Spyware For Rent &
The World of Offensive Cyber

Off by One

Fred Raynal
fraynal@quarkslab.com

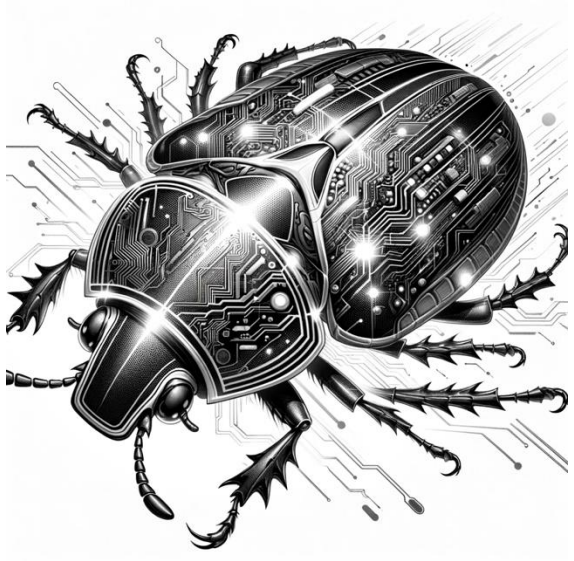
OFF-BY-ONE
2025

Quarkslab

What is spyware?

Quarkslab

Spyware?



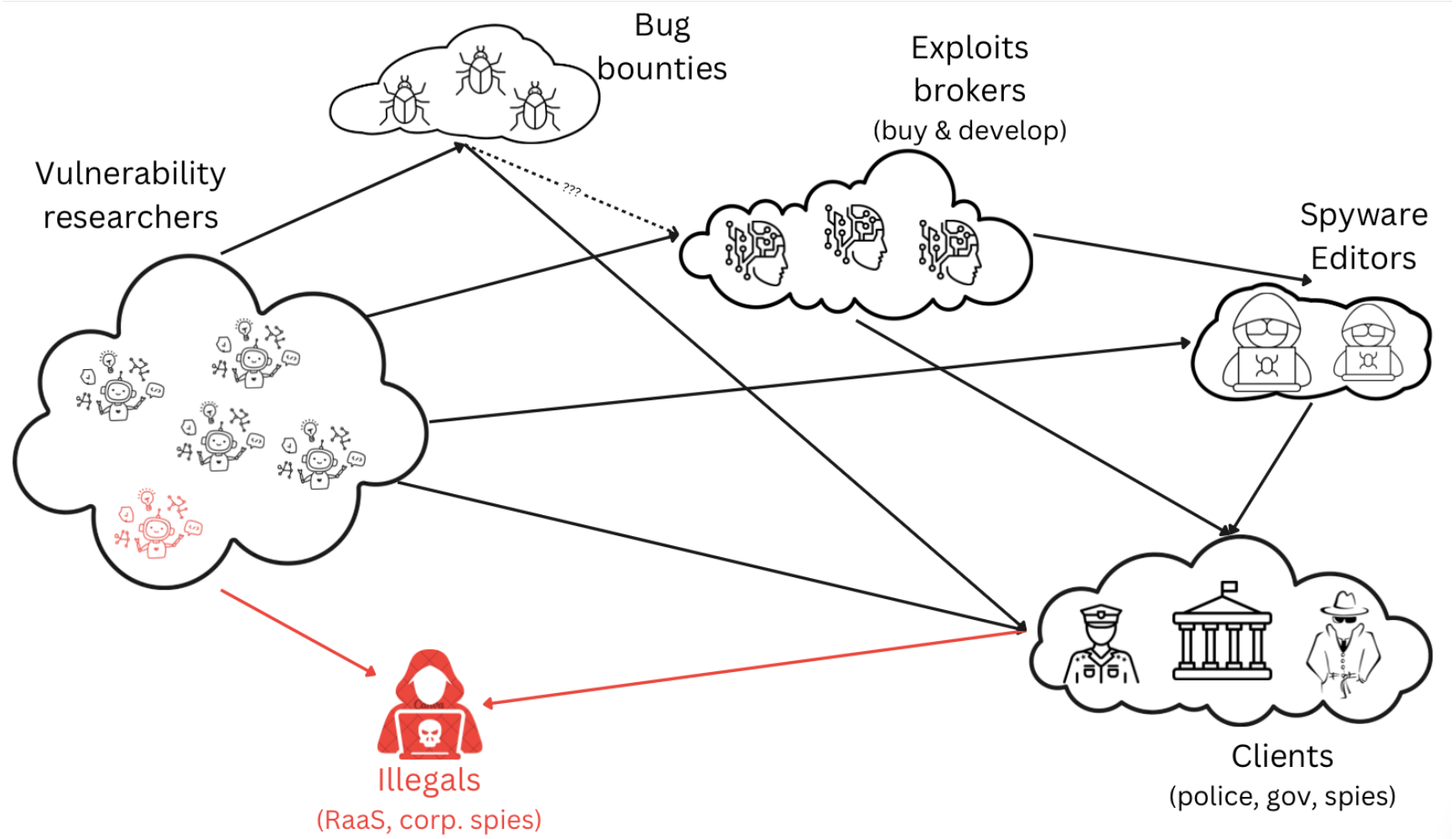
A software that enables a user to obtain covert information about another's computer activities by transmitting data covertly from their system.

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

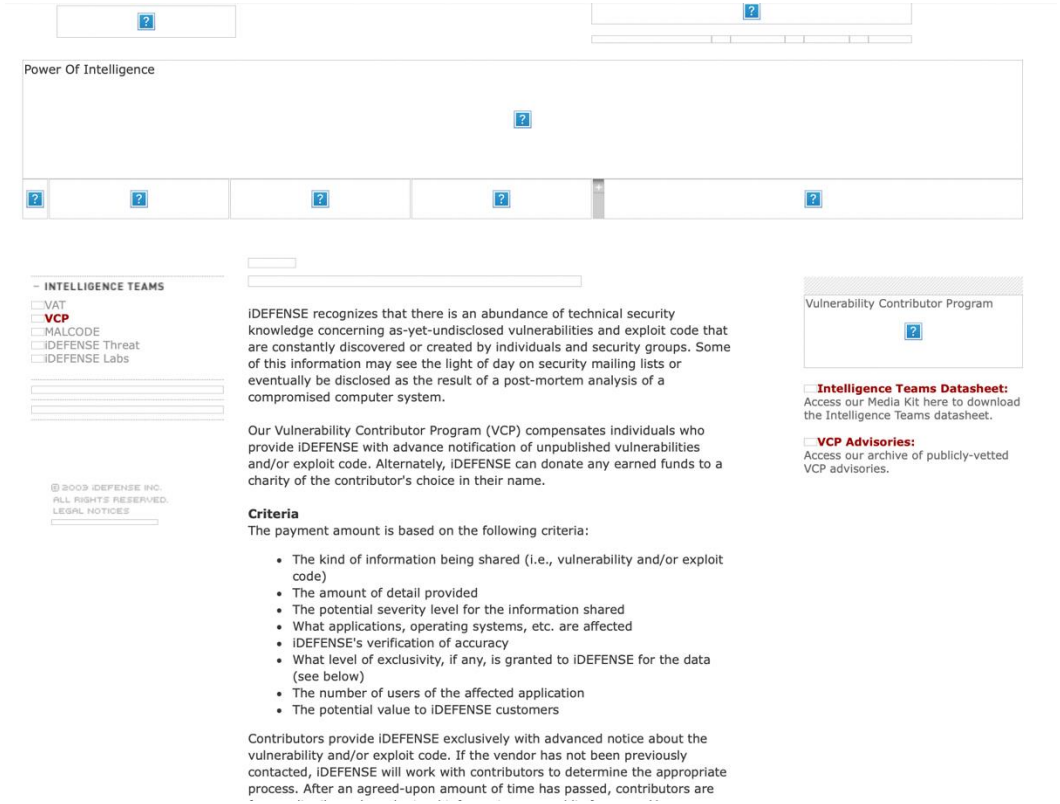
Targets

- **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)



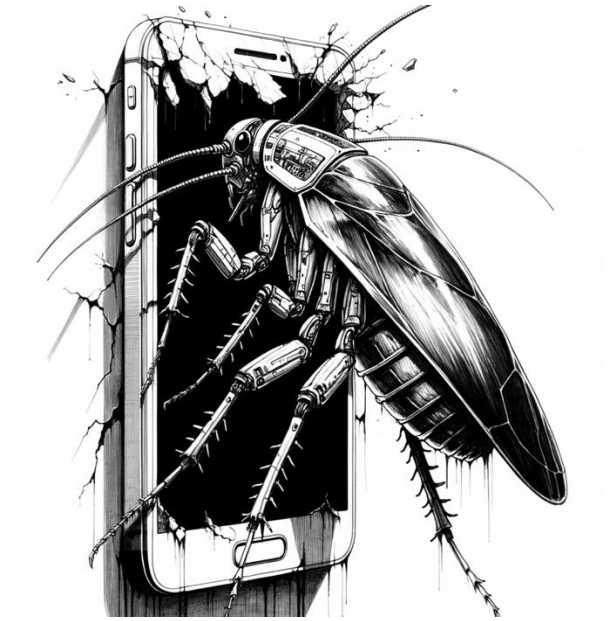
How does payment work?
I am a regular contributor. Is it possible to get a base salary and/or add to it like a bonus plan for each vulnerability report I send in?

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

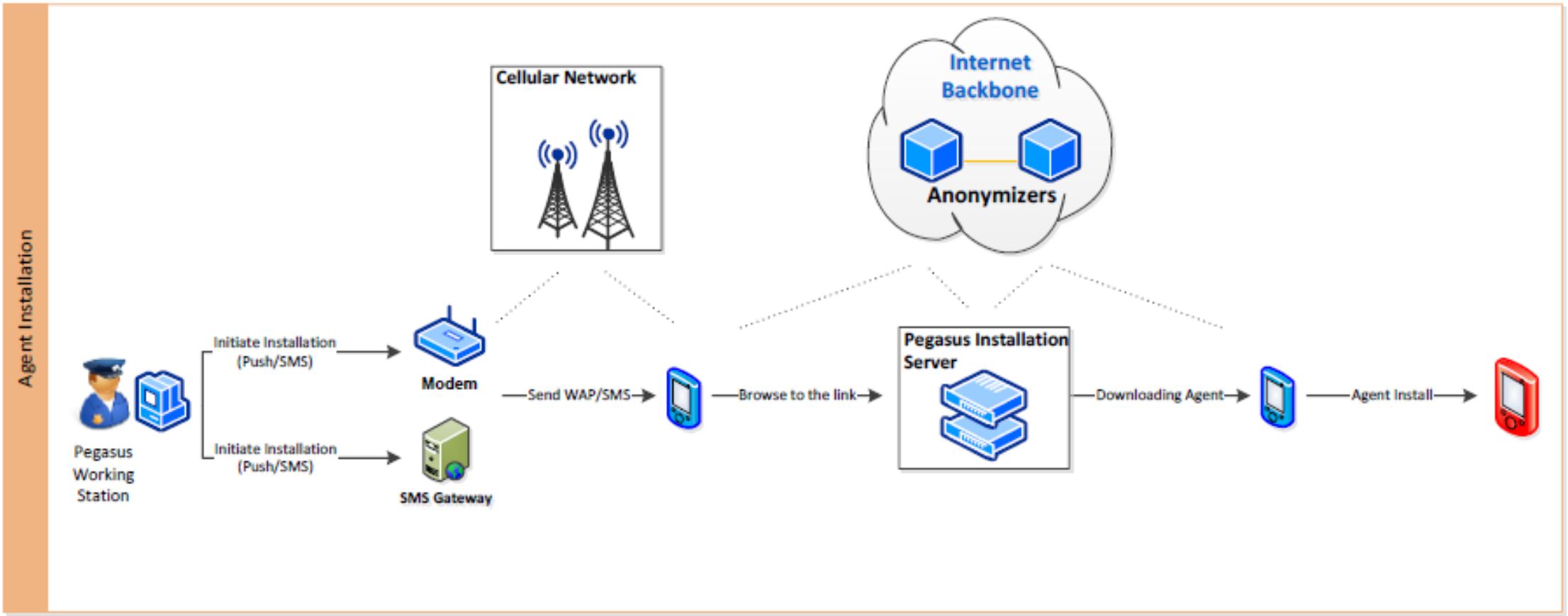
“Fun” Fact
Between 2014 and 2023**, 35/72 (49%) of 0-days targeting Google products** are directly attributed to some of the spycorps.

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

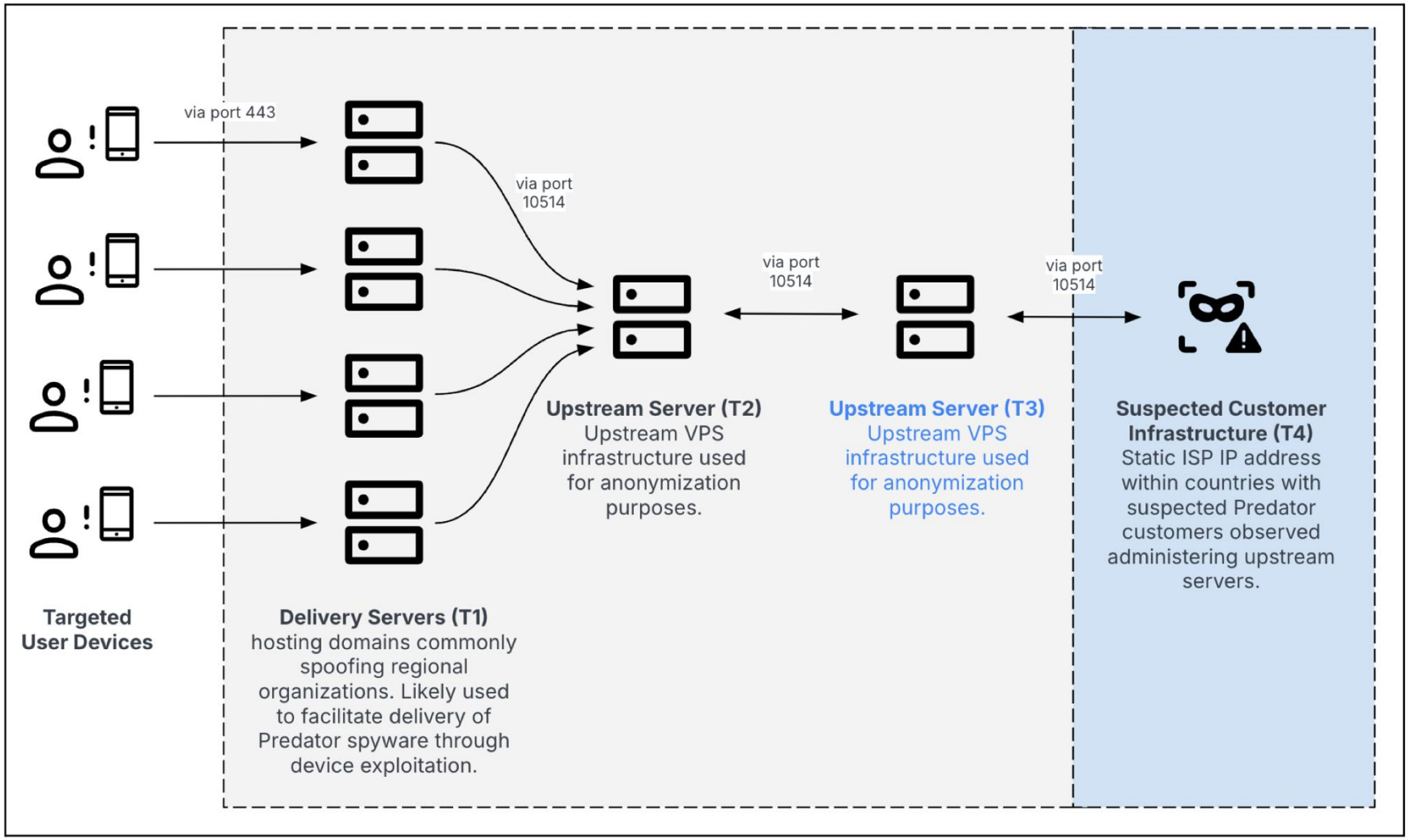


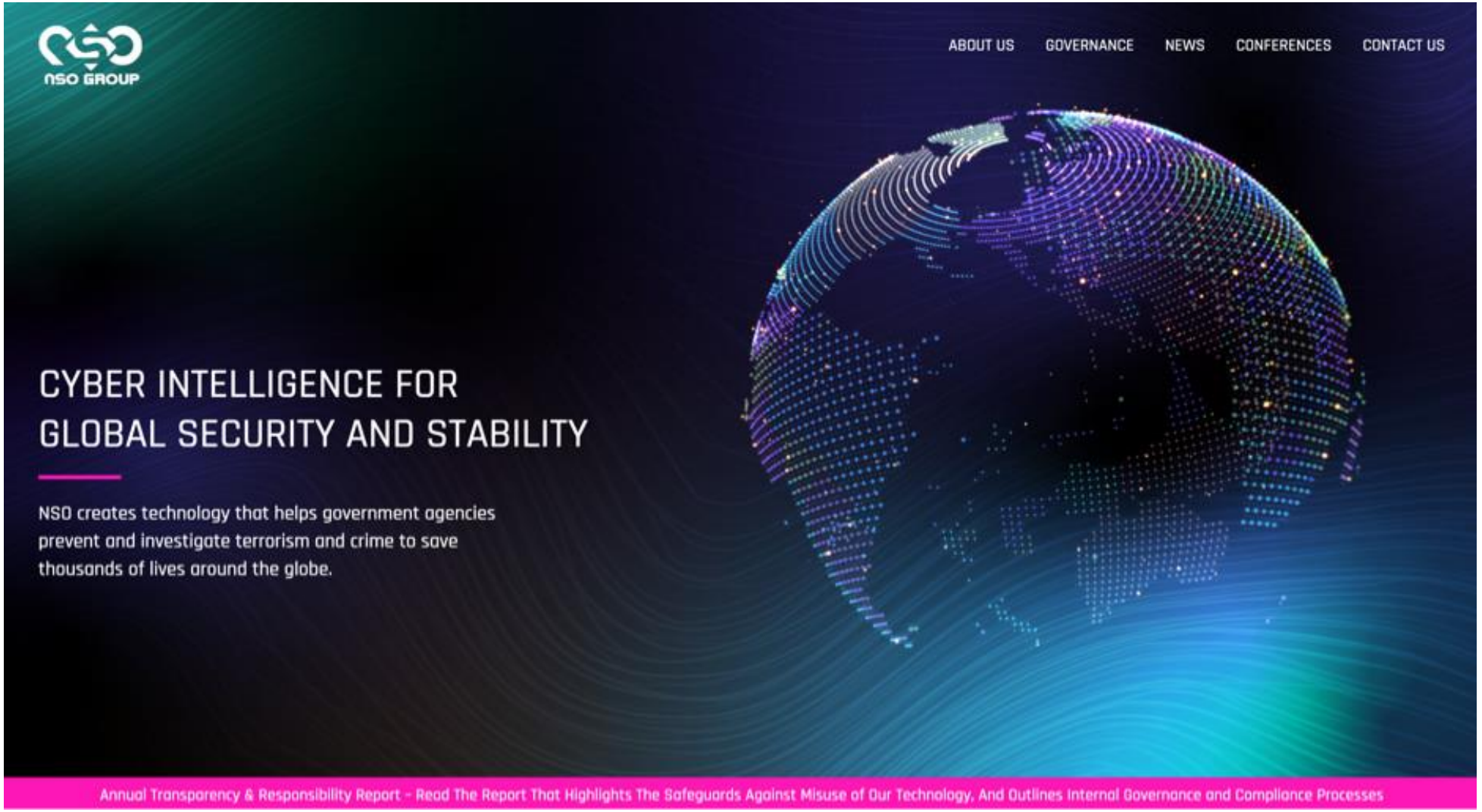
Figure 2: *Multi-tiered Predator infrastructure with additional tier (Source: Recorded Future)*

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

Marketing

Quarkslab

Marketing: NSO



Marketing: Intellexa

About us

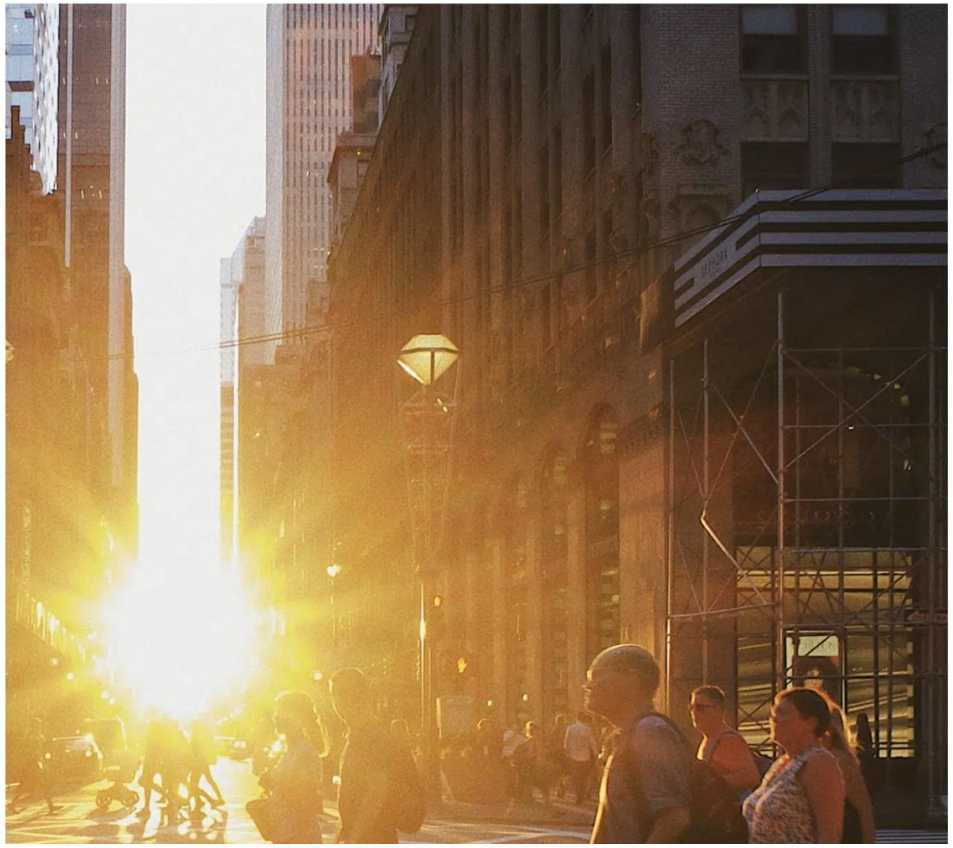
001 / CORPORATE

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

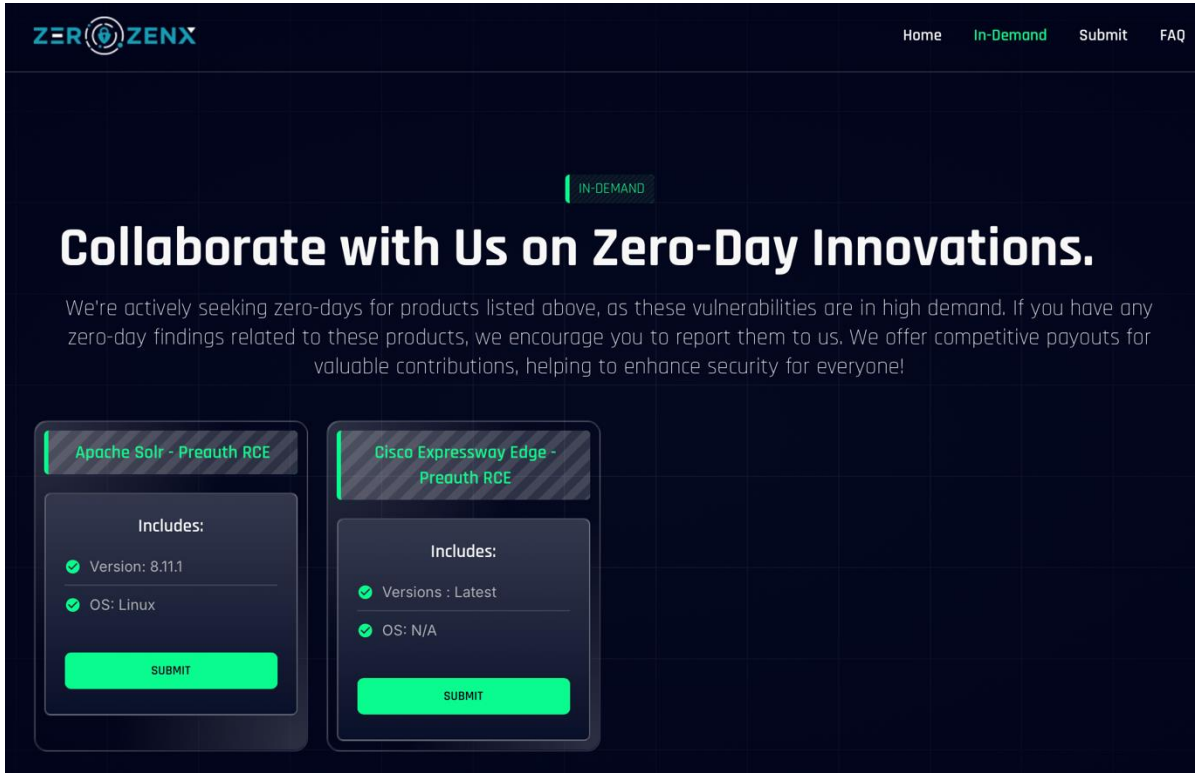
#	Item	Description	Qty.	Price (EURO)
1	Year 2 Optional Maintenance Contract	Optional maintenance contract for the second year including all services and SLA of the Warranty year.	1	30% of Contract (Per Year)
2	NOVA Persistency	Reboot-Persistency • Support for iOS & Android • Agent will survive phone 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

Rise of offensive corps

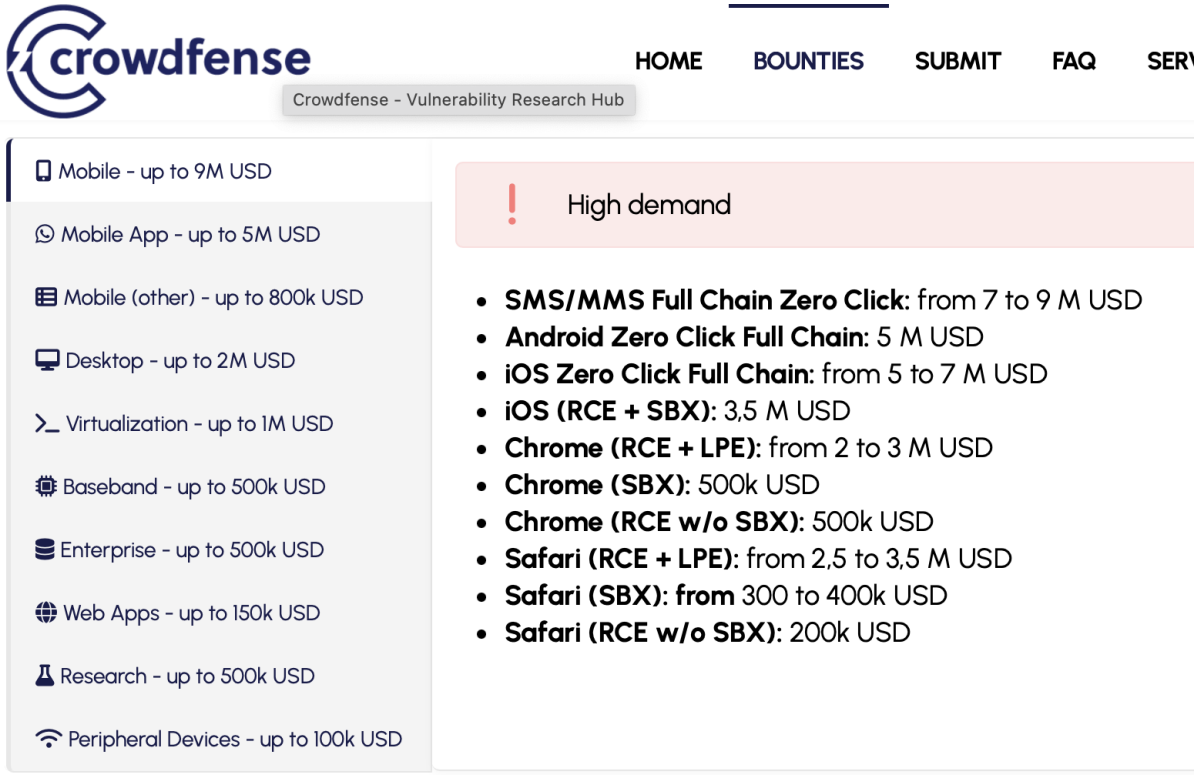
Quarkslab

Zerodium is dead, long live CrowdFense, ZeroZenX, Vuln Security…

UAE, the (new again) 0-day place to be…



Russia



Italy (?)

Economy of offensive corps: a great resource

- This list only concerns companies for which offensive activities are **publicly proven:**
  - 136 active
  - 29 unique countries

But there are many more.

- China (i-Soon <3) & Russia under-represented -> because of the government's control over the subject?
- Not so much on India whereas Appin and next gen companies?

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.

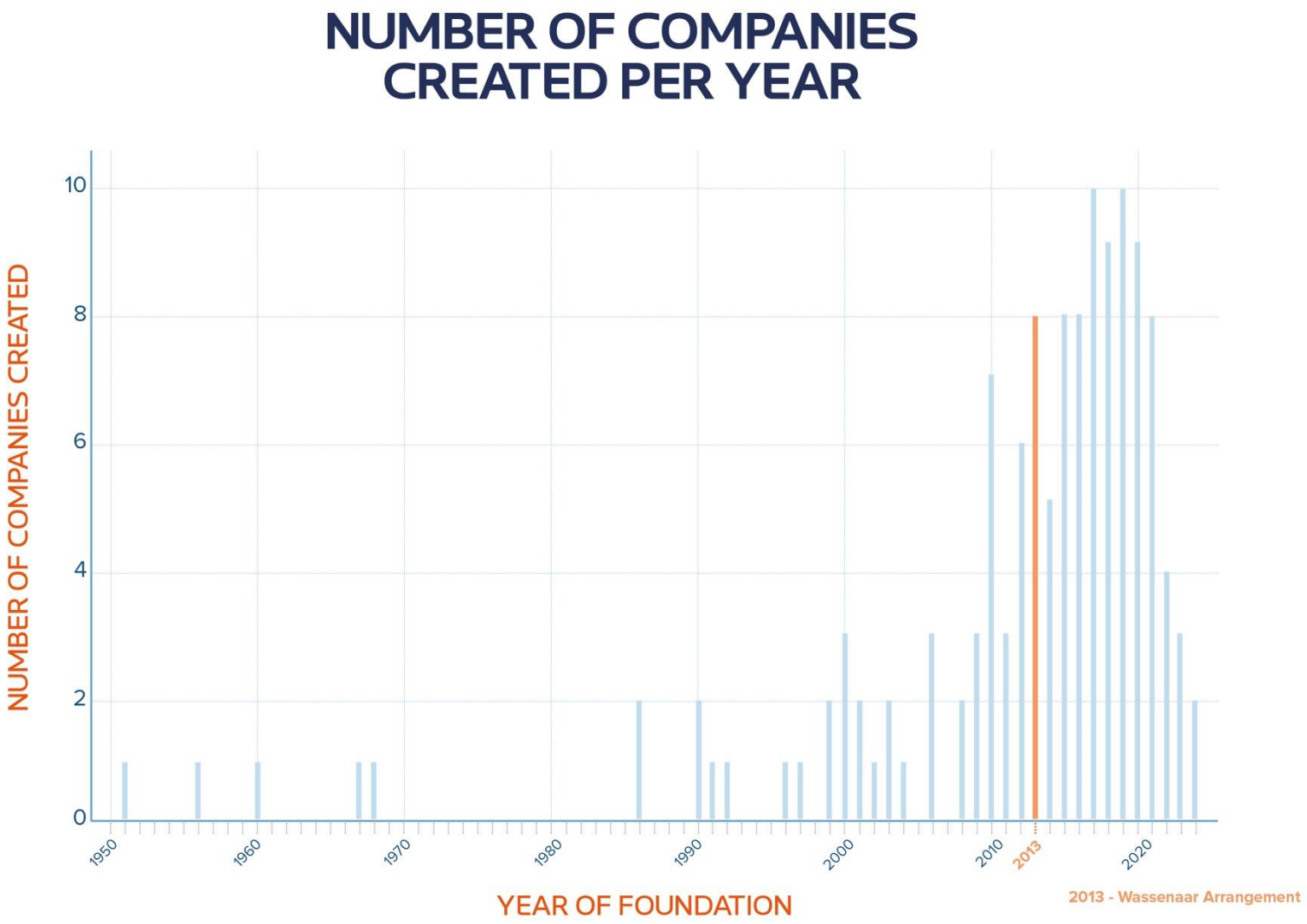
A ChangeLog is available at the end of this page. The entries are listed in alphabetic order (based on the company's name).

Last update: *19 February 2025*

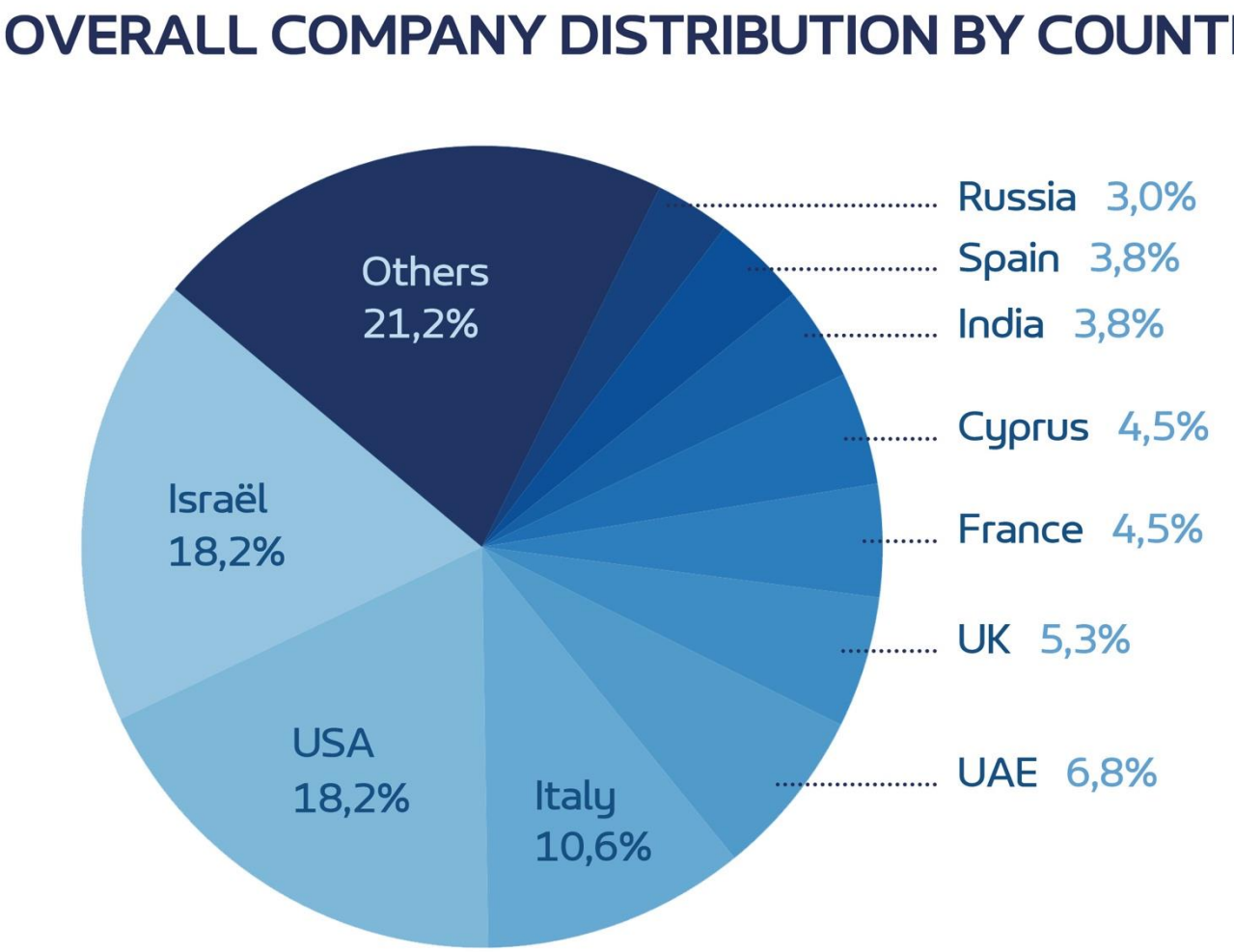
Name	Country	Founded	Status	OSINT Reference
Ability	Israel	-	-	WikiLeaks
ACE Labs	Israel	2016	Active	Calcalist
Accuvant	USA	2002	Merged (with Optiv)	TechnologyReview
AFB Systems	UAE	2021	Active	IntelligenceOne
Advanced Impact Media Solutions	Israel	2018	Active	The Guardian
Alpheratz CIA	Ecuador	2013	Active	IntelligenceOnline
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

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

Economy of offensive corps: temporality



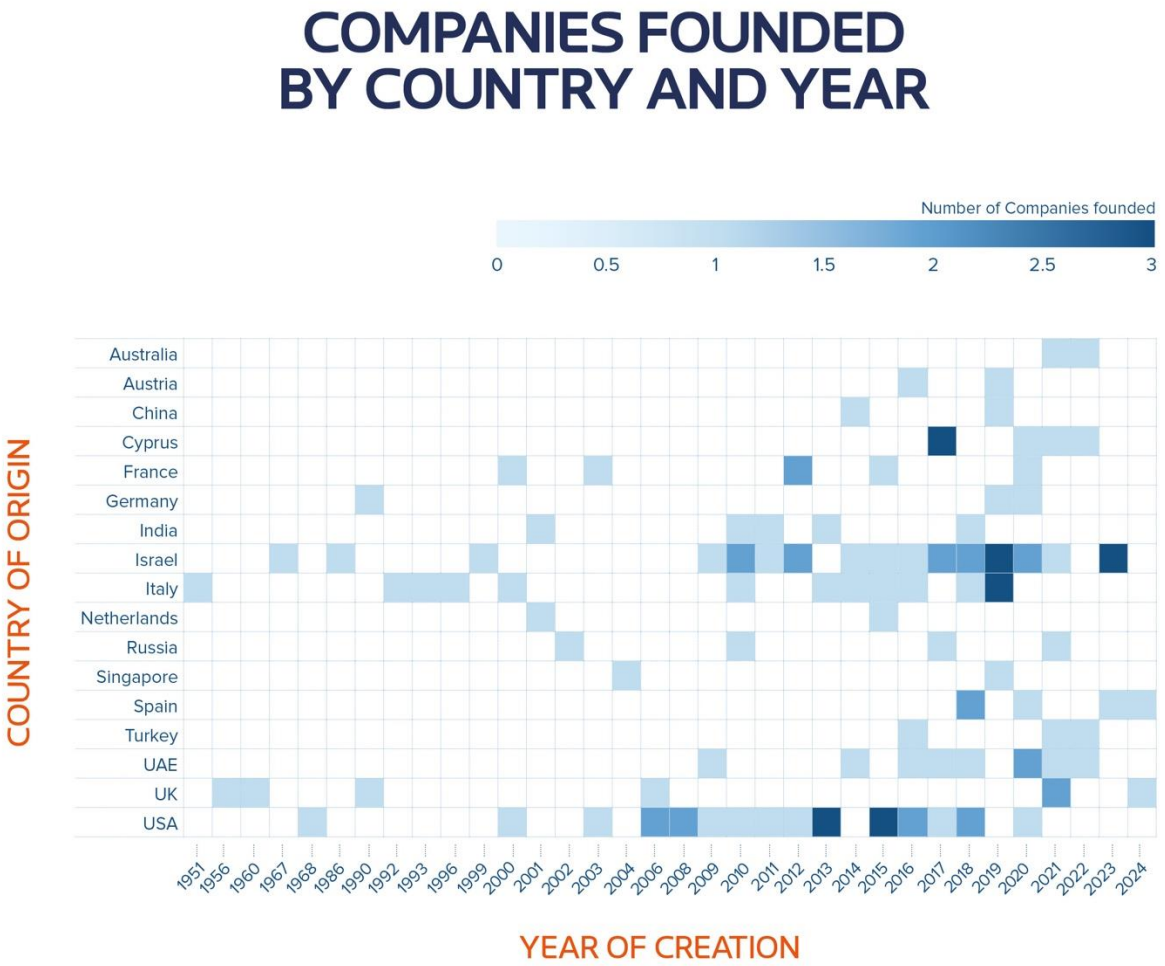
Economy of offensive corps: space



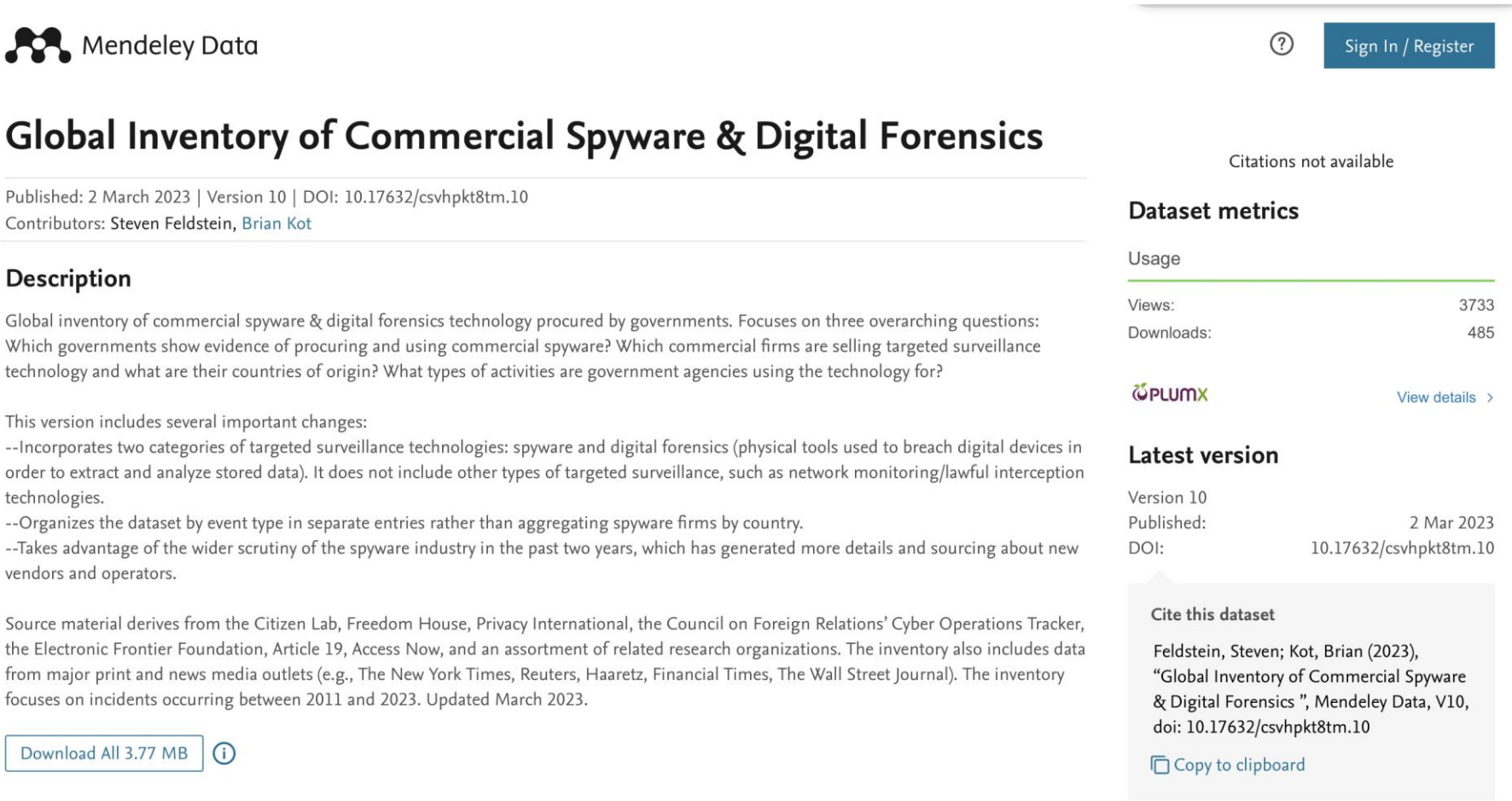
Economy of offensive corps: heatmap

- 12 countries have only 1 company, out of 29 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

- Mean year: 2011.2
- Median year: 2015
- Wassenaar: end of 2013



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

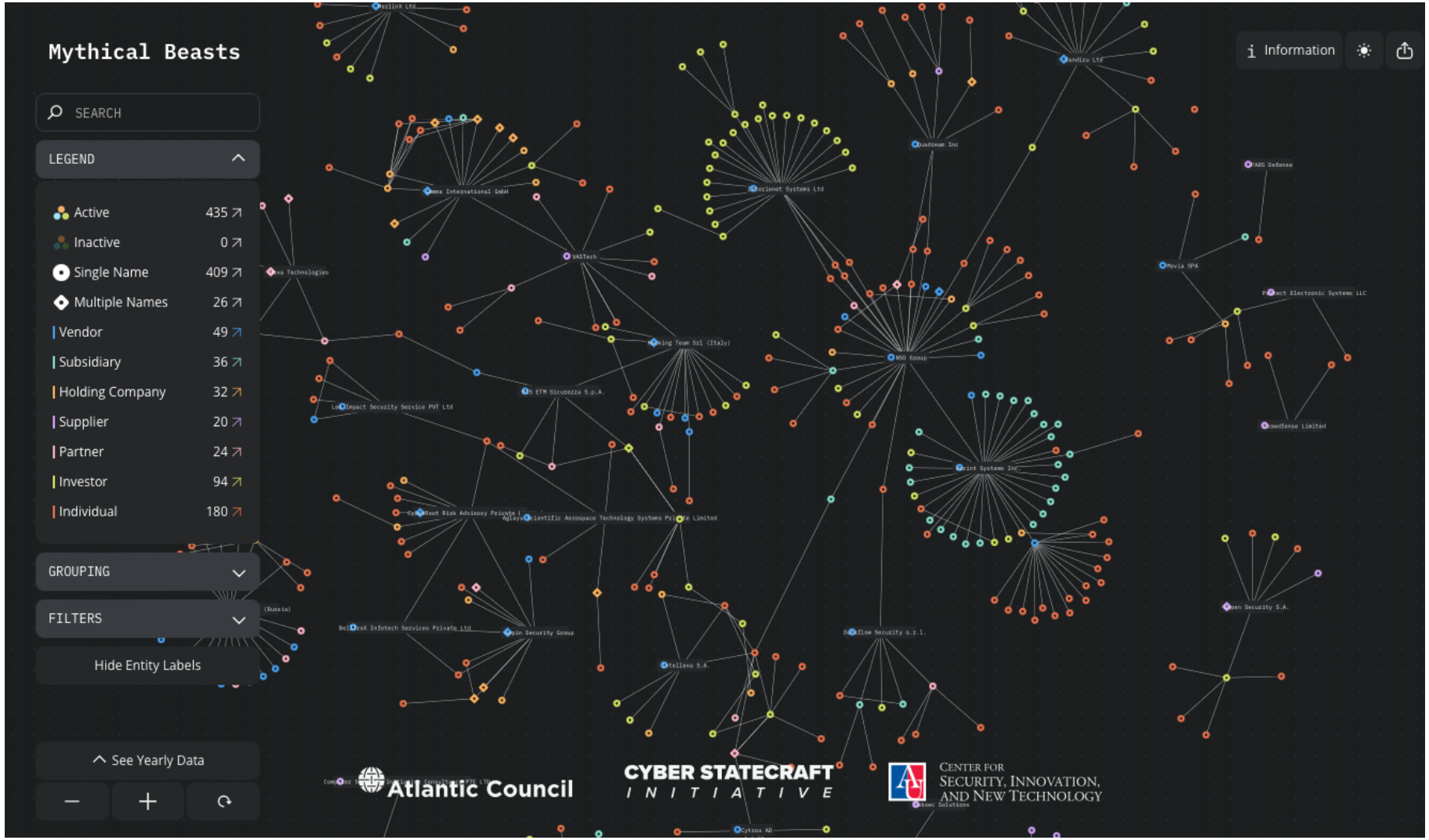
Cite this dataset

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

Copy to clipboard

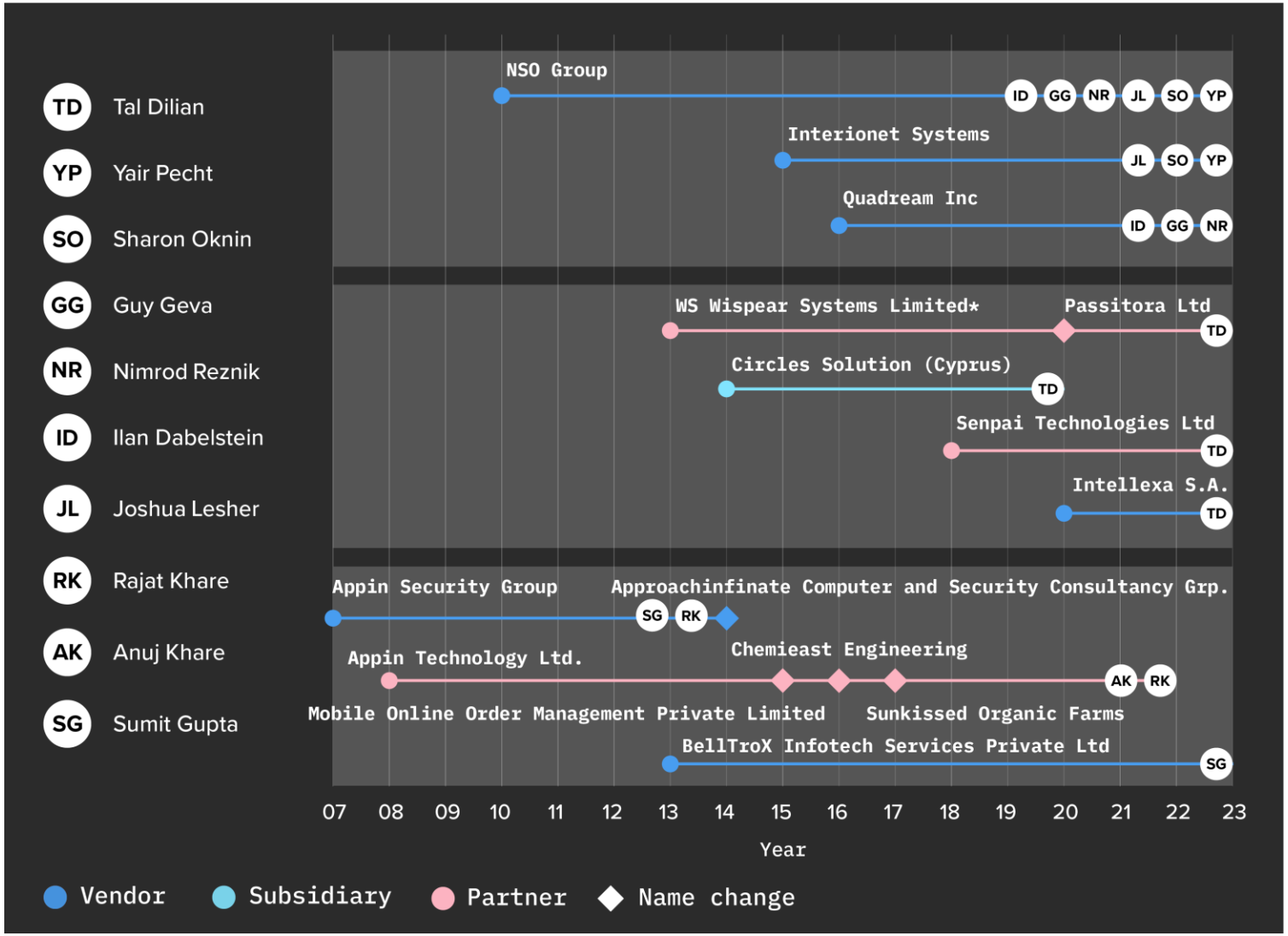
https://data.mendeley.com/datasets/csvhpkt8tm/10

And another one



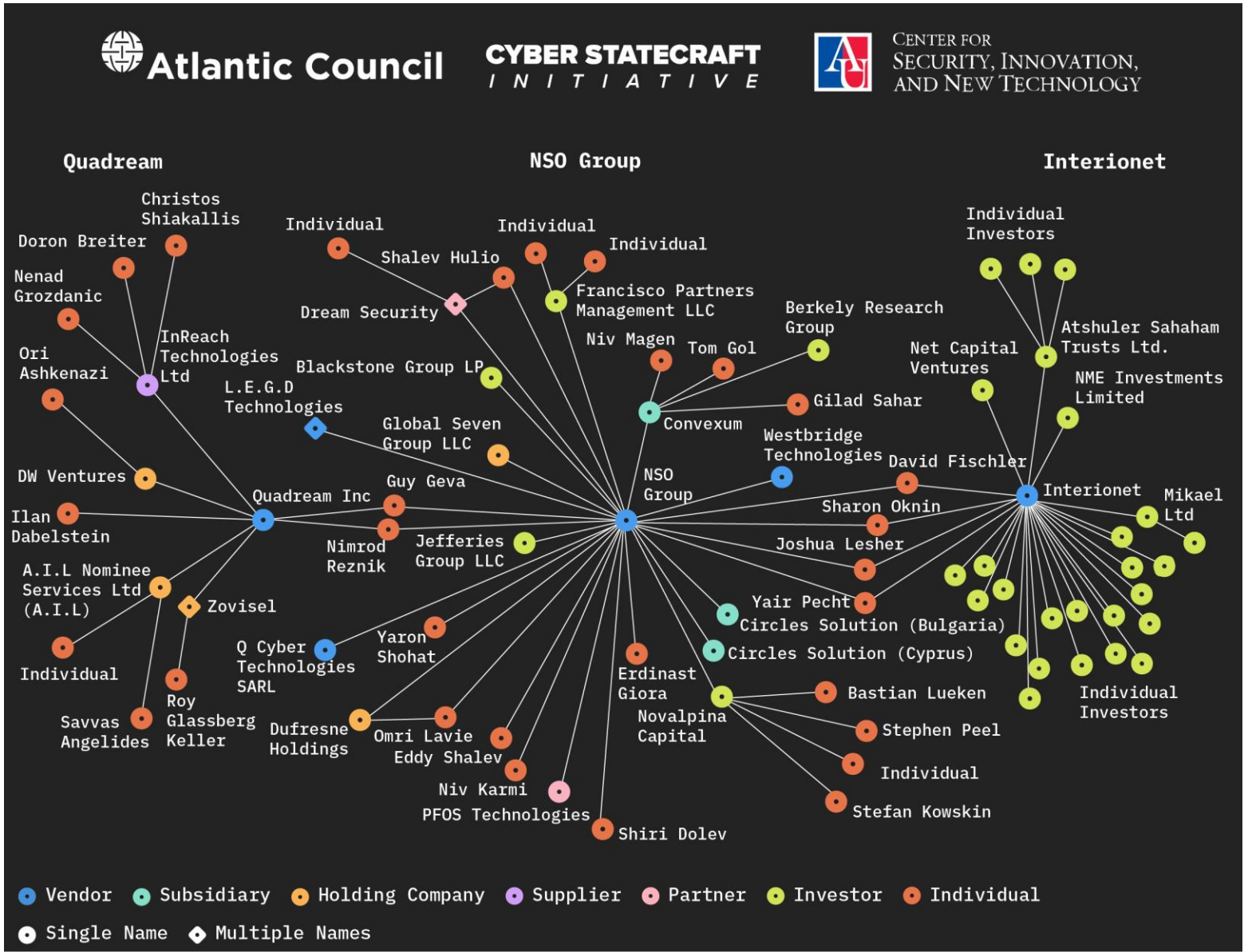
https://dfrlab.org/2024/09/04/mythical-beasts-and-where-to-find-them-report/

Mystical beasts: serial entrepreneurs

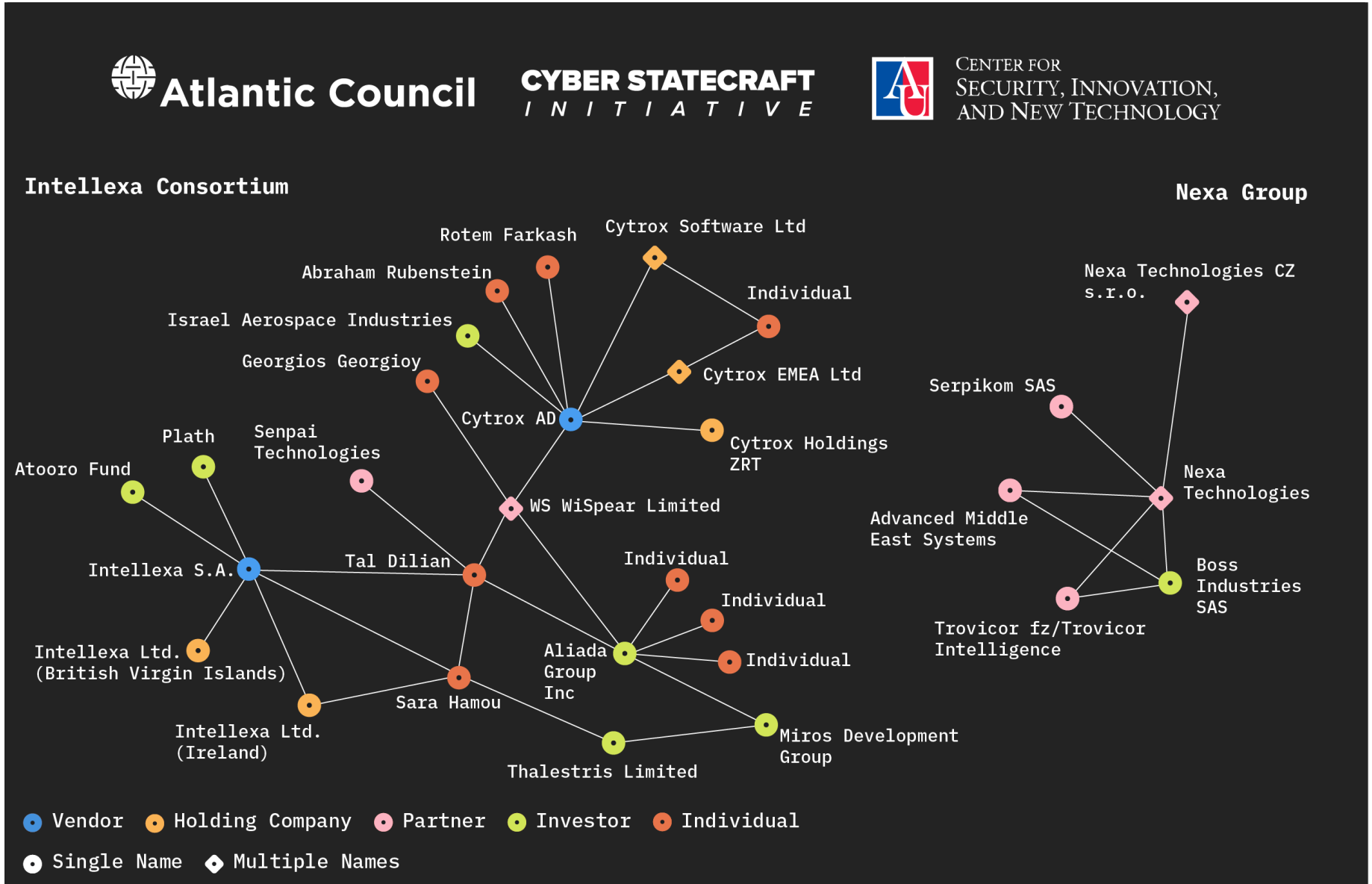


https://dfrlab.org/2024/09/04/mythical-beasts-and-where-to-find-them-report/

Mystical beasts: NSO galaxy



Mystical beasts: Intellexa constellation …



Cytrox Obfuscation

- **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/

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

https://www.issworldtraining.com

Geopolitics of Offensive Operations

Quarkslab

USA: love / hate with spyware (1/2: phantom)

- The US loved Pegasus a lot, but were worried it could spy on US citizen
- They forced NSO to ban +1 phone numbers from the platform
- Domestic US agencies want to use Pegasus, but cant because of the +1 ban
  - 2016: welcome to Westbridge Technologies, a NSO subsidiary pitching Phantom to San Diego Police
  - 2019: FBI buy a Phantom licence for 5m$, test for 2 years, discuss with DoJ on how to use it. Early 2022, Phantom is ditched. It will never be used in operations.

USA: love / hate with spyware (2/2: ban or buy?)

The ban

- 2021, Apple reveals US diplomats in Uganda have been spied with Pegasus
  - Oops, +1 is banned, but not local SIMs used by the US diplomats
- 11/21, NSO on trade blacklist by Commerce Department (+Candiru +Intellexa +Others)
  - Why? Spyware used against US diplomats in more than Uganda
- 03/23: EO by President Biden forbidding the use of spyware by any US agencies

The buy

- 2019: welcome to L3 Harris, merger fro negotiations m L3 Tech & Harris Corp
  - Paid 13m$ to settle allegations that Harris, before the merger, violated Export Control
- Early 2022: secret negotiations to buy NSO
- 07/22: leaks in the press
- 07/22: gov.us says they don't want the deal
- 07/22: negotiations dropped

The other buy

- 2019: Paragon, an IS cie
  - Ethical (vetted democracies)
  - Focus on messaging apps
- 09/24: ICE signs with Paragon (Graphite) a 2m$ contract
- 10/24: scandal, 2023 EO to cancel the deal
- 12/24: AE Partners (FL) buys Paragon for 500-900m$
- 01/25: WhatsApp notifies <100 users in Italy they are targeted
- 01/25: journalist spied in Italy
- 01/25: "licence cancelled" said Paragon, but not according to G. Melonie's partner

USA: buying a capacity

0-day stream

- **US Agencies**: internal teams like at NSA (read Snowden's leak)
- **Brokers**: Zerodium (now closed) used to pay millions for iOS and Android exploits.
- **Half-brokers, half-researchers**: Exodus Intelligence offers both 1-days and 0-days to public clients, including foreign governments, and private ones.
- **Researchers**: Azimuth Security, acquired by L3 Harris, works exclusively for the Five Eyes.
- **Defense contractors**: Companies like Northrop Grumman or Booz Allen Hamilton operate under contracts with the NSA.
- **Niche players**: Kryptonite Labs (smart home + medical devices) or ReVuln (ICS/SCADA systems).

Building a capacity: VC based

- In-Q-Tel funds Dreadnode, a startup developing offensive AI-based cybersecurity tools.
- The Pentagon and NSA work with private firms for both offensive and defensive cyber operations (L3Harris or big defense corps like Booz Allen Hamilton or Raytheon)
- Mergers like Magnet Forensics and Grayshift expand government-backed digital forensics

China: Very gov-centric

Leaked Evidence and China's Regulatory Control

- A 2024 leak from i-Soon, a cyber contractor, exposed how private firms conduct global espionage on behalf of the Chinese government.
- Leaked files showed i-Soon's work for Chinese Public Security and State Security agencies, targeting Europe, Asia, and North America.
- Chinese hacking operations are not limited to state agencies but also involve private contractors to enhance deniability and operational efficiency.
- Unlike in Western markets, China's cyber ecosystem is highly state-controlled:
  - A 2021 law requires all 0-day vulnerabilities found in China to be reported to the gov before being disclosed elsewhere.
  - Chinese firms are banned from selling exploits internationally; instead, discoveries are funnelled to state intelligence.
  - Foreign spyware products like Pegasus are rarely used, as China undoubtfully develops its own equivalents.

China: a public-private ”partnership”

Military-civil fusion in cyber operations

- China invests heavily in cyber offense through government funding, military budgets, and tech research grants.
- Universities, including elite C9 League schools, run state-funded labs dedicated to offensive cyber research.
- Government competitions and hacking challenges (like Tianfu Cup) encourage researchers to develop zero-day exploits, which are then acquired by the gov.

- Unlike Israeli or European firms, China does not commercially export offensive tools.
  - Conducts directly cyber operations rather than selling exploits abroad.
  - Some firms, like Qihoo 360, dominate global vulnerability research, often ranking highest in Android and Microsoft bug discoveries.

Russia: state sponsored hybrid warfare

Key APT Groups & Cyber Operations

- Sandworm (GRU 74455): NotPetya (2017), Ukraine power grid hacks (2022, 2024), GPS spoofing (2024).
- APT28 (Fancy Bear, GRU Unit 26165): European election phishing (2024), NATO contractor attacks.
- KillNet: Hacktivist DDoS attacks on U.S. hospitals (02/24) & European banks (04 /24).

Hybrid Warfare Tactics

- Cyber + Disinformation: leaked NATO documents (03/24), propaganda on Telegram & VK.
- Cyber + Kinetic Attacks: Sandworm’s attack on Kharkiv’s power grid (01/24) before missile strikes.
- Weaponized AI & Deepfakes: fake videos of German Chancellor Olaf Scholz (04/24) manipulated markets.

Russia: cybercriminal ecosystem & strategic shifts

Exploit Brokers & Alliances

- Exploit.in (exploit marketplace) & RAMP Forum : selling zero-day vulnerabilities
- BI.ZONE (Sberbank subsidiary): alleged link to Russian cyber ops
- Positive Technologies: sanctioned for ties to FSB & GRU

Russia's Shift to Domestic Cyber R&D

- ZeroZenX: develops mobile & desktop exploits
- Vulkan & ERA Technopolis: AI-powered cyber tools for FSB & GRU
- XakNet: hacker collective tied to Ukraine cyber-attacks (2024)
- State-funded cyber R&D hubs: training new experts, bypassing Western sanctions

Use of proxies to maintain plausible deniability

- Void Balaur: espionage-for-hire
- Evil Corp: ransomware group with Russian intelligence ties

Israel: a HUGE market

Cyber = business

- 2nd worldwide exporter: 6.86b$ in 2020
- 5-10% of worldwide cyber
- 41% of worldwide investments in cyber
- >450 active companies, 13 unicorns, 7 created in Q1 2021
- Tech = 18% of the GDP (cyber about 10%)
  - FR: tourism (7-8%), digital (6%), luxe (3-4%)

Israel: the diplomacy of spyware

Cyber = influence

- Started with opportunists growing business quickly (NSO, Candiru, Cellebrite...)
  - Exporting source code is prohibited since then to today
- Became a diplomatic leverage, same as any military hardware
  - Mexico and Panama shifted their votes at UN after acquiring Pegasus
  - Support of Arab nations for to Abraham Accords (2020) or campaign against Iran
- Funding foreign companies to grow “from the inside” and avoid bans
  - Dataflow in Italia, Epsilon in Spain, Paragon in the US
- Ethics in offensive: a new shift?
  - Paragon allegedly working only with vetted democracy
  - Cellebrite removing Serbian’s licenses after abuses, despite selling to Bengali death squad in 2021

India: cheap and domestically growing

From hack-to-hire to spycorps

- The world outsource its IT in India for cheap … same with hacking
- Appin (the origine story): starts with training then “hack-for-hire”
  - 2016: 2500$ / month for a “mission” (<100$ per day)
    - 22k$ for an iCloud account
  - Clients: lawyers, private investigators, companies, people…
- Market Growth: BellTroX, CyberRoot, Rebsec, Secfence , SideWinder, WhiteInt…

- First, behaved like mercenaries -> gained money
- Then relied on proxies with Intelligence & Army to learn and adapt the capacity (Sunworks Consultants, Semco Tech Services…) -> gained local immunity
- Now combined operations for internal (Sikh) or external (Pakistan) spying
- Declined to join US initiative for regulation

https://www.reuters.com/investigates/special-report/usa-hackers-appin/

Italy: fighting mafia then expending

Mob or privacy?

- Mafia is everywhere, from private to public sector
- Prosecutor can decide to eavesdrop on people without a judge
  - All legal interceptions are authorized (phone, cyber, electronic…)
  - Can intrude networks and operate abroad
  - 2022: 150 € / day for a spyware

=> Fighting mafia is #1 priority, whatever the cost

- Players: Memento Labs, Dataflow security, Negg Group, RCS, Area Spa, Innova,ISP, SIA…
    - Also legal interceptions, OSINT

- Too many internal players for a small market => look for new foreign markets
  - Nexa (FR) and hardened export control in Israel opened markets in SE Asia and Africa

Pall Mall

Quarkslab

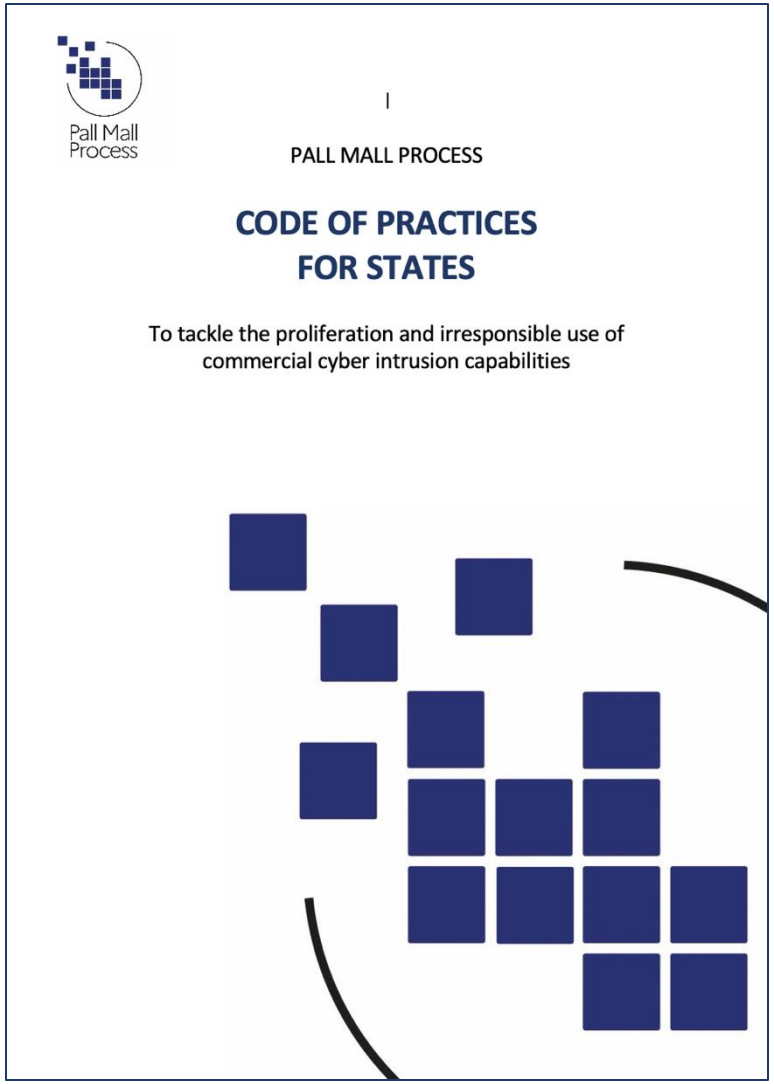
Strategic context

What is the Pall Mall Process?

- A multistakeholder international initiative launched in February 2024 by the UK and France
- Objective: Address the proliferation and irresponsible use of Commercial Cyber Intrusion Capabilities (CCICs), including spyware

Why it matters?

- CCICs expand state and non-state access to powerful surveillance tools
- Risks: human rights violations, national security threats, erosion of cyber stability
- Driven by state demand, vendor opacity, and poorly regulated global supply chains



Core good practice & policy levers

For governments

- Establish legal frameworks and independent oversight for CCIC procurement and use
- Leverage export controls, including human rights-based licensing criteria
- Use procurement policies to incentivize responsible vendor behavior
- Coordinate across government entities and foster international harmonization

For industry

- Adopt codes of conduct, transparency practices, and whistleblowing mechanisms
- Implement secure vulnerability handling, supplier vetting, and end-user auditing
- Provide ethical guidance and training to customers

Forward strategy & challenges

International action

- Develop shared definitions and accountability mechanisms
- Promote global norms (e.g., UN GGE, EU Dual-Use Regulation)
- Consider an international oversight body and certification schemes

Tensions & risks

- Balancing security and transparency
- Managing dual-use dilemmas (e.g. penetration testing vs. espionage)
- Avoiding fragmentation and exploitation of regulatory gaps

Conclusion

- The Pall Mall Process seeks to foster a responsible, rights-respecting global CCIC market
- Success depends on coordinated, enforceable action by both governments and industry

Conclusion

Quarkslab

Breaking news: May 7th

Super spyware maker NSO must pay Meta $168M in WhatsApp court battle

Don't f&#k with Zuck

Iain Thomson — Tue 6 May 2025 // 23:50 UTC

A California jury has awarded Meta more than $167 million in damages from Israeli surveillanceware slinger NSO Group, after the latter exploited a flaw in WhatsApp to allow its government customers to spy on supposedly secure communications.

In May 2019 engineers at WhatsApp discovered a zero-click, zero-day vulnerability in the Meta-owned chat platform that would allow an attacker to install malware on a device with just a single phone call and no requirement on the victim to do anything other than have their handheld switched on. The surveillanceware in question was Pegasus, developed by the NSO Group.

Compensatory damages: 445m$

➔ Just for NSO to repair the hack

Punitive damages: 168m$

➔ For EVERY SPYCORP doing the same

Spycorps are like cockroaches?

Spycorps = Corporate Cockroaches

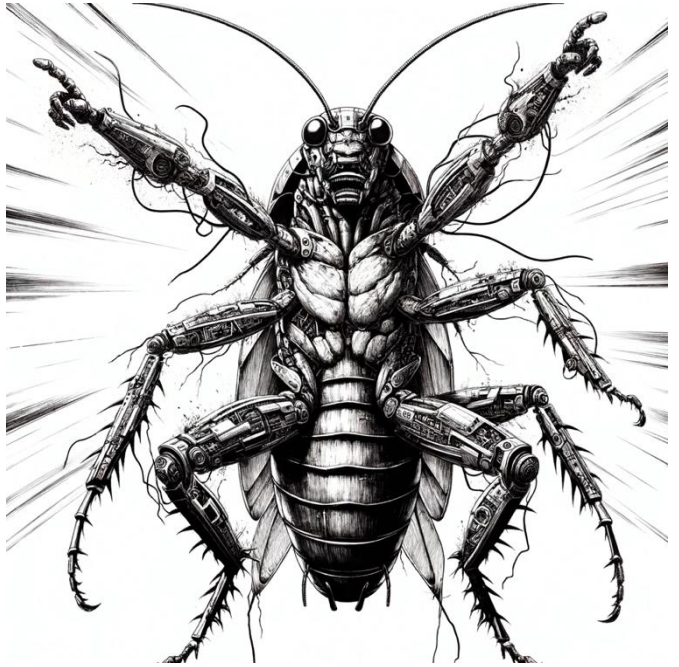
Despite scandals, leaks, and lawsuits, spyware companies persist—adaptable and built for survival.

1. Customers
- Repressive and democratic states keep buying
- “Terrorist” label justifies surveillance
- Demand remains strong despite exposure

2. Legal
- Frequent rebranding (e.g., Candiru: 8+ names)
- Shell companies, insolvencies, and restructures blur accountability
- Lawsuits don’t stop operations

3. Regulation
- Wassenaar Arrangement (2013) poorly enforced.
- Key players (US, Israel, China) bypass or ignore it.
- New effort: Pall Mall Process (2024) is promising but early.

4. Tech
- Infrastructure easy to rebuild with modern DevOps.
- Pegasus, Predator exposed, yet still operational.
- Tools redeployed in new forms, under new names.

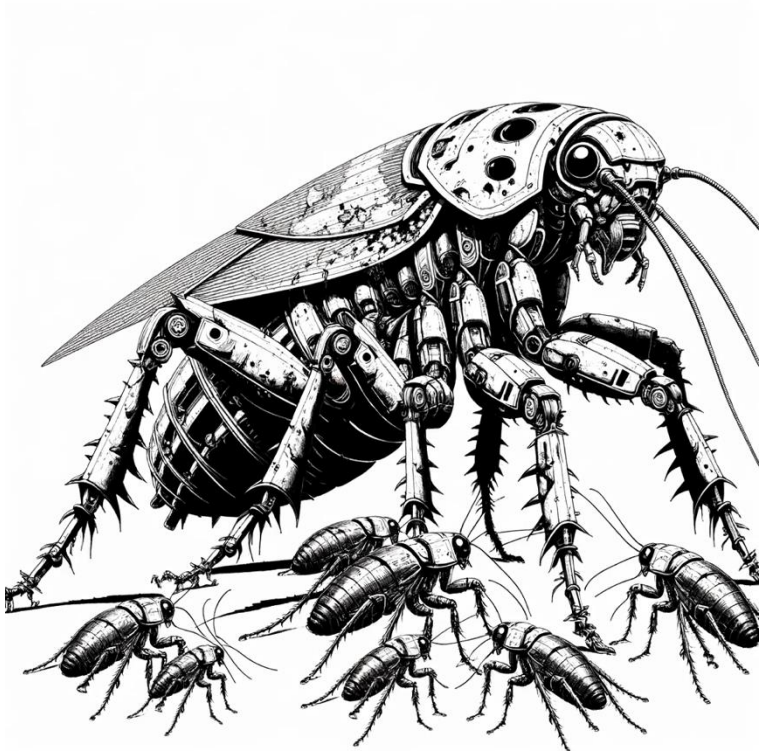


Spycorps thrive because demand, loopholes, and technology enable constant reinvention.

Political economy of the spyware market

Demand is extremely high => even when a supplier sanctioned, financial motivation for others to fill in the gap

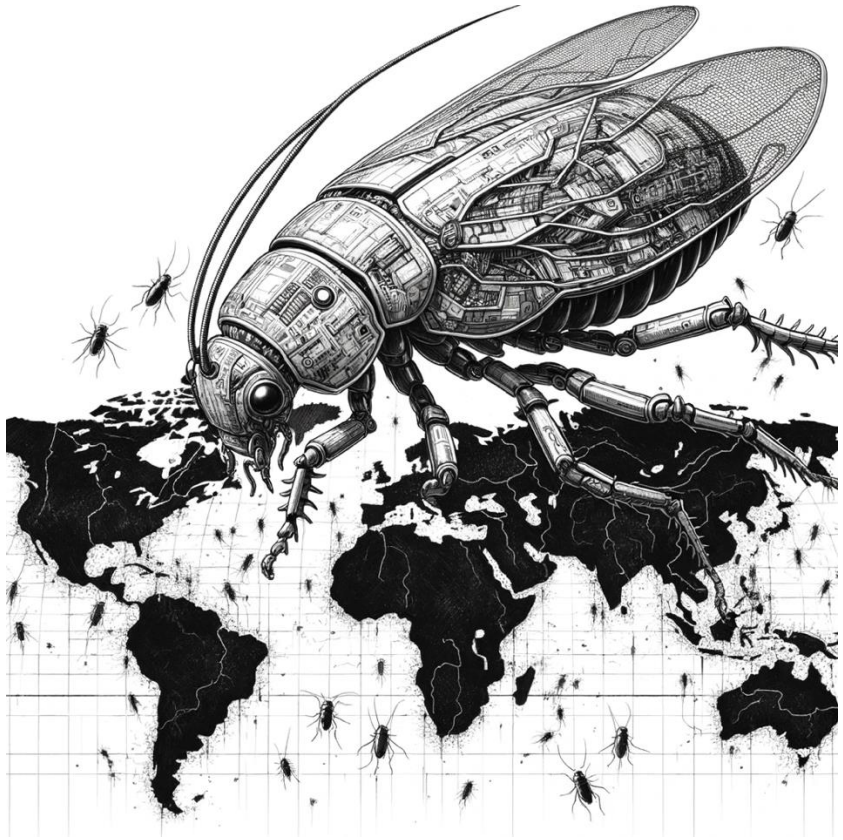
- Old suppliers (FinFisher, Hacking team) replaced by new ones (NSO, Cytrox, Candiru, Paragon, Intellexa…)
- Even if top-tier firms were shut down, there are enough boutique firms & hacker-for-hire to replace



Ethical offensive: a new trend?

- Paragon working for identified democracies
- Cellebrite revoking a licences
- CrowdFense or DataFlow claiming a strict internal vetting

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

OUR CONSULTING

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

OUR PRODUCT: QSHIELD

- SENSITIVE ASSETS IN-APP PROTECTION

MERCI ☺

Fred Raynal
fraynal@quarkslab.com

Quarkslab