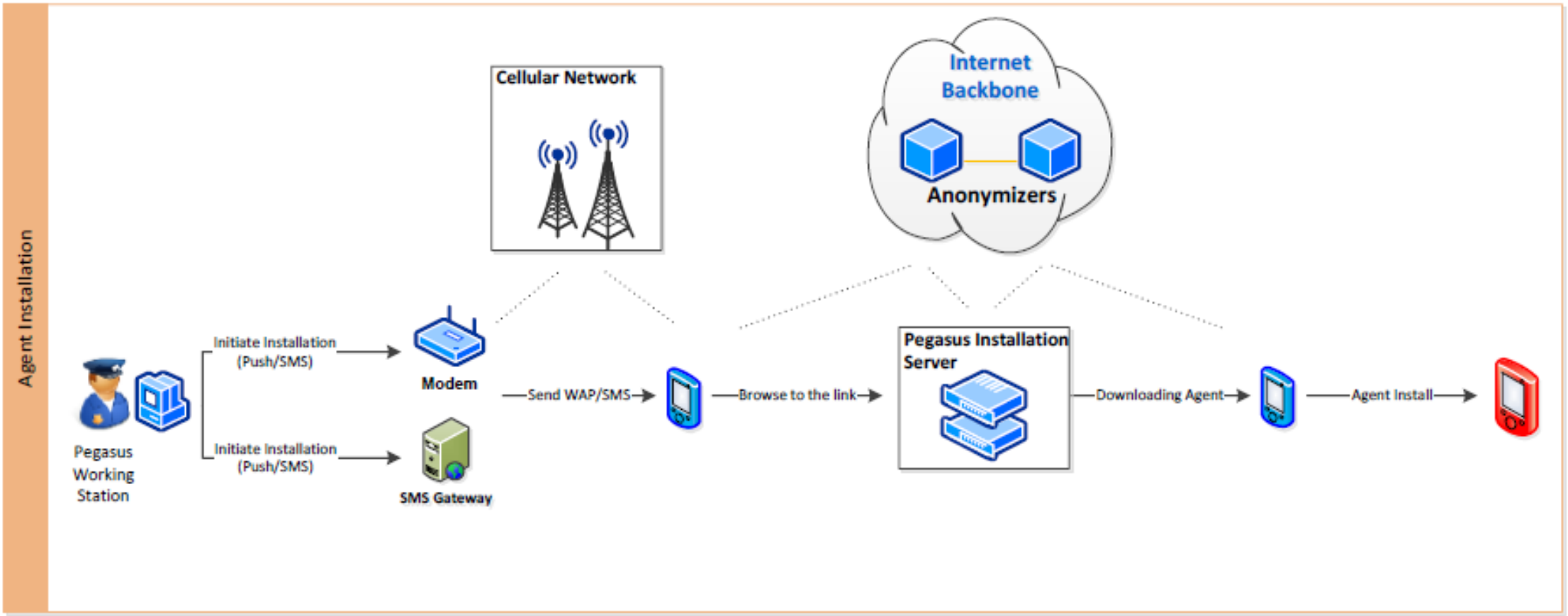
- **Before 2018**: a sms was sent to the target with a link, an image, anything, requiring to click to trigger the exploit
- **From 2018-2019**: applications were also targeted (WhatsApp, Messenger…)
- **1-click**: user needs to click on something to trigger the exploit (web chain)
- **0-click**: exploit is sent and executed without the need for the user to do anything

Data Gathering

- Textual: Textual information includes text messages (SMS), Emails, calendar records, call history, instant messaging, contacts list, browsing history and more. Textual information is usually structured and small in size, therefore easier to transmit and analyze.
- Audio: Audio information includes intercepted calls, environmental sounds (microphone recording) and other audio recorded files.
- Visual: Visual information includes camera snapshots, photos retrieval and screen capture.
- Files: Each mobile device contains hundreds of files, some bear invaluable intelligence, such as databases, documents, videos and more.
- Location: On-going monitoring of the device location (Cell-ID and GPS).

From Pegasus: product description (about **2013**!!)

How does it work: overall architecture



From Pegasus : product description (about **2013**!!)

Data Exfiltration

OPSEC 101

1. Data is collected on the phone
   - Data is usually encrypted
2. Data is pushed on anonymized servers
   - Encryption / authentication with the servers
3. Data is collected by spycorp
   - Push (mobile -> servers) / pull (servers <- backend)
4. Data is analyzed & provided to the customers
   - Forensic capabilities to extract / visualize key information

How does it work: anonymisation layers

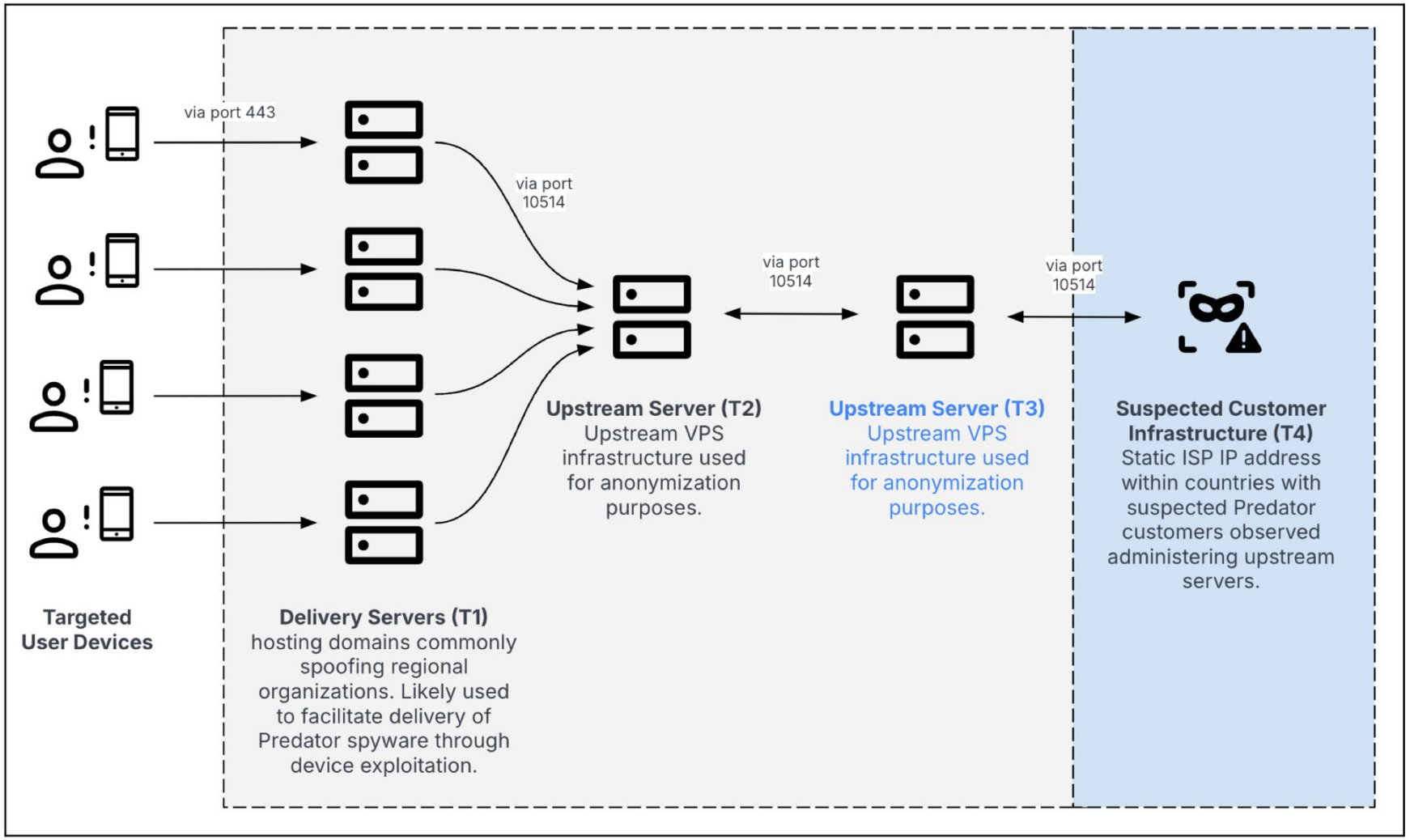


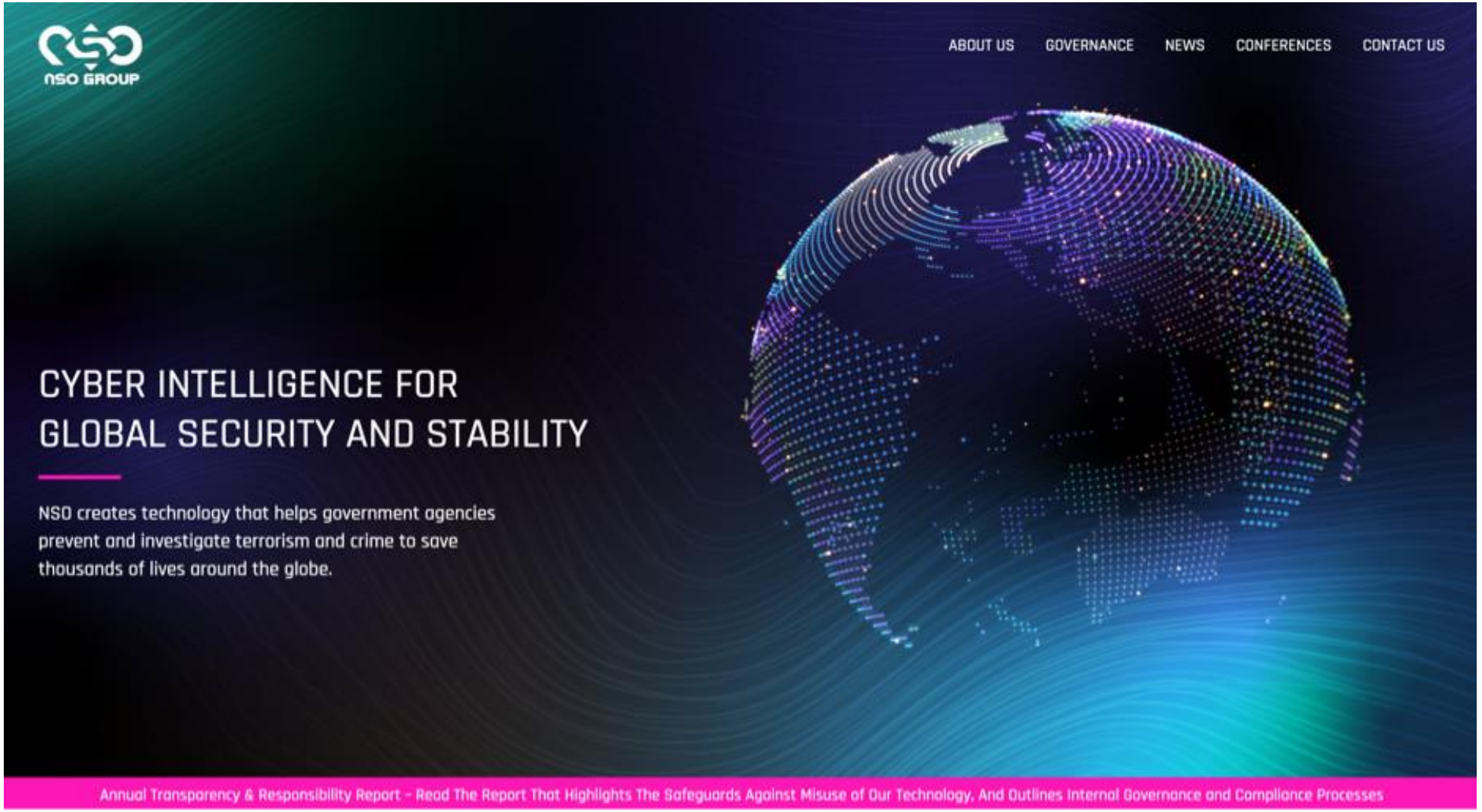
Figure 2: *Multi-tiered Predator infrastructure with additional tier (Source: Recorded Future)*

https://www.recordedfuture.com/research/predator-spyware-infrastructure-returns-following-exposure-sanctions

Marketing

Quarkslab

Marketing: NSO



Marketing: Intellexa

About us

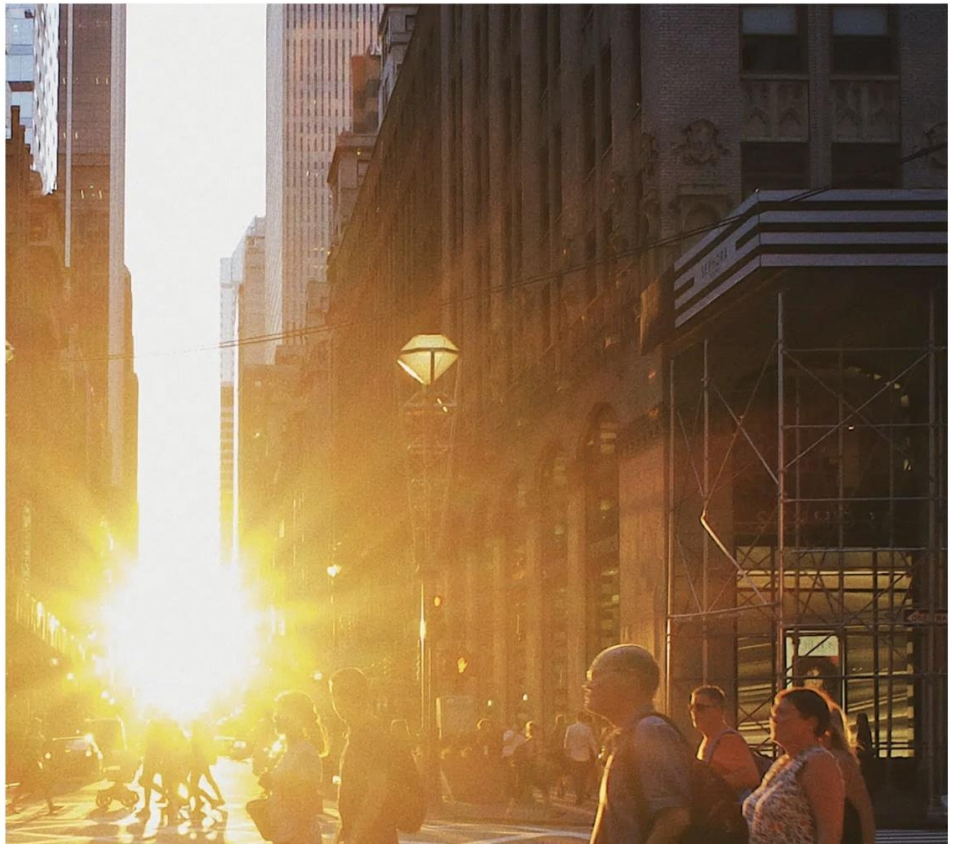
001 / CORPORATE

WE DEVELOP AND INTEGRATE TECHNOLOGIES TO EMPOWER LEAs AND INTELLIGENCE AGENCIES TO HELP PROTECT COMMUNITIES

Fighting crime in the digital dimension has become a tremendous challenge for law enforcement agencies around the world. Criminals operating under an encrypted multi digital eco-system, have made data collection virtually impossible. And data is only a part of the equation.

Deep, insightful and actionable intelligence demands an holistic approach. Connecting the dots and creating a 360-degree perspective feeds precise decision making and results.

We enhance your power to investigate from paedophiles to organized terror groups, human trafficking or financial fraud.



Marketing: Candiru

:))

Pricing

Quarkslab

Intellexa
Aug. 2022

intellexa

2 Price Proposal

#	Item	Description	Qty.	Price (EURO)
1	**Nova** Remote Data Extraction from Android & iOS Devices & Analytics system	Delivery Studio: Remote 1-Click Browser-based capability to inject Android & iOS payload to mobile devices through link delivery	1	Included
		Supported devices: iOS & Android supported devices (list attached)	1	
		Android Support:* • Android 12 (latest version)*** + 18 months back **iOS Support: *** • iOS latest version*** 15.4.1 + 12 months back	1	
		Agent Concurrency Scope: • 10 Concurrent infections for both OS families (iOS and Android) (i.e. total of 10 infections which may be split between iOS and Android as per the customer sole decision).	10	
		Successful infections magazine: • Magazine of 100 Successful infections.	100	
		Geographical Coverage: Inside the country for local SIM cards on iOS or Android devices.	1	
		Fusion & Analytics system Investigation platform for analysis of all Cyber data extracted by NOVA system. • Cases and targets investigation • Search, filter, analyze and manage cyber data		
2	**Hardware & Software**	The entire Nova Suite will be delivered turnkey: • All proprietary software and 3rd party software shall be provided by Intellexa. unless written specifically otherwise under the agreement. • Cloud services, domains and anonymization chain which will be provided and managed by customer.	1	Included
3	**Project Management**	A complete project plan will be provided by INTELLEXA to be approved and coordinated with the customer: • Delivery & Project Plan • Final Design Review • Site Acceptance Testing (Customer site) Technical, operational and methodology	1	Included
4	**Warranty**	Twelve (12) months Warranty as further detailed under section 2.2 below.	1	Included
5	**Price**			**€8,000,000**

Intellexa
Aug. 2022

2.2 Warranty & Maintenance as Part of the Contract

	Warranty & Maintenance	Description	Qty.	Price (EURO)
1	**12 Months Warranty**	Complete warranty and support for 1 year after completion of solution delivery to customer. Warranty includes: • Major and minor updates and upgrades • Bug-fixes and technical-support	1	Included
2	**Maintenance Services** for OS and Supported Devices	Standard package. Include- Minor and Major updates (Appendix B).	1	Included

2.3 Optional Products & Services

#	Item	Description	Qty.	Price (EURO)
1	Year 2 Optional Maintenance Contract	Optional maintenance contract for the second year including all services and SLA of the Warranty year.	1	30% of Contract (Per Year)
2	NOVA Persistency	Reboot-Persistency • Support for iOS & Android • Agent will survive phone shutdown and reboot. • Agent will not survive factory reset • Persistency method will not prevent version updates on the device. Effects of versions updates on persistency may vary and shall be reflected in SLA commitment	1	€3,000,000
3	NOVA International	Additional 5 countries package to be mutually agreed on, with no geographic limitation of target location	1	€1,200,000

Some insights from NSO

Quarkslab

An example through NSO Timeline

- 2010 : founded by
  - Niv Karmi (former MOSSAD),
  - Omri Lavie, and Shalev Hulio, former founders of CommuniTake (remote support from cellphone)
- 2011 : 1st version of Pegasus
- 2013: annuel revenue = $40 million
- 2014 : private equity Francisco Partners (US) buys NSO for $130 million + Circle (phone geolocation tool) for $130 million,
- 2015: annual revenue = $150 million
- 2017 : Francisco Partners tried to sell NSO for $1 billion
- 02/2019 : Francisco Partners sold back 60% of NSO to co-founders Shalev Hulio and Omri Lavie supported by European private equity fund Novalpina Capital for a valuation of about $1 billion
- 07/2021 : Novalpina Capital handed over all of its assets (including NSO) to Berkeley Research Group (BRG) due to unresolved personal dispute amongst the co-founders
- 11/2021: The U.S. Commerce Department added Israel's NSO Group and Candiru to its trade blacklist
  - All along with Positive Technology (RU) and Computer Security Initiative Consultancy PTE LTD (SG)
- 12/2021: NSO described the company as insolvent
- H1/2022: L3Harris Technologies engaged secret talks to acquire NSO tech and team
  - US ownership would lift the ban, L3Harris provider for the 5 eyes
  - Israel wanted to keep being the ones issuing export licences, and forbid L3Harris developers in NSO
- 06/2022: press publish about the talks, the deal blow
- 08/2022: Hulio stepped down from his role of CEO + downsizing workforce from 750 to 650
- 03/2023: Omri Lavie re-emerged in control of NSO after legal fights

NSO: "A few" controverses along the road

- 10/2018: NSO suspected to be involved in the murder of the Saoudi journalist Jamal Khashoggi by selling Pegasus to Saoudi Arabia
- 04/2019: NSO froze its deals with Saudi Arabia
- 10/2019: WhatsApp sued NSO for exploiting 1500 users in 20 countries, including journalists and human rights activists
- 07/2021: Forbidden stories disclosed the results of their investigation following the leak in 2020 of a target list of 50,000 phone numbers
  - The Pegasus Project : https://forbiddenstories.org/case/the-pegasus-project/
  - List of targets: https://en.wikipedia.org/wiki/Pegasus_Project_%28investigation%29
- 11/2021: Apple sued NSO following FORCEDENTRY exploit
- 01/2022: Israeli police caught spying Israeli citizens without warrants with Pegasus
- 10/2023: former head of the Spanish intelligence services charged with spying on the regional president of Catalonia with Pegasus
- 02/2024: Polish Watergate brought to Parliament: from 2015 to 2023, the conservative Law and Justice party (PiS) used Pegasus to spy on any opposition massively
- 03/2024: Court ordered maker of Pegasus spyware to hand over code to WhatsApp
- 09/2024: Apple drops lawsuit

Pegasus vs. Phantom

- NSO has blocked Pegasus to target US phone numbers deep in the code
- But many US agencies would like to use it
- NSO creates a subsidiary in the US (Westbridge)
- Westbridge gets an export licence from Israel to sell only to US gov agencies
- Phantom is just a rebrand of Pegasus with the restriction on US phone numbers lifted

NSO: a battle for power between US and Israel

In the US

- Testing the spyware for years, in the US (FBI, DOJ, DEA and many others) and abroad
- Had a protection embedded in the code so that it cannot target US numbers, no matter where they are
- Tried to take control of it either though funding or acquisition

In Israel

- Israel angry in part about U.S. hypocrisy: American ban came after years of testing Pegasus (FBI, DOJ, DEA and many others) + attempt to take control
- NSO is part of Israel security strategy and diplomacy with their export control
  - Mexico and Panama have shifted their positions in key votes at UN after acquiring Pegasus
  - Gained support of Arab nations leading to Abraham Accords (2020) or campaign against Iran

Ecosystem of offensive corps

Quarkslab

Economy of offensive corps: a great resource

- This list only concerns companies for which offensive activities are **publicly proven**.
  - There are many more.
  - China (i-Soon <3) & Russia under-represented -> because of the government's control over the subject?
  - Where is Inida?

- Total=171 firms, 22 have stopped practicing => 149 remaining

xorl %eax, %eax

Offensive Security Private Companies Inventory

This is a collection of any publicly known private companies who have been involved in nation-state offensive cyber operations. Most of them have been involved by providing capabilities such as software implants and intrusion sets (e.g. 0day exploits, exploitation frameworks, security bypassing techniques, communications interception products, etc.) If you noticed any private company that is publicly known for such activities and is not listed below, please let me know to update it accordingly.

Disclaimer: This is not about leaking any sensitive or confidential information, just aggregating what is already publicly available for this space. This is why all entries have an OSINT reference that already mentions this private entity as involved with this business. Also, the reason why you will not see any of the dozens of private companies that aren't publicly known listed here.

A ChangeLog is available at the end of this page. The entries are listed in alphabetic order (based on the company's name).

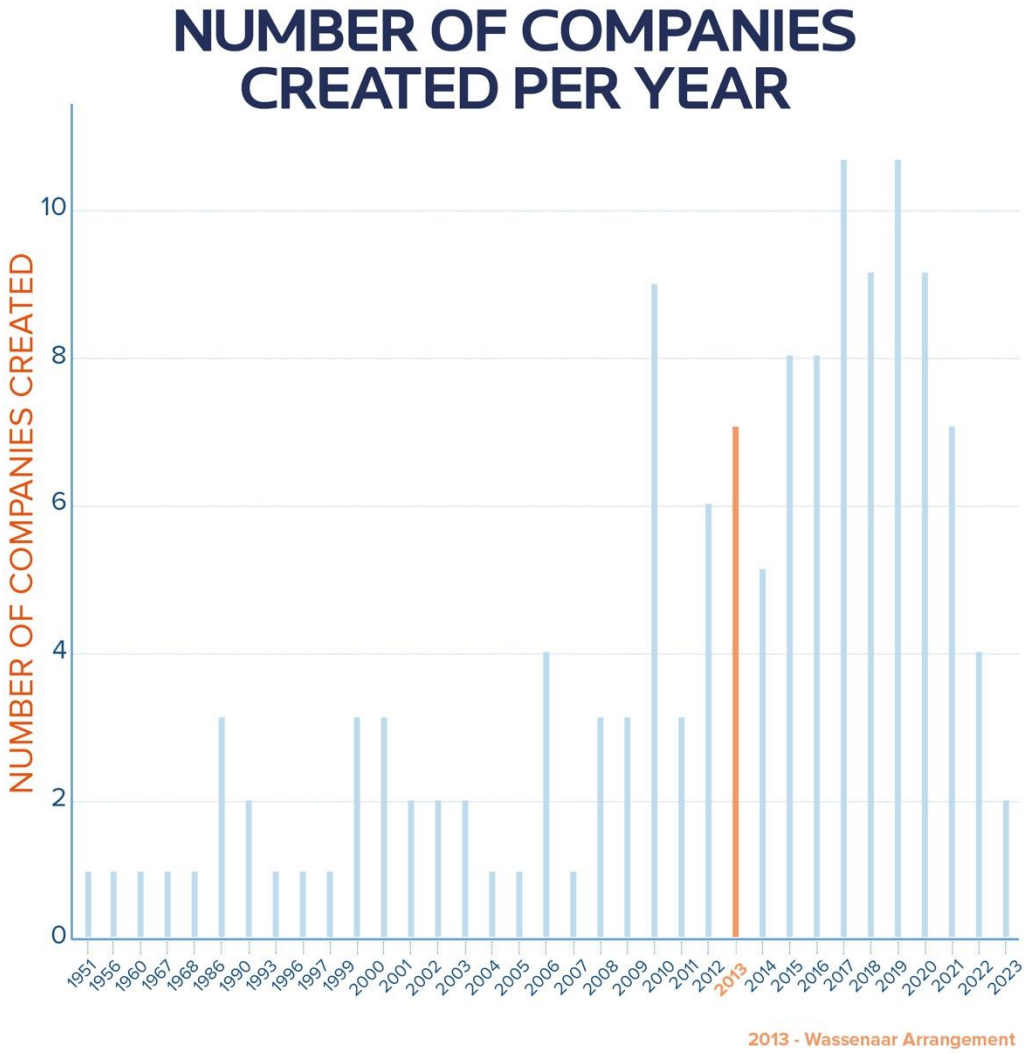
Last update: *22 February 2024*

Name	Country	Founded	Status	OSINT Reference
Ability	Israel	-	-	WikiLeaks
ACE Labs	Israel	2016	Active	Calcalist
Accuvant	USA	2002	Merged (with Optiv)	TechnologyReview
AFB Systems	UAE	2021	Active	IntelligenceOne
Advanced Impact Media Solutions	Israel	2018	Active	The Guardian
Altrnativ	France	2020	Active	Politico
Aliada Group Inc.	Israel	2017	Active	CitizenLab
Amesys	France	2008	Ceased (succeeded by Nexa Tech)	WikiLeaks
Andreas Fink	Switzerland	-	Active	Haaretz
Anomaly Six	USA	2018	Active	The Intercept

https://xorl.wordpress.com/offensive-security-private-companies-inventory/

Economy of offensive corps: geography

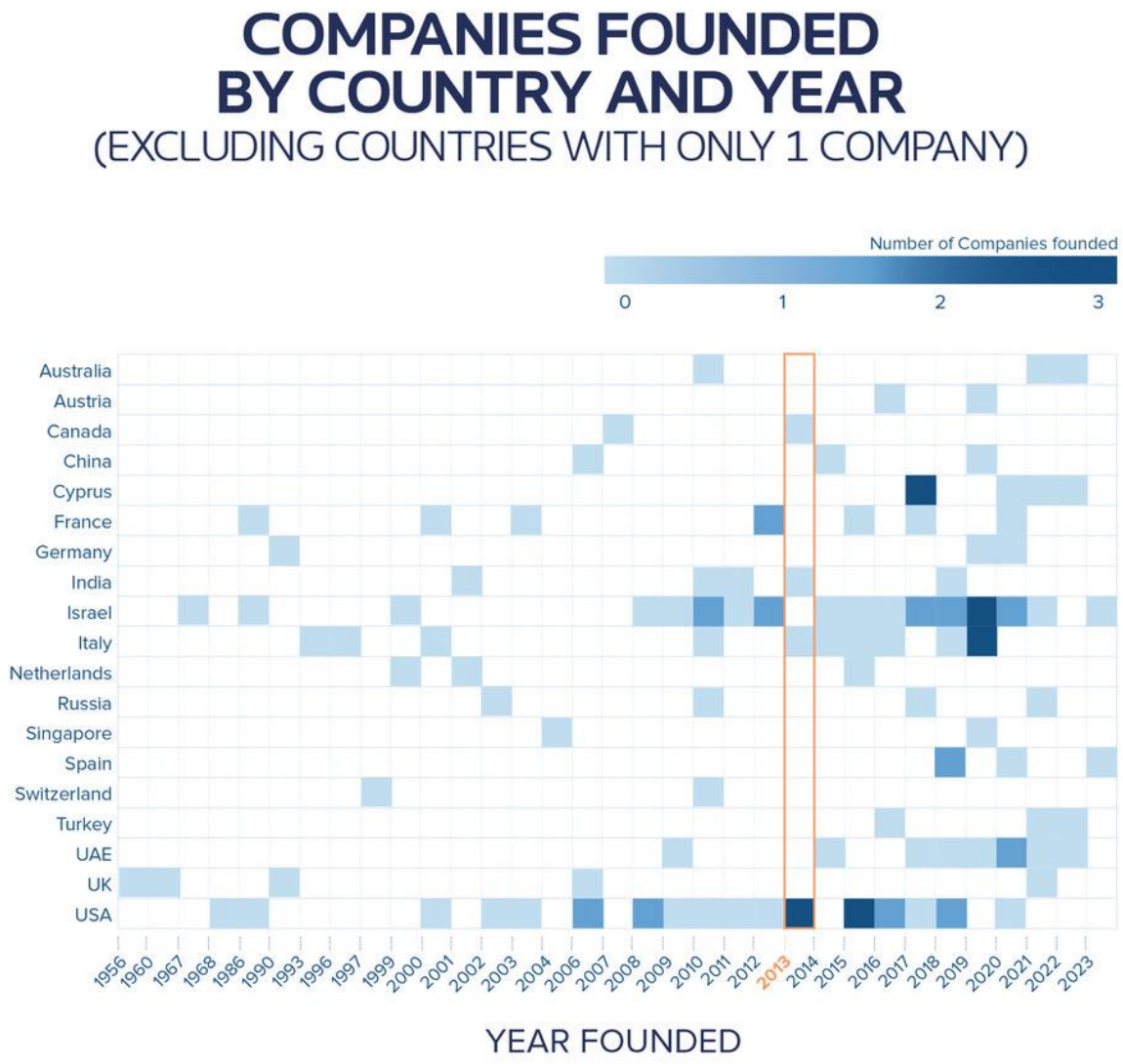
Economy of offensive corps: temporality



Economy of offensive corps: heatmap

- 13 countries have only 1 company, out of 32 in total
- From 2008, the USA and Israel have a regularly active private sector
- Italy was active between 2010 and 2019, nothing revealed since then
- the United Arab Emirates have been very active since 2016
- 5 of the 8 French boxes are created from 2012

- Median year: 2014
- Wassenaar: end of 2013

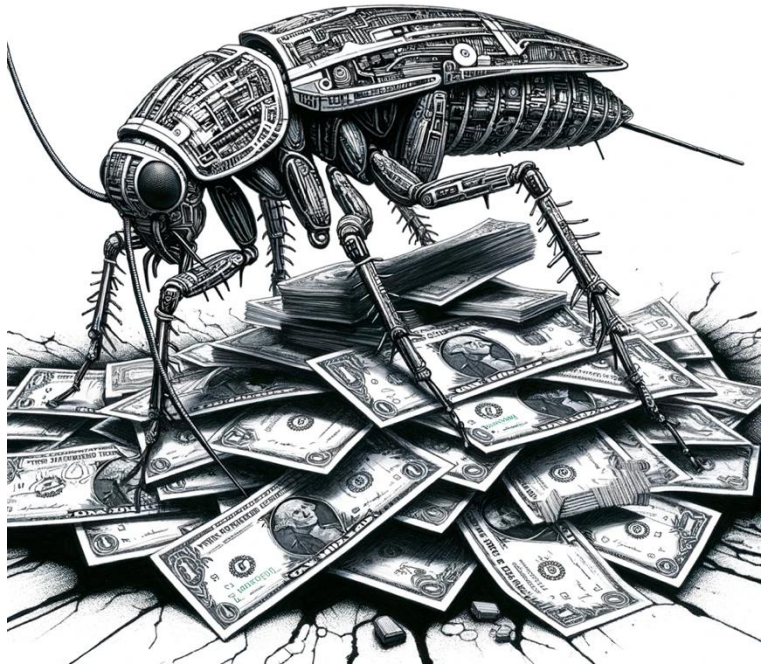


Economy of offensive corps

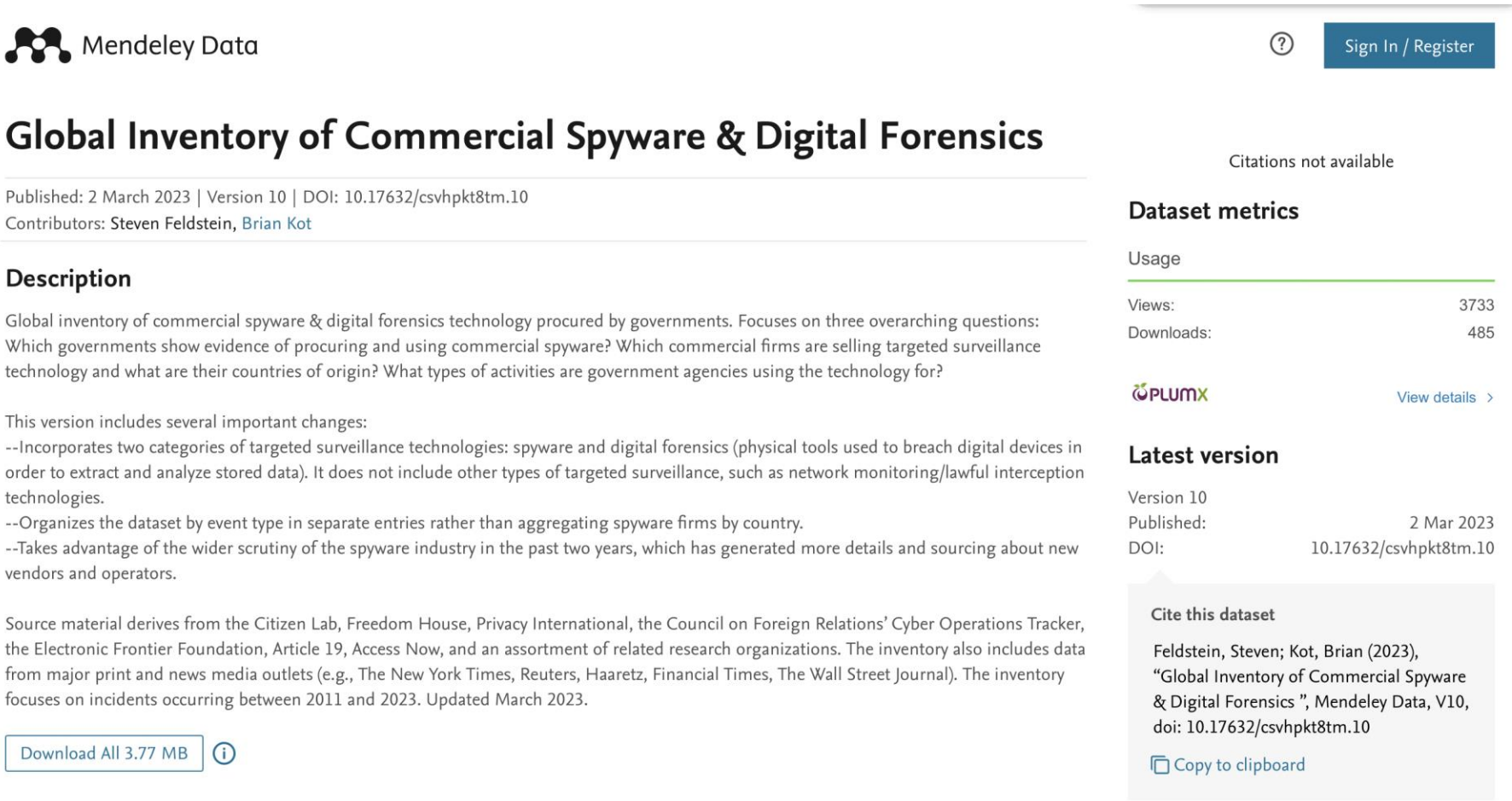
What's the conclusion to be drawn ?
There is a high demand, particularly from countries that do not have the internal capacity.
The Arab Spring (2010-11) and the fear created among certain heads of state are undoubtedly not unrelated.

So an offer was created.

“Fun” Fact
Between 2014 and 2023**, 35/72 (49%) of 0-days targeting Google products** are directly attributed to some of these private firms.



Another source



Mendeley Data

Sign In / Register

Global Inventory of Commercial Spyware & Digital Forensics

Published: 2 March 2023 | Version 10 | DOI: 10.17632/csvhpkt8tm.10
Contributors: Steven Feldstein, Brian Kot

Description

Global inventory of commercial spyware & digital forensics technology procured by governments. Focuses on three overarching questions: Which governments show evidence of procuring and using commercial spyware? Which commercial firms are selling targeted surveillance technology and what are their countries of origin? What types of activities are government agencies using the technology for?

This version includes several important changes:
--Incorporates two categories of targeted surveillance technologies: spyware and digital forensics (physical tools used to breach digital devices in order to extract and analyze stored data). It does not include other types of targeted surveillance, such as network monitoring/lawful interception technologies.
--Organizes the dataset by event type in separate entries rather than aggregating spyware firms by country.
--Takes advantage of the wider scrutiny of the spyware industry in the past two years, which has generated more details and sourcing about new vendors and operators.

Source material derives from the Citizen Lab, Freedom House, Privacy International, the Council on Foreign Relations' Cyber Operations Tracker, the Electronic Frontier Foundation, Article 19, Access Now, and an assortment of related research organizations. The inventory also includes data from major print and news media outlets (e.g., The New York Times, Reuters, Haaretz, Financial Times, The Wall Street Journal). The inventory focuses on incidents occurring between 2011 and 2023. Updated March 2023.

Download All 3.77 MB

Citations not available

Dataset metrics

Usage

Views:	3733
Downloads:	485

PLUMX View details >

Latest version

Version 10	
Published:	2 Mar 2023
DOI:	10.17632/csvhpkt8tm.10

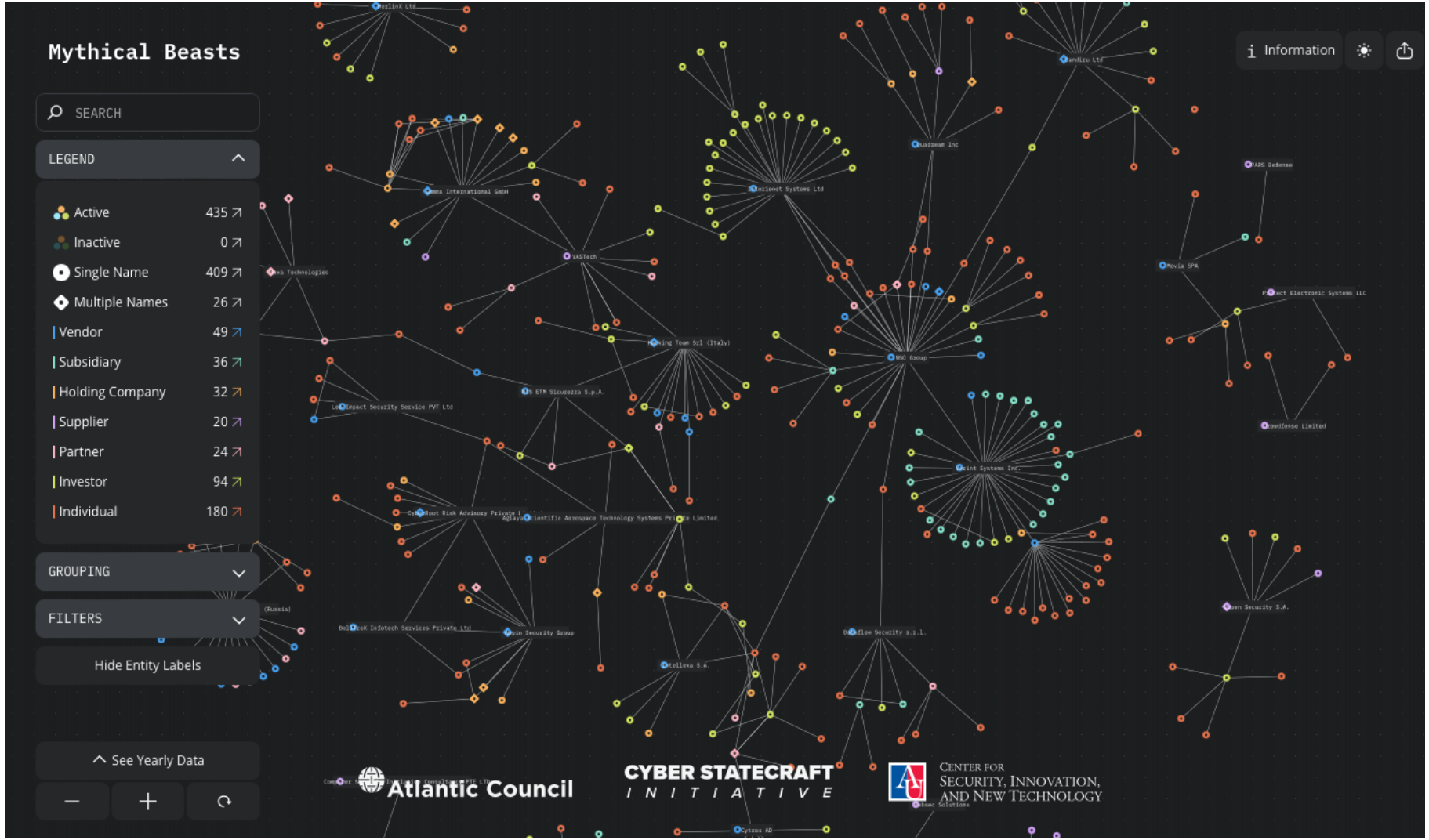
Cite this dataset

Feldstein, Steven; Kot, Brian (2023), "Global Inventory of Commercial Spyware & Digital Forensics ", Mendeley Data, V10, doi: 10.17632/csvhpkt8tm.10

Copy to clipboard

https://data.mendeley.com/datasets/csvhpkt8tm/10

And another one



https://dfrlab.org/2024/09/04/mythical-beasts-and-where-to-find-them-report/#executive-summary

ISS World: the surveillance business

Tracks

1: Lawful Interception and Criminal Investigation
2: LEA, Defense and Intelligence Analyst
3: Social Network Monitoring, Artificial Intelligence and Analytics
4: Threat Intelligence Gathering and Cyber Security
5: Investigating DarkWeb, Bitcoin, Altcoin and Blockchain Transaction
6: Mobile Signal Intercept
7: Electronic Surveillance
8: 5G Lawful Intercept, Tracking and Forensics

Resilience

Quarkslab

How to tackle spycorps?

A cockroach survives a level of radiation that would kill a man.
He survives longer than us after decapitation.

The people who set up these companies understood that public opinion and certain governments were not favorable to them.

As wise entrepreneurs, they have developed the resilience of their companies to deal with crises, such as having customer or internal data exposed.

4 main axis

- Customers
- Legal
- Regulation
- Tech

Customers

There will always be governments ready to pay to monitor “terrorists” (variable geometry definition)

=>

Unlikely to dry up revenues

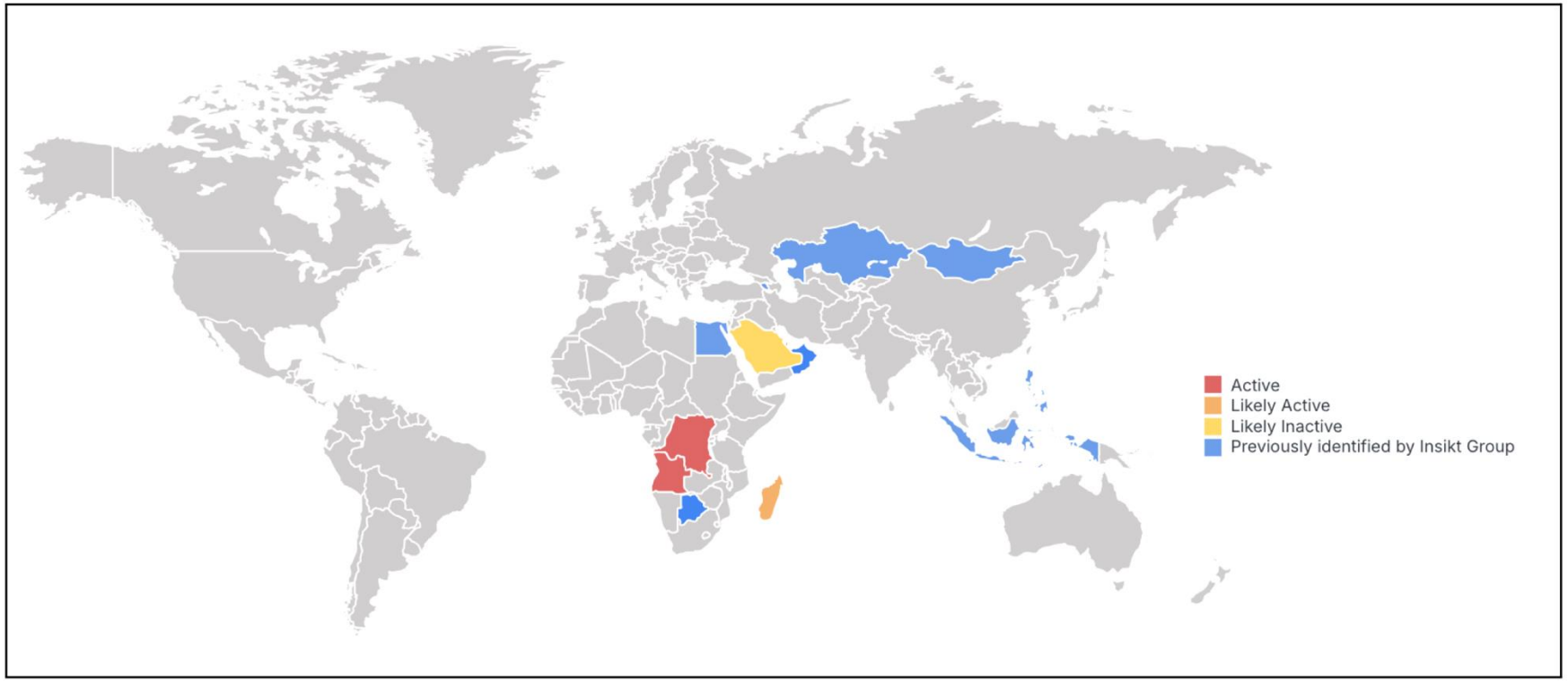


Figure 3: *Countries with suspected Predator customers (Source: Recorded Future)*

https://www.recordedfuture.com/research/predator-spyware-infrastructure-returns-following-exposure-sanctions

Legal

- The **FinFisher** / Gamma Group history has been exposed: its internal data (40Gb, price list, source code, price, etc.) leaked following the compromise by a certain Phineas Fisher in 2014.

  In 2021, the company declared itself insolvent. This would involve a rebranding towards Vilicius Holding GmbH which would continue the same activities(?)

- The enigmatic **Candiru** (Israel, 2014) has changed names at least 8 since its creation!

Paper trail difficult to follow when it is easy to incoroporate a new company or a subsidiary

Bonus: All spycorps are sued, but continue to operate.

PRESS RELEASE

November 23, 2021

Apple sues NSO Group to curb the abuse of state-sponsored spyware

Apple also announced a $10 million contribution to support cybersurveillance researchers and advocates

Regulation

Israel News | National Security & Cyber

Israeli Spy Tech Sold to Bangladesh, Despite Dismal Human Rights Record

Advanced cyber tools to intercept mobile and internet traffic were sold to the Interior Ministry, internal security agency and armed forces, via Cyprus. Israel and Bangladesh do not have diplomatic relations

Save Zen Read

Oded Yaron and Zulkarnain Saer Khan

Jan 10, 2023

Advanced surveillance equipment, developed by a company controlled by the former commander of Israeli intelligence's technology unit, was sold last year to the government of Bangladesh, official government documents and international export records show, despite Bangladesh not being on Israel's list of countries that such technology may be sold to – and despite its consistently poor human rights record

- Surveillance software has been subject to the **Wassenaar Arrangement** since 2013.
  - Only 42 states have ratified this agreement.

- Being in the agreement does not mean that there will be no export, but that it is subject to government approval.
  - USA US negotiated a "research exception" in Dec. 17
  - Israel IL is not in the agreement and has its own system of authorizations, governed by its national security and diplomacy.
  - China CN is not in the agreement: they control and use cyber
  - Russia RU is a member, but not Belarus BY.

- A new initiative, **Pall Mall Process**, has just been launched in March 2024.
  - Mix of government, companies and NGOs

Tech

Pegasus, NSO's spyware, and its infrastructure have been exposed several times.
Predator, Cytrox's spyware, and its infrastructure have been exposed several times.

In the age of DevOps, putting together an infrastructure is far from insurmountable:

- Register domain names
- Rent VPS here and there
- Push exploit servers here
- Push data collection servers

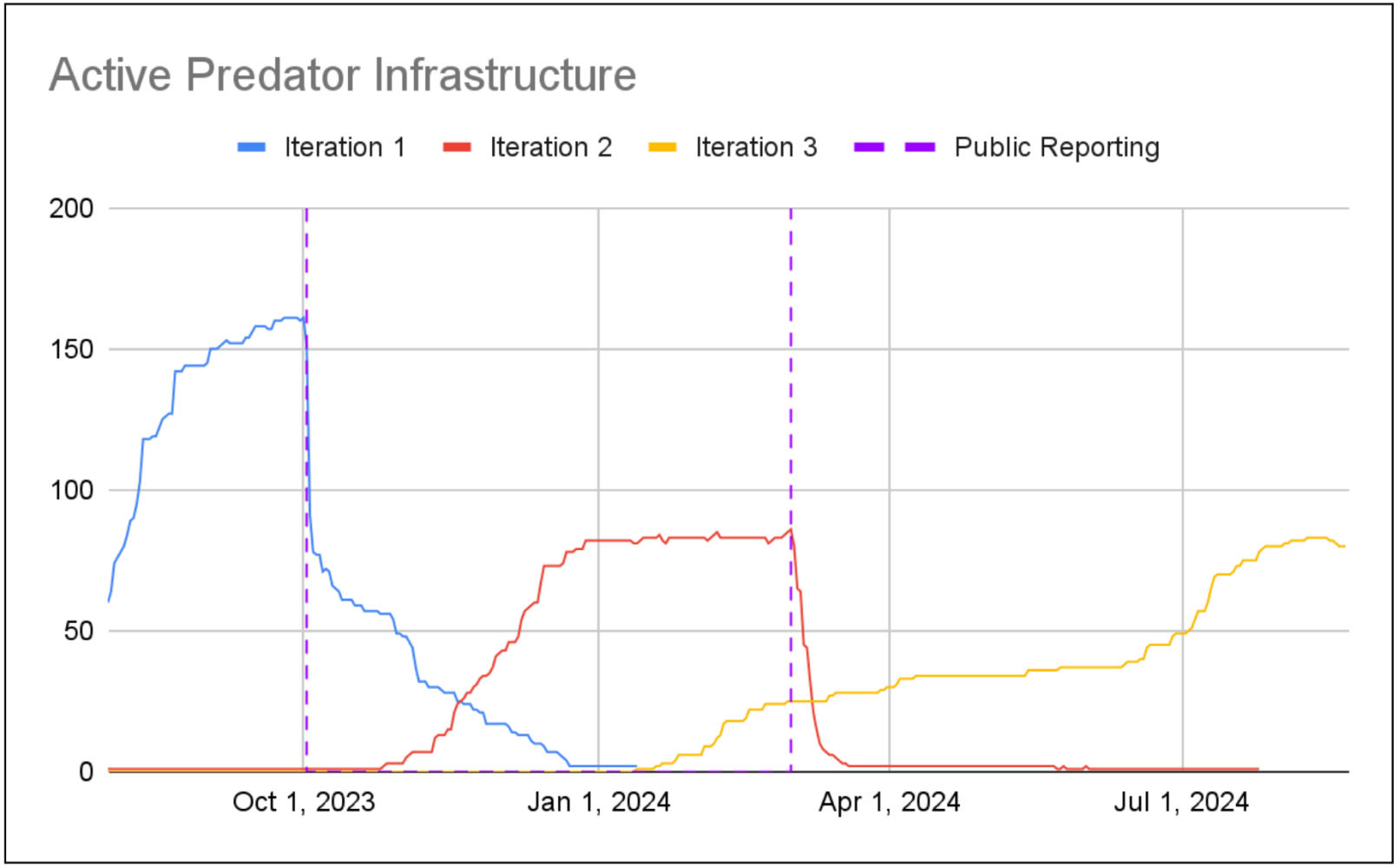
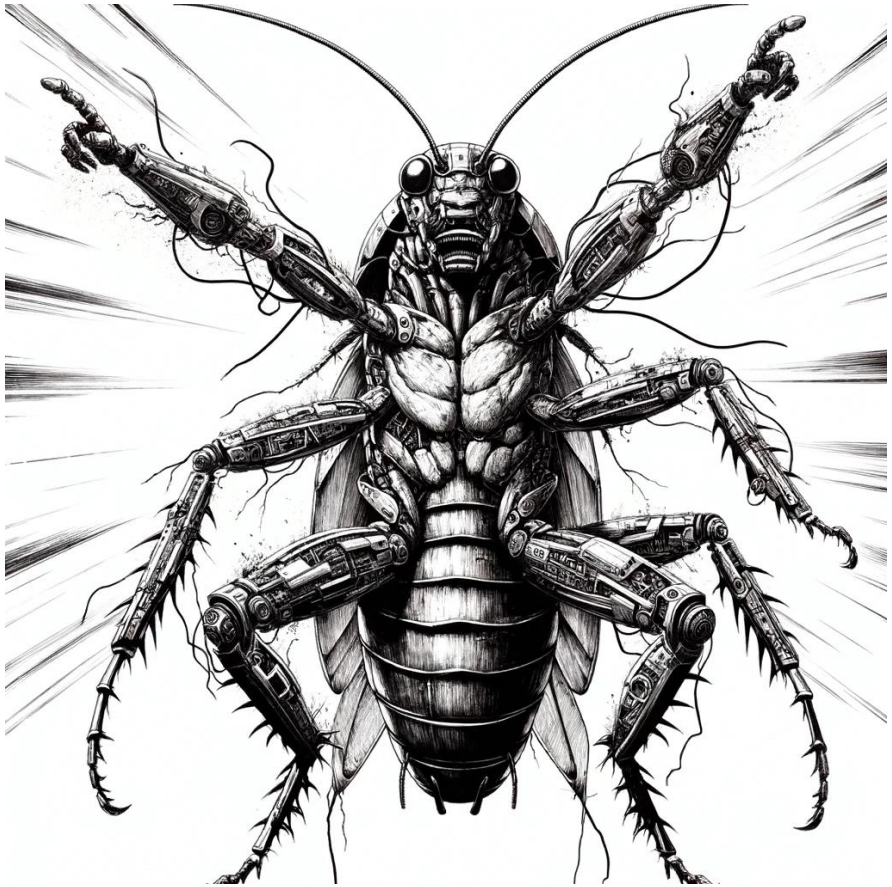


Figure 1: *Active Predator infrastructure before and after public reporting (Source: Recorded Future)*

https://www.recordedfuture.com/research/predator-spyware-infrastructure-returns-following-exposure-sanctions

Spycorps are like cockroaches?



Why are they so resistant?

- Customers will exist for a long time,
- Cyber has become an integral part of state diplomacy, pushing regulation to the background
- progress facilitates legal or technological ”rebirth”

Latest fun (or not) news

Quarkslab

Russia APT29 used spyware's exploits

- APT29 / CoztBear (RU) used exploits very similar to those of spyware vendors
- Involved vendors:
  - NSO Group (Pegasus)
  - Intellexa (Predator)
- Targeted exploits:
  - CVE-2023-41993 (WebKit/iOS) - identical to Intellexa's
  - CVE-2024-5274 (Chrome/Android) - very similar to NSO Group's
  - CVE-2024-4671 (Chrome/Android) - resembles previous Intellexa exploits
- Uncertainty about how APT29 obtained these exploits
- Raises concerns about the proliferation of exploits developed by the commercial surveillance industry

- NSO Group denied selling its products to Russia

https://www.metacurity.com/russias-apt-29-hackers-used-spyware-vendors-exploits/?

Russia APT29 used spyware’s exploits

- **Obscured Ownership**: complex structure using offshore registrations to evade scrutiny
- **Exploiting Legal Loopholes**: based in North Macedonia allowing easy export of spyware
- **Shifting Jurisdictions**: changes locations across countries to avoid legal scrutiny
- **Nominee Directors (💔)**: Cytrox's director was a Czech 70 y.o. pensioner unaware of her role

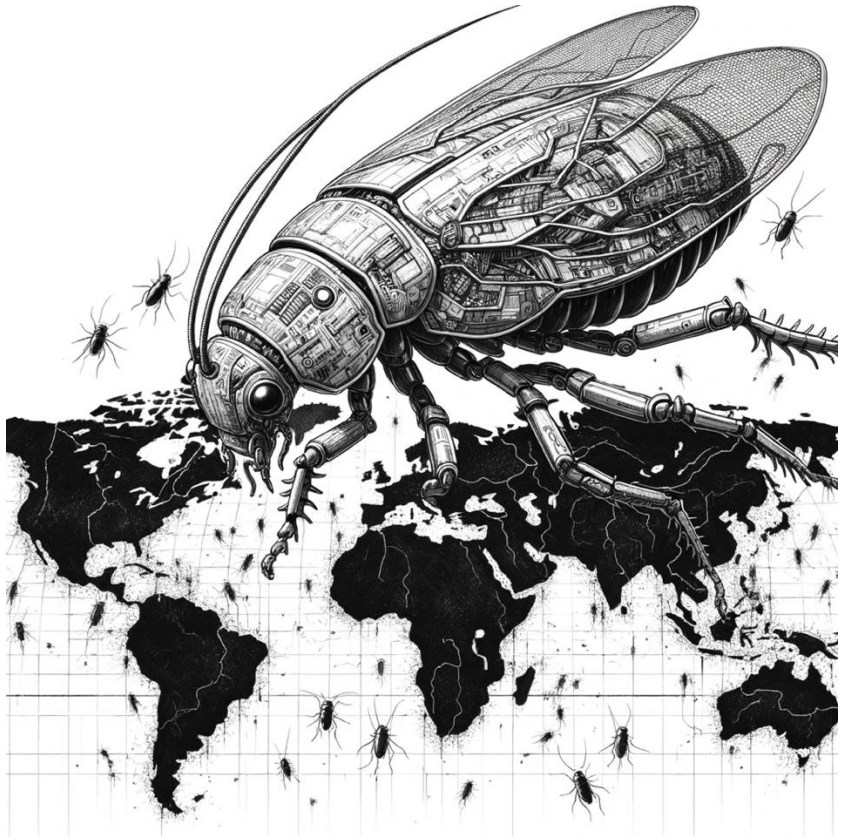
Intellexa Co-CEO Tal Dilian

https://vsquare.org/predator-cytrox-czech-republic-poland-spyware-israel/

Conclusion

Quarkslab

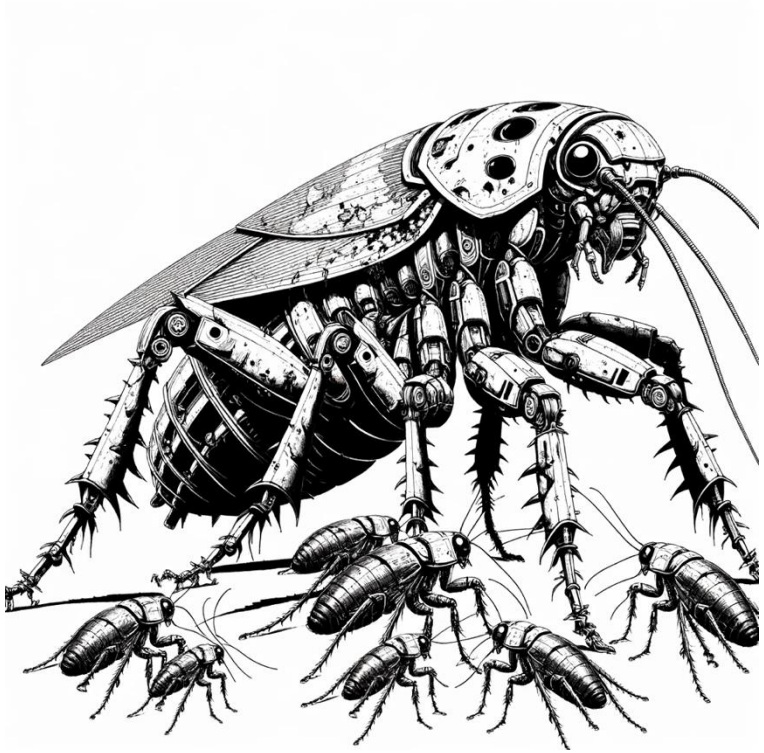
Cyberweapons: a business as usual … for influence



Cyberweapons are now seen as **regular military hardware** (fighter jets, centrifuges…): not only as pivotal to national defense but also as a currency with which to buy influence around the world

Political economy of the spyware market

- **Demand is extremely high** => even when a supplier sanctioned, financial motivation for others to fill in the gap
  - Old suppliers (FinFisher, Hacking team) replaced by new ones (NSO, Cytrox, Candiru)
  - Even if top-tier firms were shut down, there are enough boutique firms & hacker-for-hire to replace



Best practice for defense

- **Regular software update**: kills vuln used by spyware, making it harder to reactivate
- **Device reboot**: can block temporarily the spyware until reactivation
- **Lockdown mode**: block unauthorized access and exploitation attempts
- **Mobile Device Management (MDM)**: enforce security protocols in employee devices
- **Security Awareness Training**: learn to identify spear phishing and other social engineering tactics

OUR CONSULTING

- PENTEST
- CRYPTOGRAPHY
- SECURITY DEVLOPMENT
- REVERSE ENGINEERING
- VULNERABILITY RESEARCH

OUR PRODUCTS

- SENSITIVE ASSETS IN-APP PROTECTION
- SCALABLE THREAT DETECTION PLATFORM

MERCI ☺

Rendez-vous stand K33

(niveau Ravel)

Fred Raynal
fraynal@quarkslab.com

Quarkslab