Spyware for rent

Nullcon Berlin 2024

Fred Raynal
fraynal@quarkslab.com

NULLCON
INTERNATIONAL SECURITY CONFERENCE

Quarkslab

Warning

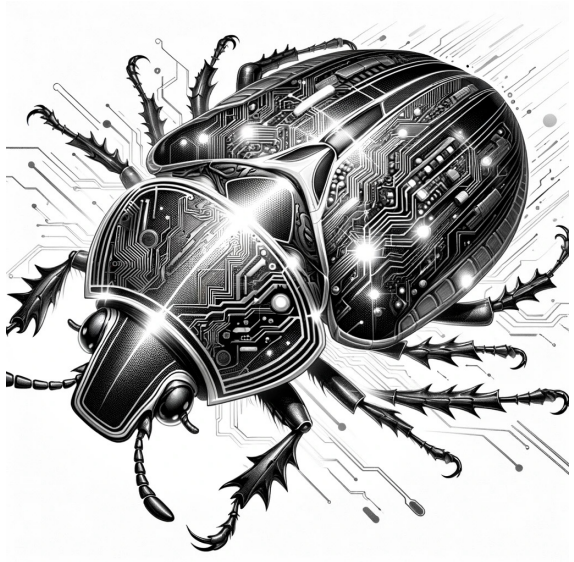
- This talk is mostly based on **open source information**
  - A lot is available thanks to leaks + CitizenLab, Amnesty International, Wikileaks…
  - Bias: Russia & China are not well represented

- **Law != Ethic**
  - Law = set of rules agreed by a group of « people »
  - Ethic = individual rules & values

What is spyware?

Quarkslab

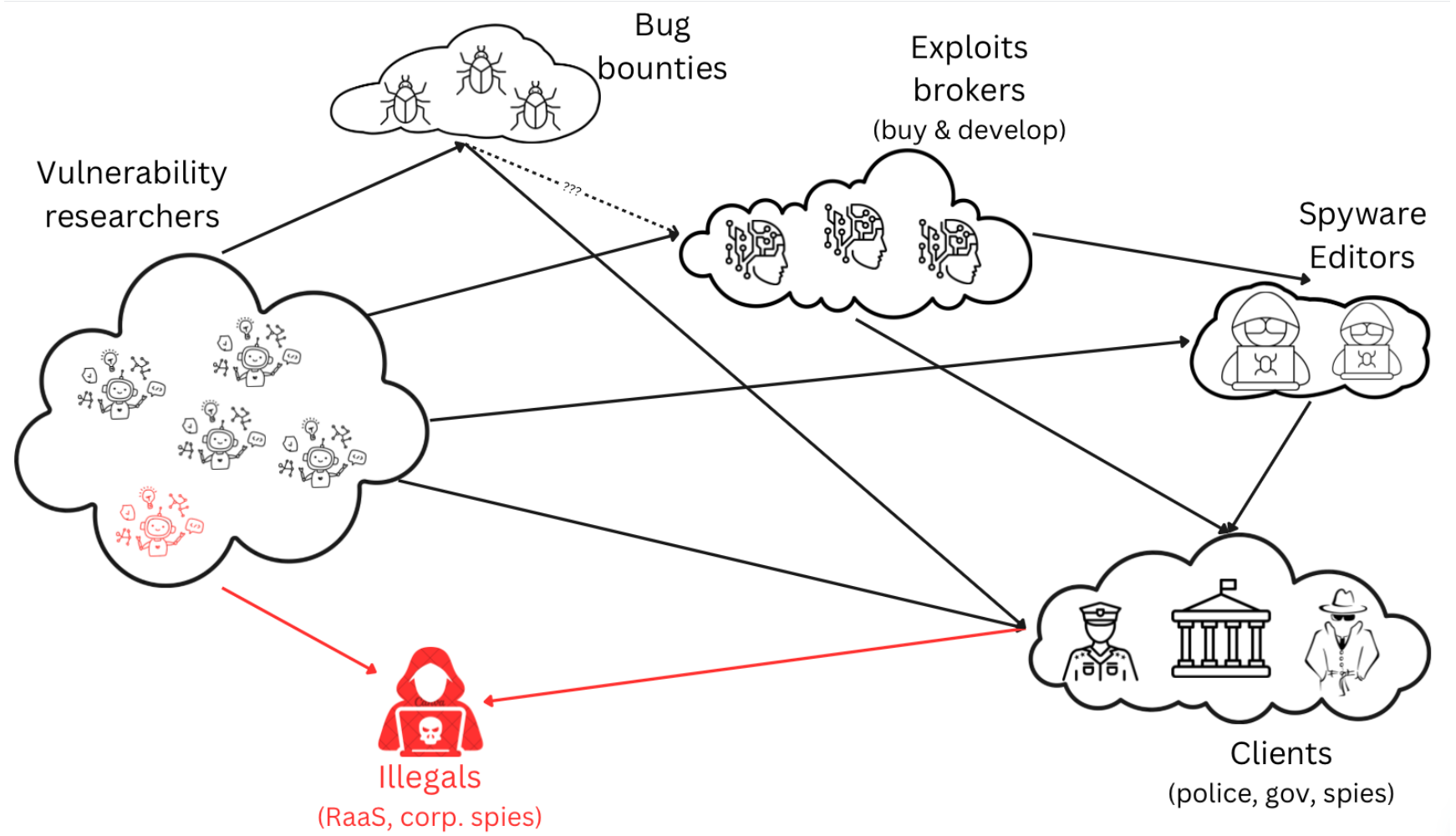
SPYWARE ?



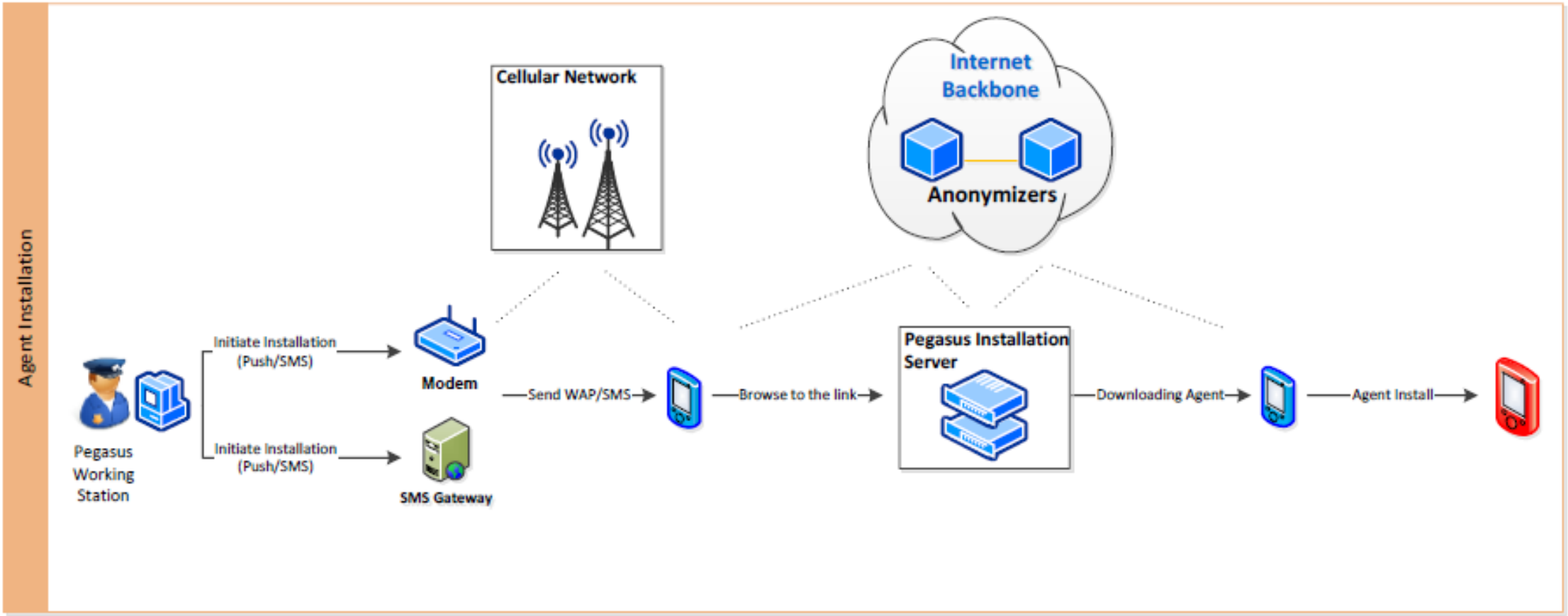
A software that enables a user to obtain covert information about another's computer activities by transmitting data covertly from their system.

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

The spyware (under)world

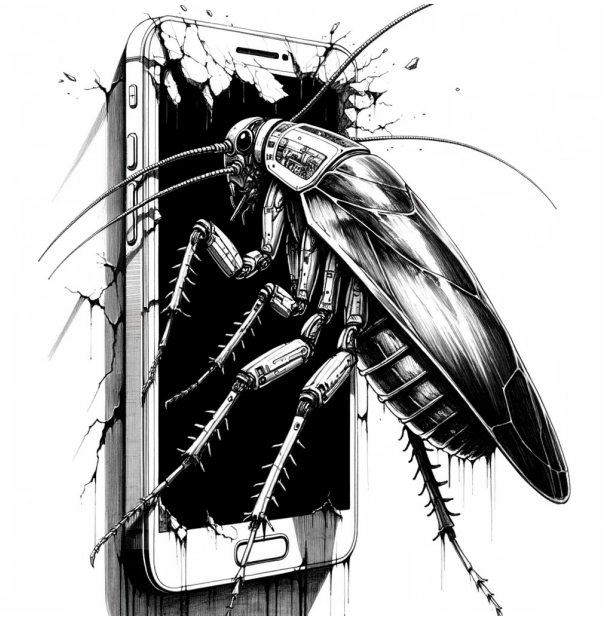


How does it work: overall architecture



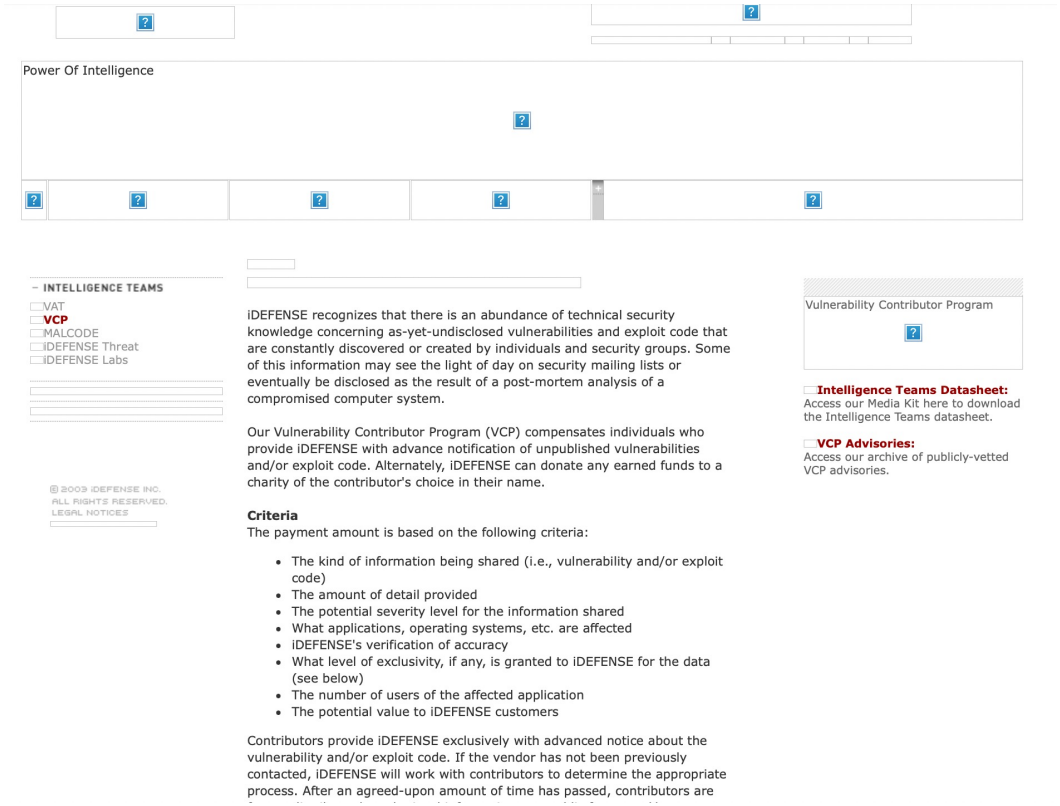
From Pegasus : product description (about **2013**!!)

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
- **0-click**: exploit is sent and executed without the need for the user to do anything

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

Buying 0-days: TippingPoint / 3Com (2005)

http://www.zerodayinitiative.com/ 07/2005

Buying 0-days : TippingPoint / 3Com (2005)

Since 3Com and TippingPoint customers are protected prior to the disclosure, are they aware of the vulnerability?

In order to maintain the secrecy of a researcher's vulnerability discovery until a product vendor can develop a patch, 3Com and TippingPoint customers are only provided a generic description of the filter provided but are not informed of the vulnerability. Once details are made public in coordination with the product vendor, TippingPoint's Digital Vaccine® service for the Intrusion Prevention System provides an updated description so that customers can identify the appropriate filters that were protecting them. In other words, 3Com and TippingPoint will be protected from the vulnerability in advance, but they will not be able to tell from the description what the vulnerability is.

Why are you giving advance notice of the vulnerability information you've bought to other security vendors, including competitors?

We are sharing with other security vendors in an effort to do the most good with the information we have acquired. We feel we can still maintain a competitive advantage with respect to our customers while facilitating the protection of a customer base larger than our own.

How it worked?

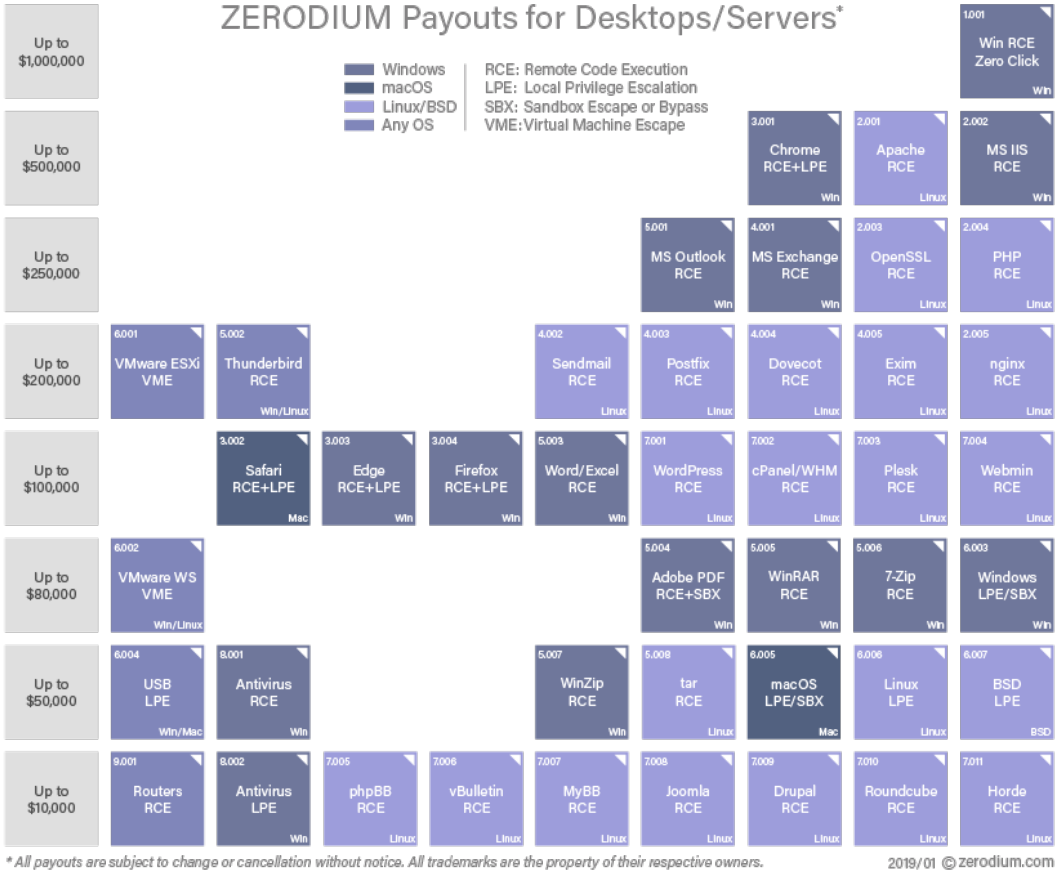
- A vuln is reported
- TP / 3Com “shares” the information with other vendors & the ditor
- TP / 3Com provides a signature for the vuln
- A patch is realeased … later

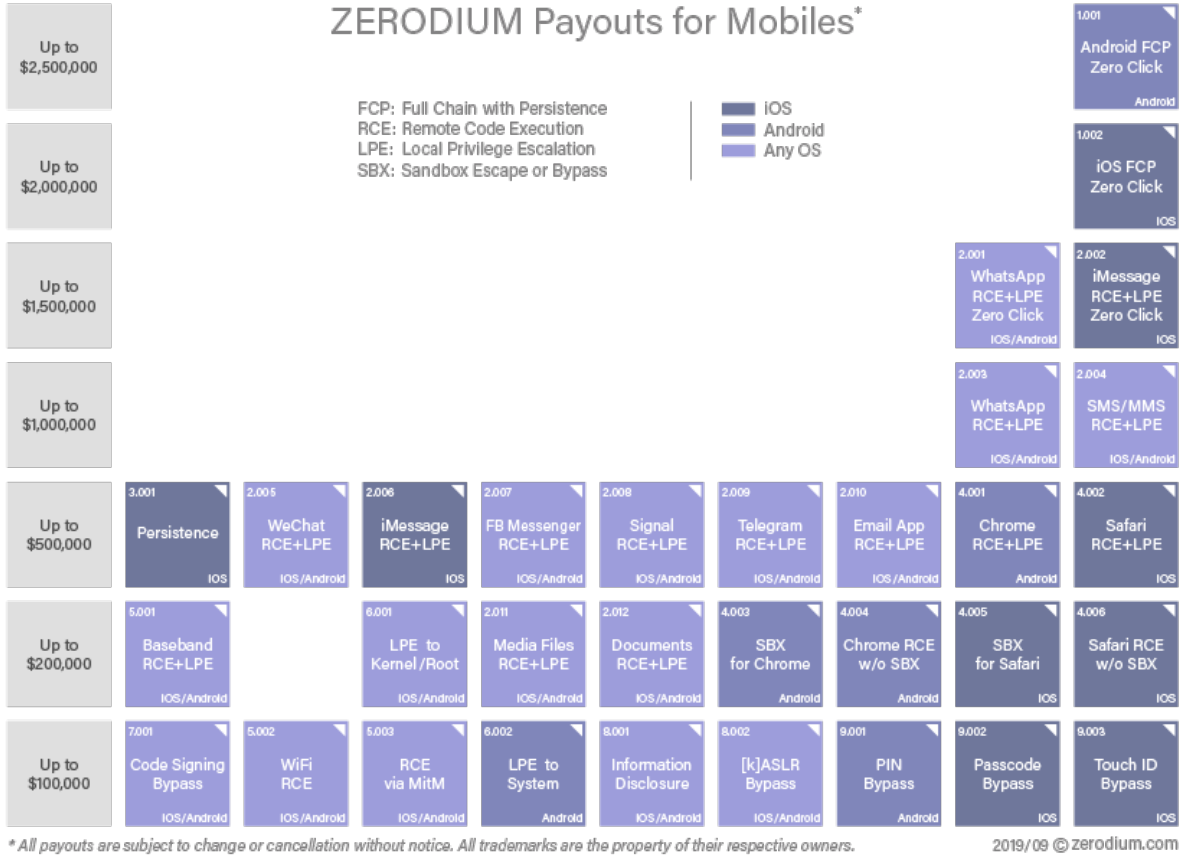
The problem

OPSec failure => can retrieve root cause from signature

http://www.zerodayinitiative.com/ 07/2005

Buying 0-days : Zerodium (2015)





https://zerodium.com/program.html/ 01/2019

Spyware (aka « agent ») Installation

1. The exploit gives full control on the target phone
2. The payload connects to a website to download the spyware
3. Spyware is installed

Persistence: on some mobile, spyware can survive reboot. Not on other.

A big deal?

Not really as attackers just have to relaunch an initial access to get access to the phone … until the next reboot

From the attacker: an **OPSEC** problem
How to preserve its infrastructure?

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**!!)

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

Marketing

Quarkslab

Marketing: Hacking Team

]HackingTeam[| About us | The Solution | Customer Policy | Careers | Contacts

Home ▸ About us

About us

Here in HackingTeam we believe that fighting crime should be easy: we provide effective, easy-to-use offensive technology to the worldwide law enforcement and intelligence communities. Technology must empower, not hinder.

Exclusively focused on offensive security, HackingTeam was founded in 2003. In 2004, we were the first to propose an offensive solution for cyber investigations, with such a strong reception that in 2007 we were venture backed. All the development is made in Milan, by a team of 40+ professionals focusing on all the aspects of offensive security, Our technology is used daily to fight crime in six continents.

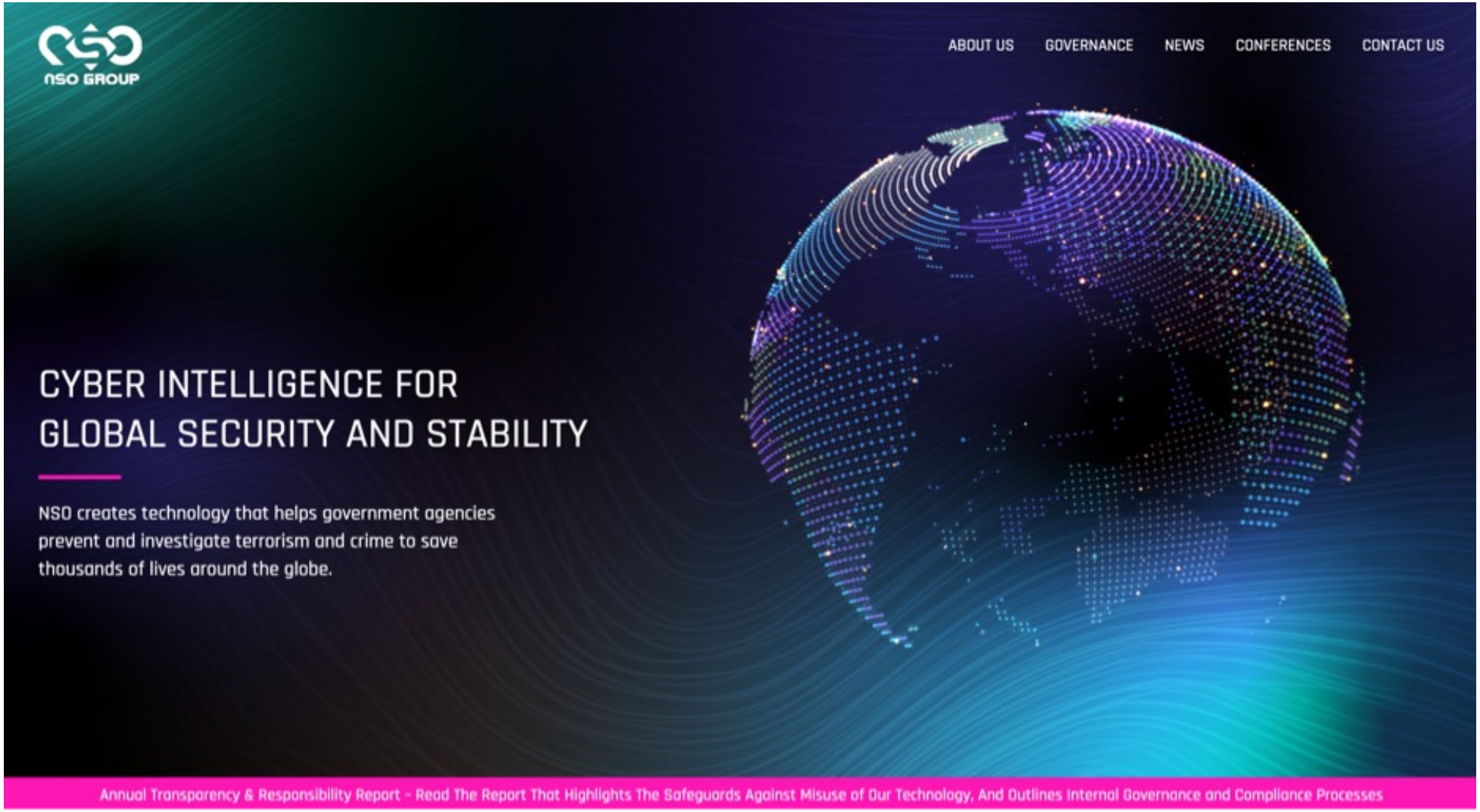
Hacking Team

Via della Moscova n.13
20121 - Milano
Italy

1997 Annapolis Exchange Parkway
Suite 300, Annapolis, MD 21401
U.S.A.

UOB Plaza 1
80 Raffles Place Level 35-25
Singapore 048624

Marketing: NSO



Marketing: Intellexa

001 / CORPORATE

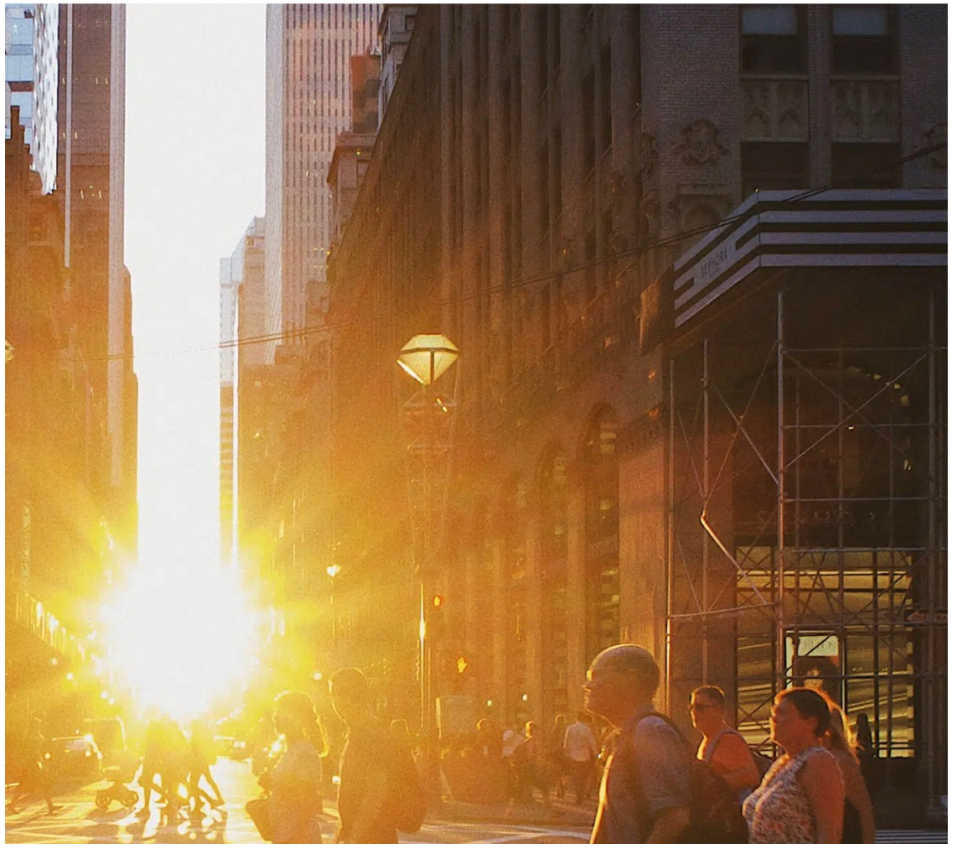
About us

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

FinFisher (Gamma Group) 2011

FinFisher Pricing 2H 2009

ITEM	DESCRIPTION	MODEL	QTY		UNIT PRICE EURO	LINE TOTAL EURO	UNIT PRICE EURO	LINE TOTAL EURO
1.1.4	FinSpy Mobile Activation License (Q4, 2011): - Blackberry - Windows Mobile - iPhone	FSMOB	0	1	1'950.00	0.00	1'560.00	0.00
1.1.5	**Optional Voice Recording (Q4, 2011):** FinSpy Mobile Voice Server License (for PRI Provisioning of calls) - VOIP recording included in standard solution	FSVR	0	1	25'000.00	0.00	20'000.00	
1.1c	**FinSpy Software: Medium (31 to 150 Targets)**							
1.1.1	FinSpy Relay License FinSpy Master License FinSpy Generation License	FSPY-PLSW FSPY-MLSW FSPY-GLSW	1	1	185'000.00	185'000.00	148'000.00	148'000.00
1.1.2	FinSpy Agent License (per client)	FSPY-AGLSW	10	1	9'500.00	95'000.00	7'600.00	76'000.00
1.1.3	FinSpy Activation License: - Windows - OSX	FSPY-PCALSW	75	1	1'462.50	109'687.50	1'170.00	87'750.00
1.1.4	FinSpy Mobile Activation License (Q4, 2011): - Blackberry - Windows Mobile - iPhone	FSMOB	0	1	1'462.50	0.00	1'170.00	0.00
1.1.5	**Optional Voice Recording (Q4, 2011):** FinSpy Mobile Voice Server License (for PRI Provisioning of calls) - VOIP recording included in standard solution	FSVR	0	1	25'000.00	0.00	20'000.00	
1.1d	**FinSpy Software: Open (151 to 500)**							
1.1.1	FinSpy Relay License FinSpy Master License FinSpy Generation License	FSPY-PLSW FSPY-MLSW FSPY-GLSW	1	1	250'000.00	250'000.00	200'000.00	200'000.00
1.1.2	FinSpy Agent License (per client)	FSPY-AGLSW	3	1	9'500.00	28'500.00	7'600.00	22'800.00
1.1.3	FinSpy Target Activation License: - Windows - OSX	FSPY-PCALSW	250	1	1'170.00	292'500.00	936.00	234'000.00
1.1.4	FinSpy Mobile Target Activation License (Q4, 2011): - Blackberry - Windows Mobile - iPhone	FSMOB	0	1	1'170.00	0.00	936.00	
1.1.5	**Optional Voice Recording (Q4, 2011):** FinSpy Mobile Voice Server License (for PRI Provisioning of calls) - VOIP recording included in standard solution	FSVR	0	1	25'000.00	0.00	20'000.00	
1.2	**FinSpy Hardware**							
1.2.1	FinSpy Master Server	FSPY-MASTSVR	1	2	5'500.00	5'500.00	4'950.00	4'950.00
1.2.2	Option1: Unified Network Storage 4TB	FSPY-UNS4TB	0	2	1'700.00	0.00	1'530.00	0.00
1.2.3	Option 2: Unified Network Storage 8TB	FSPY-UNS8TB	0	2	2'200.00	0.00	1'980.00	0.00
1.2.4	**Optional Voice Recording:** FinSpy Mobile Voice Server	FSVR	0	2	8'000.00	0.00	7'200.00	
1.2.5	FinSpy Agent Workstation	FSPY-AGWS	3	2	1'000.00	3'000.00	900.00	2'700.00
1.2.6	FinSpy Common & Spare Parts	FSPY-COMMON	1	2	11'000.00	11'000.00	9'900.00	9'900.00
1.3	**FinSpy - Support**							
1.3.1	FinLifeline Support: FinSpy Update & Upgrade Fee (Year 1)	FLL-FSS1	1	1	255'338.00	255'338.00	204'271.00	204'271.00
1.3.2	FinLifeline Support: FinSpy Update & Upgrade Fee (Year 2)	FLL-FSS2		1	280'872.00	0.00	224'698.00	0.00
1.3.3	FinLifeline Support: FinSpy Update & Upgrade Fee (Year 3)	FLL-FSS3		1	308'960.00	0.00	247'168.00	0.00
1.4	**FinSpy - Installation & Training**							
	FinSpy Installation and Product Training Number of Students: 2-4 Location: In-country Duration: 2 days Installation + 3 days Training Documentation: Soft and hard copies Including: Trainer's airfare, accommodation, subsistence	FSPYT	1	2	17'500.00	17'500.00	15'750.00	15'750.00
2	**FinSpy Mobile Stand Alone system (Delivery before Q4/2011)**							
2.1	**FinSpy Mobile Software**							

Hacking Team 2012-2015

HT S.r.l.
Sede legale e operativa: Via della Moscova,13 – 20121 Milano – Tel: +39.02.29.06.06.03
e-mail: info@hackingteam.it – web: http://www.hackingteam.it – Fax: +39.02.63118946
P.IVA: 03924730967 – Capitale Sociale: € 223.572,00 i.v.
N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

NISS - National Intelligence ans Security Services
Arkweet 61/354
Abaed Khatim St.
Kartoum
Sudan

Registration number 352/07

Milan, September 5th, 2012

Invoice no. 116/2012
Ref. Our Offer no. 20120601.088-1.MM
Ref. Contract signed on June 29th, 2012

Remote Control System - Second payment 50%	480,000.00
Total Amount	**480,000.00**

VAT does not apply in accordance with Italian Presidential Decree 633/72, art. 7

Terms of payment:
15 days invoice date

By wire bank transfer to:
HT S.r.l. - Deutsche Bank via S. Prospero 2, 20121 Milan, Italy IBAN IT50P0310401600000000825132 BIC/ SWIFT Code: DEUTITMM

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	1	
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

Candiru 2020

Infection Vectors

>	Hyperlink	
>	Weaponized file – Office file OR other (for Windows OS only)	**Included**
>	Online physical attack vector (for Windows OS only)	
>	Dissemination vector between platforms	
>	Man in The Middle (MiTM) attack vector/price per browser	
>	Sherlock for Windows, iOS and Android platforms – Optional	**(€6,000,000)**
>	Integration to existing tactical solution	

SYSTEM ADDITIONAL PRICING OPTIONS

NO.	ITEM DESCRIPTION	QTY.	TOTAL (EURO)
SYSTEM LICENSES			
1	**Additional 15 concurrent Infiltration Agents and 1 more country** (Total of X concurrent agents and XX countries)	1	**€1,500,000**
2	**Additional 25 concurrent Infiltration Agents and 5 more countries** (Total of X concurrent agents and XX countries)	1	**€5,500,000**

Additional Agent Applications & Capabilities			
Retrieval of user cookies from supported browsers/price per browser		1	**€200,000**
Development and maintenance of the following applications:			
	• Twitter	1	**€200,000**
	• Viber	1	**€200,000**
	• Signal	1	**€500,000**

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

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

March 2024: NSO to give its code source to WhatsApp

As part of the ongoing dispute between NSO and WhatsApp, a California judge has just ordered NSO to hand over the source code of its Pegasus spyware to WhatsApp.

WhatsApp launched a procedure in 2019 following revelations of 1,400 users being spied on by Pegasus.

The judge further specifies that NSO must provide “all relevant software” (0-days too?) for the period of one year before and after the 2 weeks when WhatsApp users were targeted, i.e. from April 29, 2018 to May 10, 2020.

NSO must also detail the functionality of Pegasus.

On the other hand, they will not have to disclose their customers, targets and elements of its order infrastructure.

https://www.theguardian.com/technology/2024/feb/29/pegasus-surveillance-code-whatsapp-meta-lawsuit-nso-group

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 spycorps: 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?
- 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.

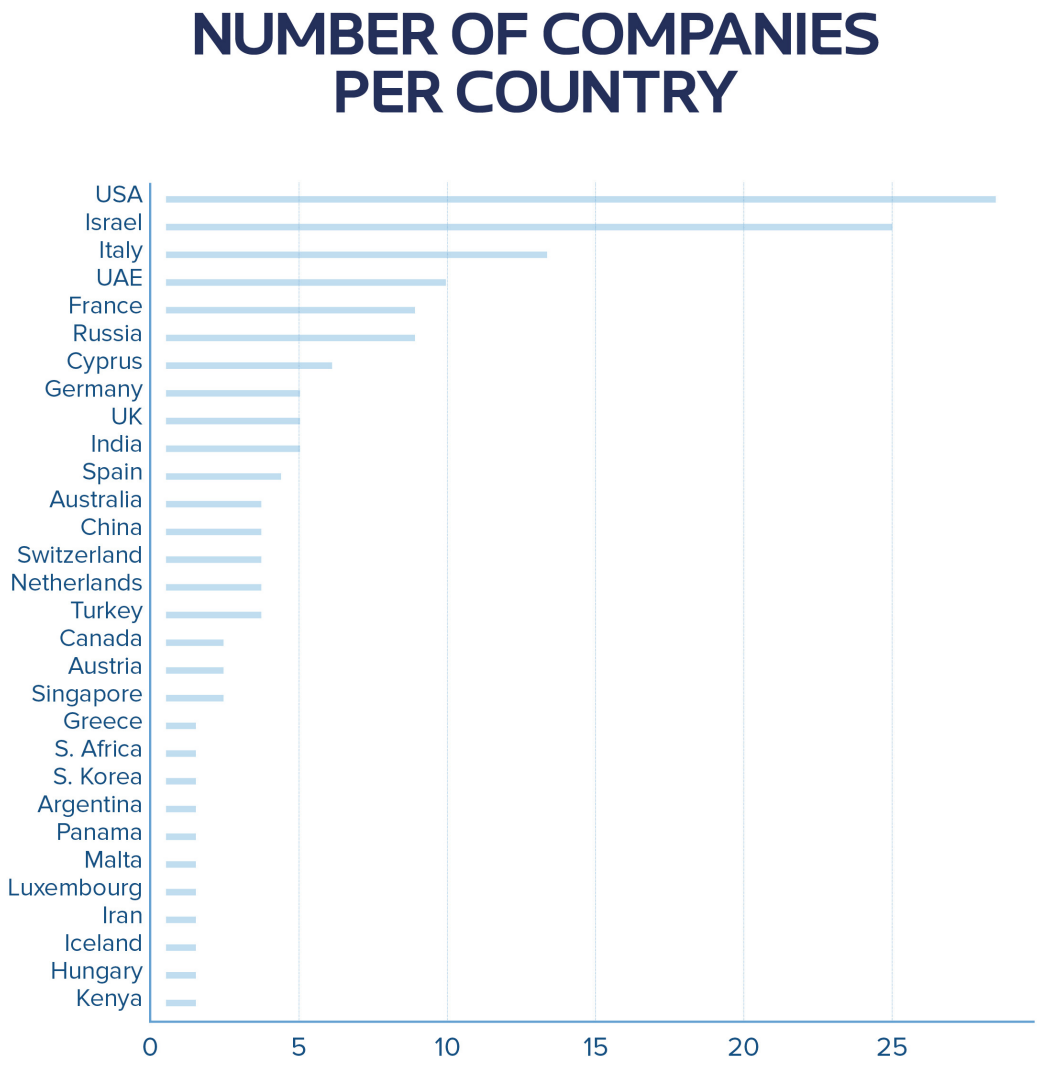
A ChangeLog is available at the end of this page. The entries are listed in alphabetic order (based on the company's name).

Last update: *22 February 2024*

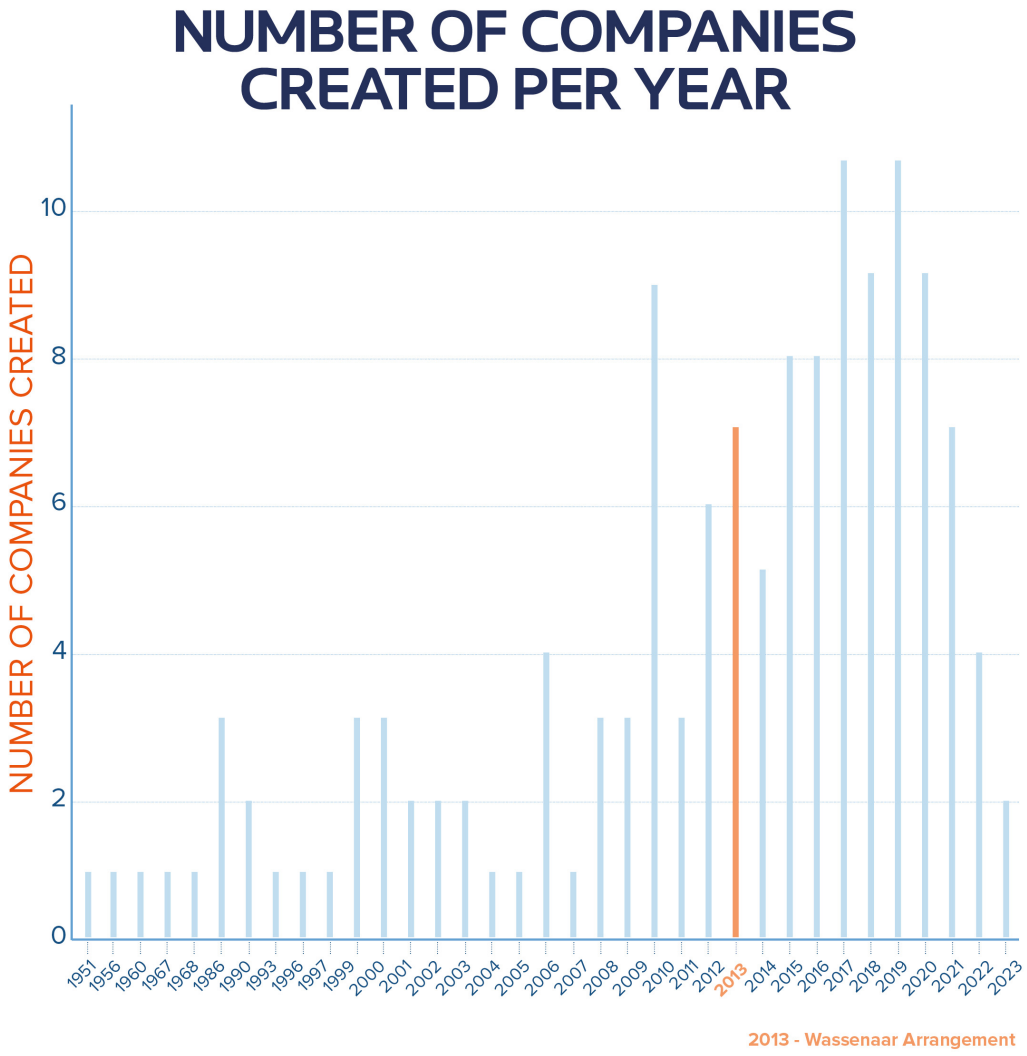
Name	Country	Founded	Status	OSINT Reference
Ability	Israel	-	-	WikiLeaks
ACE Labs	Israel	2016	Active	Calcalist
Accuvant	USA	2002	Merged (with Optiv)	TechnologyReview
AFB Systems	UAE	2021	Active	IntelligenceOne
Advanced Impact Media Solutions	Israel	2018	Active	The Guardian
Altrnativ	France	2020	Active	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 spycorps: geography



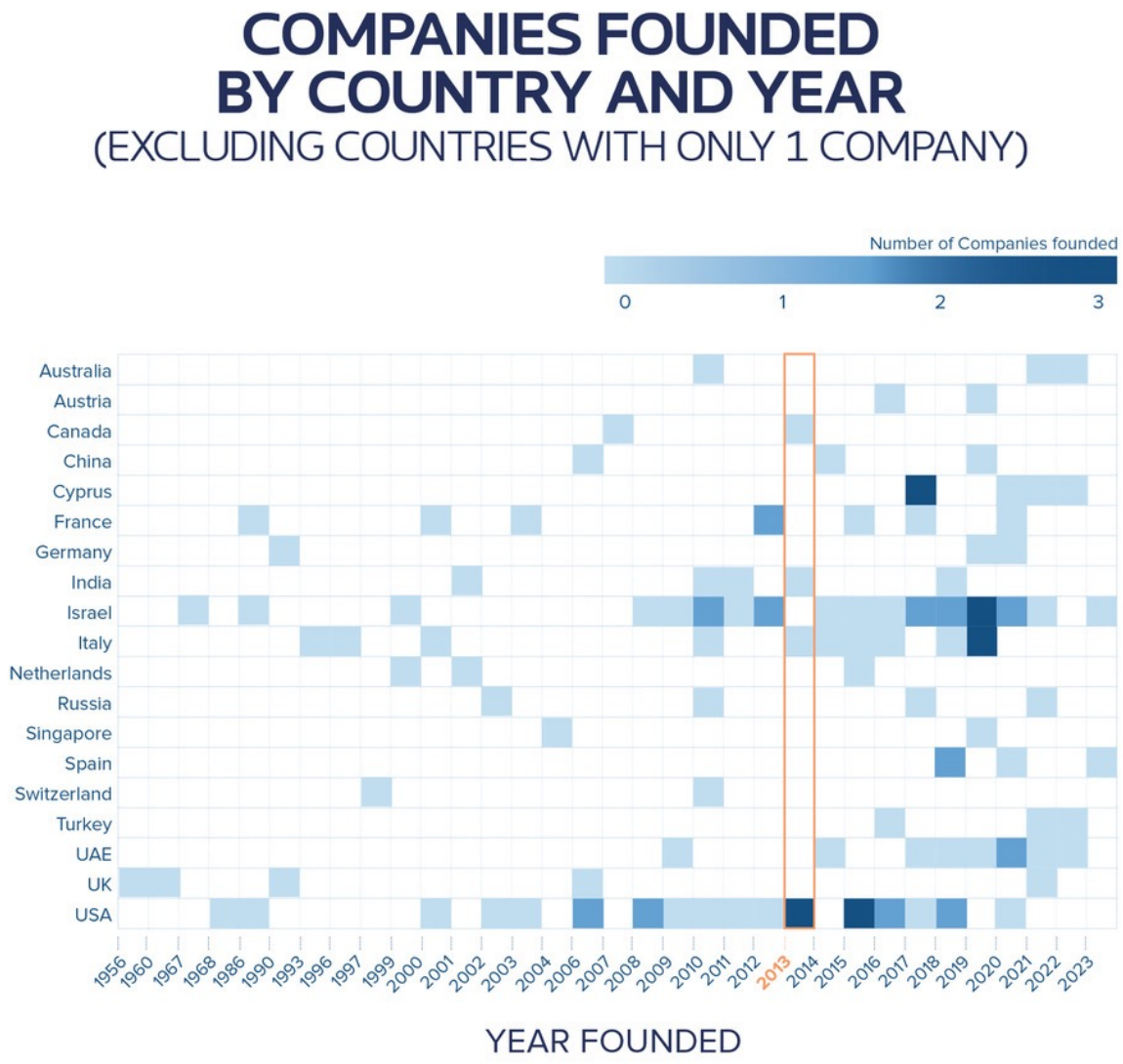
Economy of spycorps: temporality



Economy of spycorps: 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

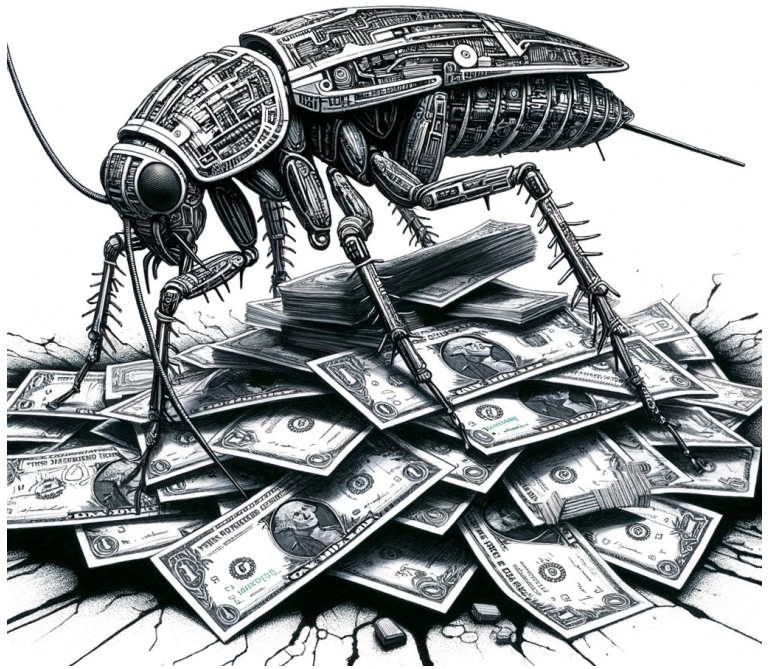


Economy of spycorps

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.



Beyond spycorps

Quarkslab

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

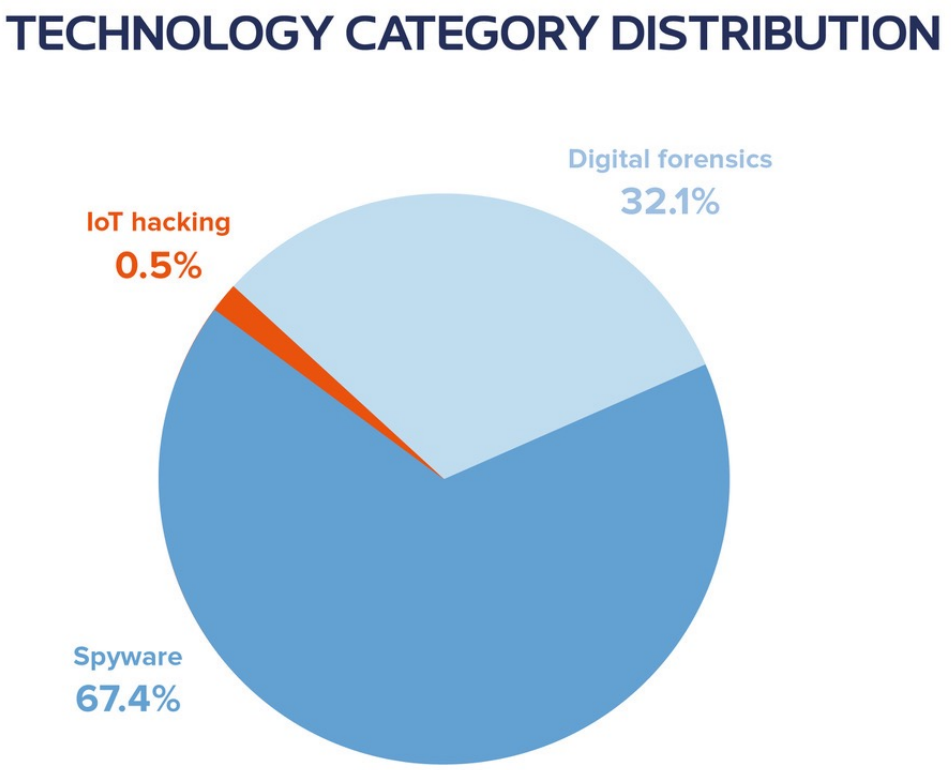
Copy to clipboard

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

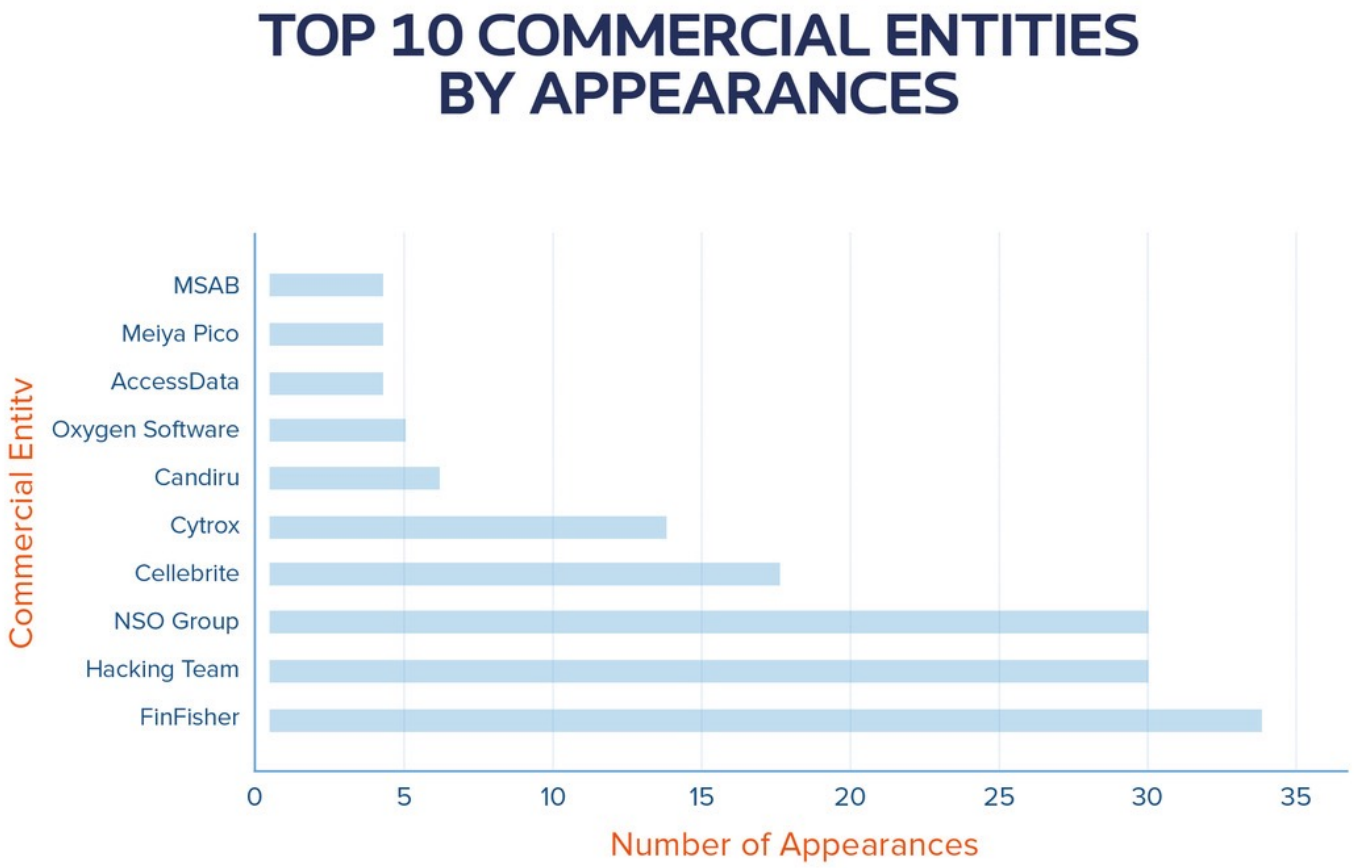
Categories

3 categories

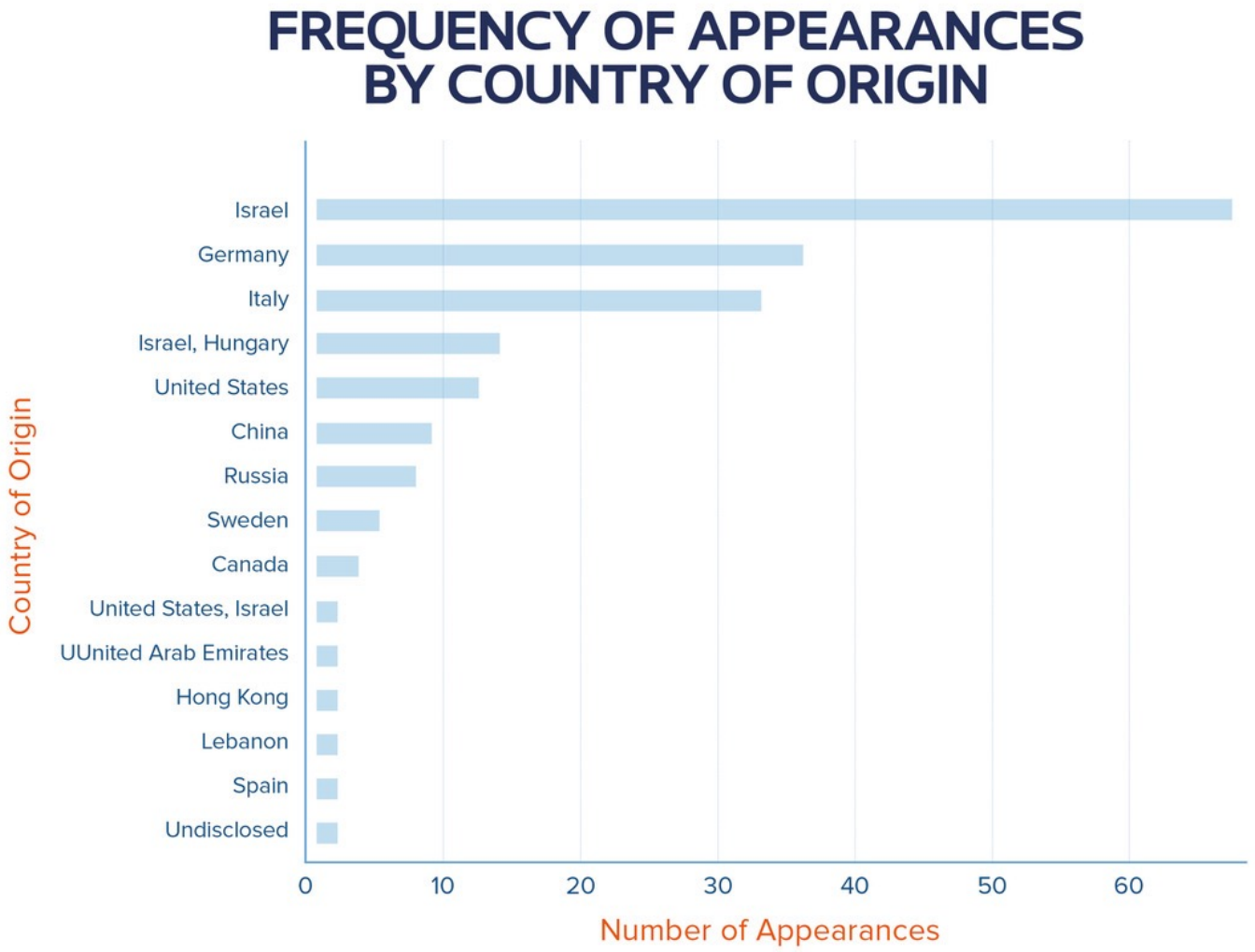
- Spyware: what we talked about so far
- Digital Forensic: requires a physical access to a device BUT allow to dig into erased files on the whole device
- IOT Hacking: Allow clients to locate security cameras, hack into them, watch their live feed a even alter it



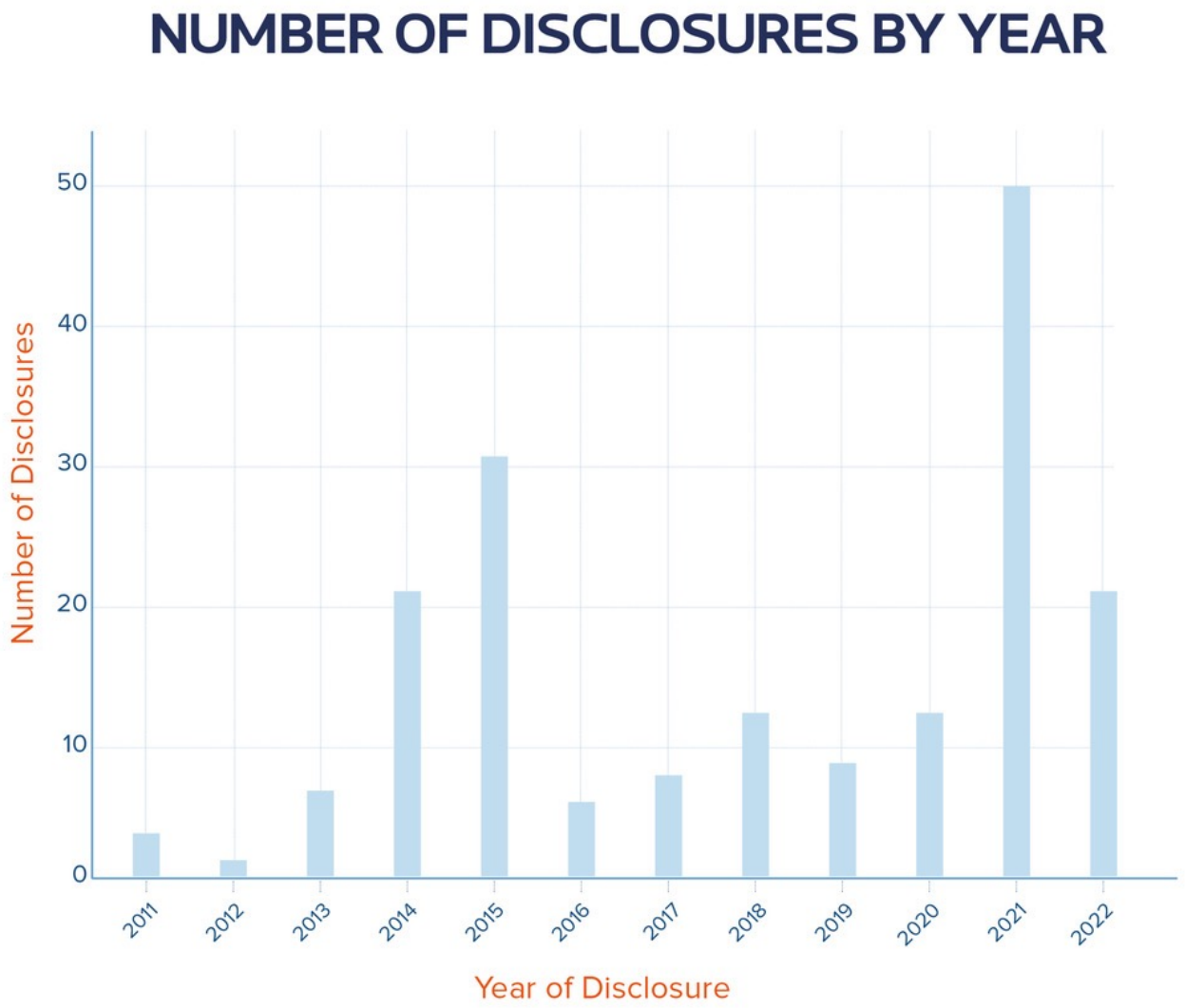
Disclosed business winners



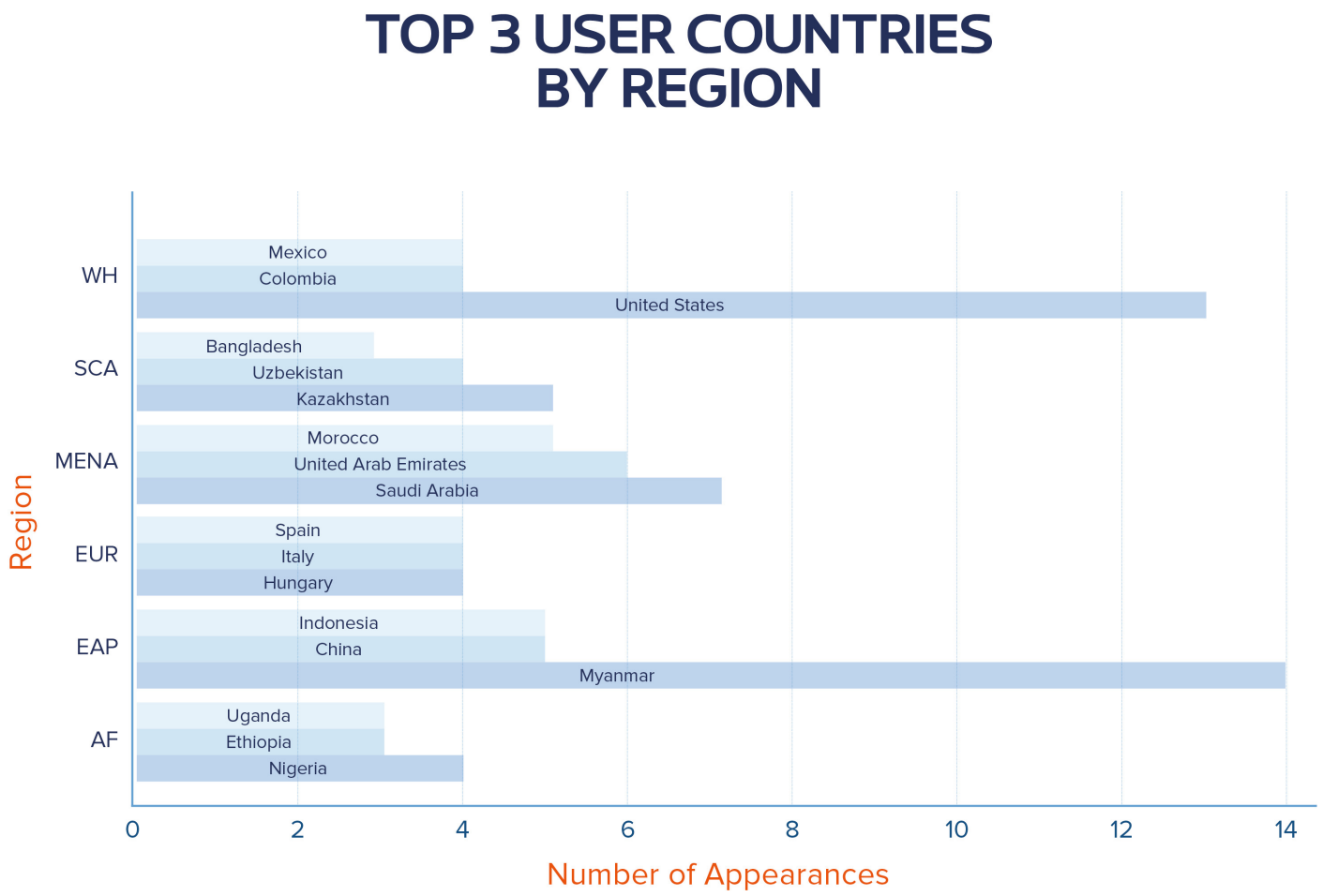
Business winners per country



Disclosure per year



Top 3 of geography of disclosures per region



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

sekoia | **Countries deduced from Lycantrox domain names**

Note: They may not be customers of Cytrox/Intellexa

sekoia | **Potential Predator users deducted from the newly discovered infrastructure**

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 🇺🇸 negotiated an exception for research purposes in Dec. 17
  - Israel 🇮🇱 is not in the agreement and has its own system of authorizations, governed by its national security and diplomacy.
  - China 🇨🇳 is not in the agreement: they control and use cyber
  - Russia 🇷🇺 is a member, but not Belarus 🇧🇾.

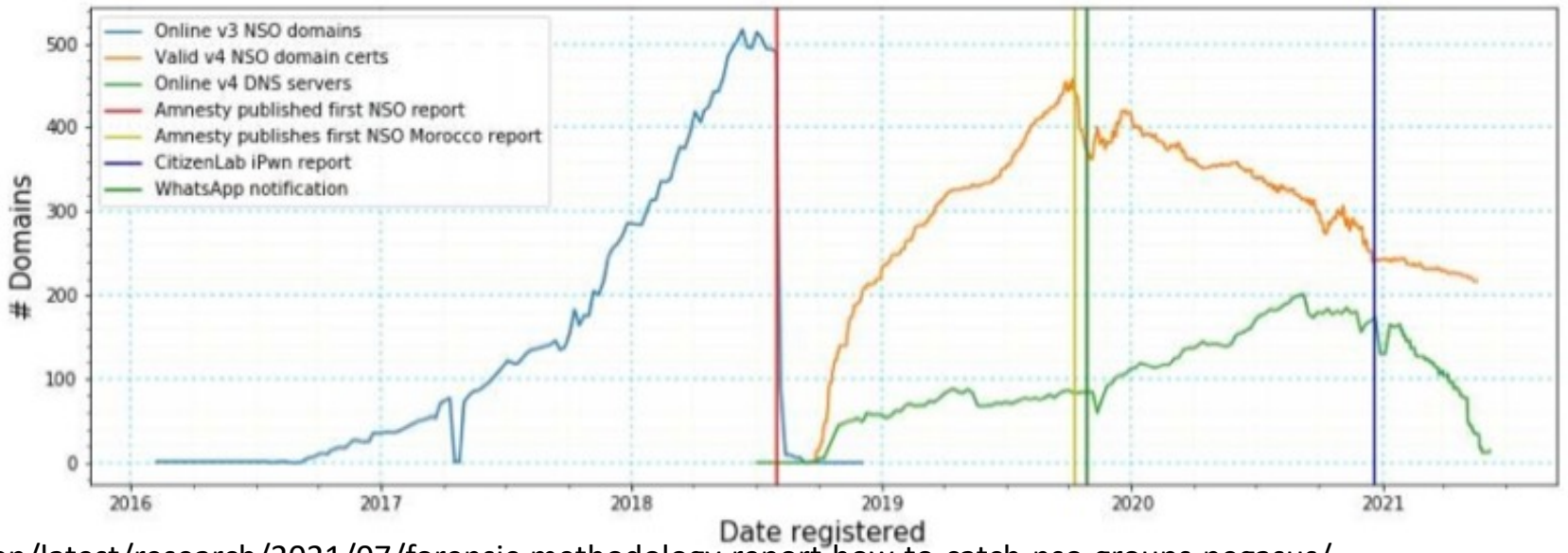
- A new initiative, **Pall Mall Process**, has just been launched in March 2024.
  - Mix of government, companies and NGOs

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



https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/

Spycorps are like cockroaches?

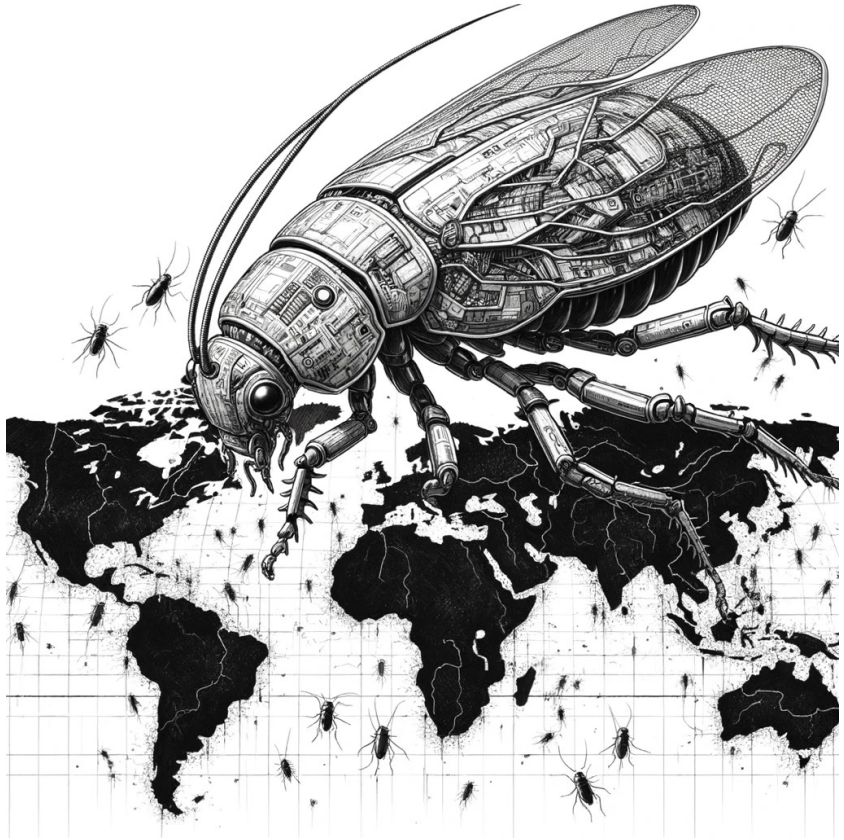
Why are they so resistant?

- 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”

Conclusion

Quarkslab

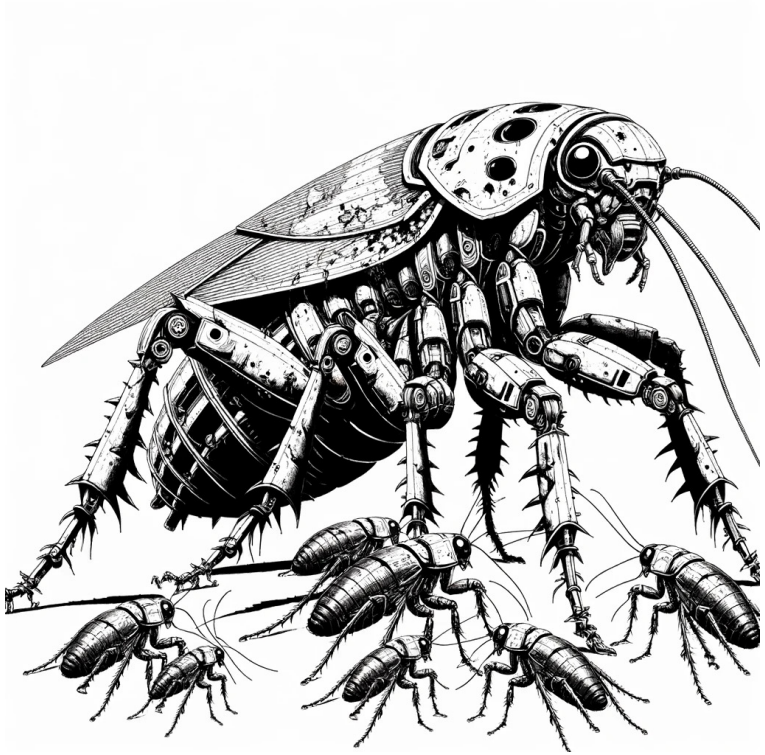
Cyberweapons: a business as usual … for influence



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



My (pappy's) code

25+ years in cyber, I have the same simple code of conduct almost from day 1

```
try:
  # If I don't know where/how it will be used, it stinks
  rule1="Never do something illegal"

  # There are countries or companies for which I (hence Quarkslab) will not work
  rule2="Never do something against my own ethic"

  do_cyber(rule1, rule2)

except IllegalError:  # Civil exceptions eventually, never gov related
  if pedo, ransomware, … do_cyber("", rule2)
except EthicalError:
  print(rule2)
except:
  exit(COMPLICATION OVERFLOW)
```

Thank you ☺

Fred Raynal – fraynal@quarkslab.com
https://www.linkedin.com/in/fredraynal/

Quarkslab