The boom, the bust, the adjust and the unknown

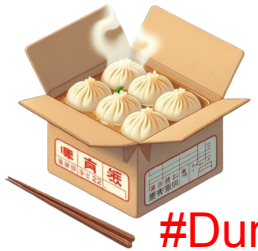
ZERO CON

About me - Maor Shwartz

I’ve been part of the offensive cyber industry for more than 8 years now (side note, the offensive cyber industry is ~20 years old).

My roles have included helping researchers, companies, research groups, brokers, and governments to navigate the offensive cyber industry from a supply-chain (vulnerabilities/researchers) standpoint.

Twitter: @malltos92



#DumplingsLife

Tl;dr - The offensive cybersecurity industry in the near-mid term future

- End to end companies will have to “pick a side” - either working only with the US/EU or to only work with the rest of the world
  - Some End to end companies will go bankrupt
  - Some End to end companies will be put on the US and EU sanction list
- Individual people in the offensive cybersecurity industry will be put on the US and EU sanction list -> already happened (!!)
- Over supply - In the next year we are going to see a lot of researchers and research groups trying to sell their inventory on the market
- The supply chain is going to experience a second shock wave - this time is from the demand side
  - Some of the clearing houses and research groups will go bankrupt
  - There are more high-end researchers that are looking for a job than ever before

Tl;dr - The offensive cybersecurity industry in the near-mid term future

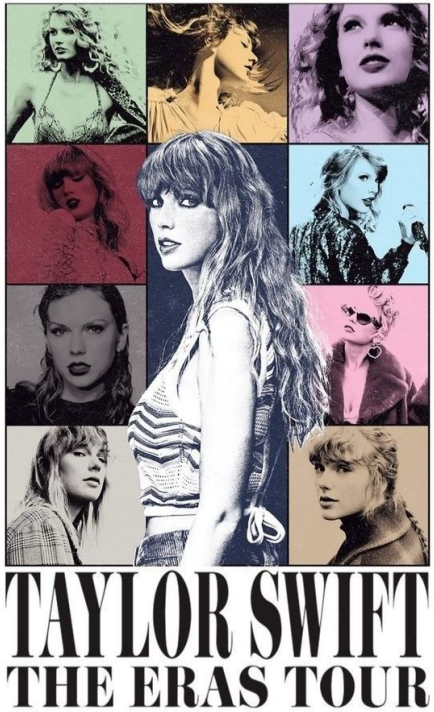
- There are going to be researchers with items in hand that they can't sell
  - Prices for vulnerabilities and exploits will decrease
- Due to export control regulations - governments will have to stop operations outside their own country (i.e research hubs / shell companies)
- Clearing houses and research groups will take less risk and reduce research speculation (i.e pivoting to research on items that sold upfront)
- Clearing houses and research groups will not maintain chains - back to the item era
- Clearing houses and research groups will pivot away from traditional 1click solutions (mostly on the speculation side)

How did we get there?

The ripple effect

Agenda (the eras)

- Introduction to the offensive cybersecurity market
- ~~The transition from community to industry~~
- ~~The boom (2017–2019)~~
- ~~The bust (2020–2021)~~
- The adjust (2022-2024)
- The unknown (2024+)



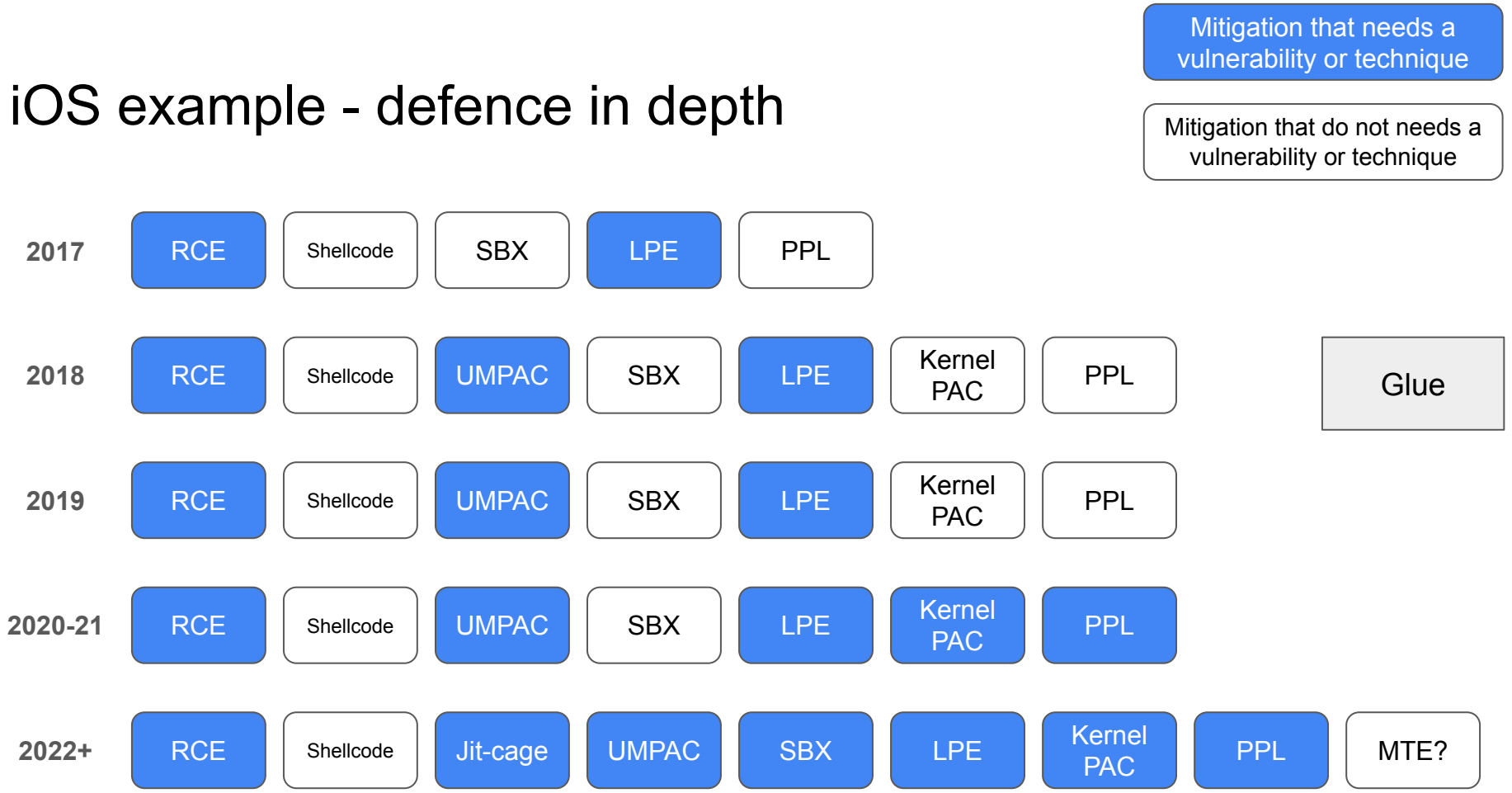
The vendors

The vendors

In the context of offensive cybersecurity, the vendors have two main goals:

- Make their products more secure
- Disrupt the offensive cybersecurity industry operations
  - “In the wild“
  - Naming names and attribution
  - Working with NGOs and potential victims directly

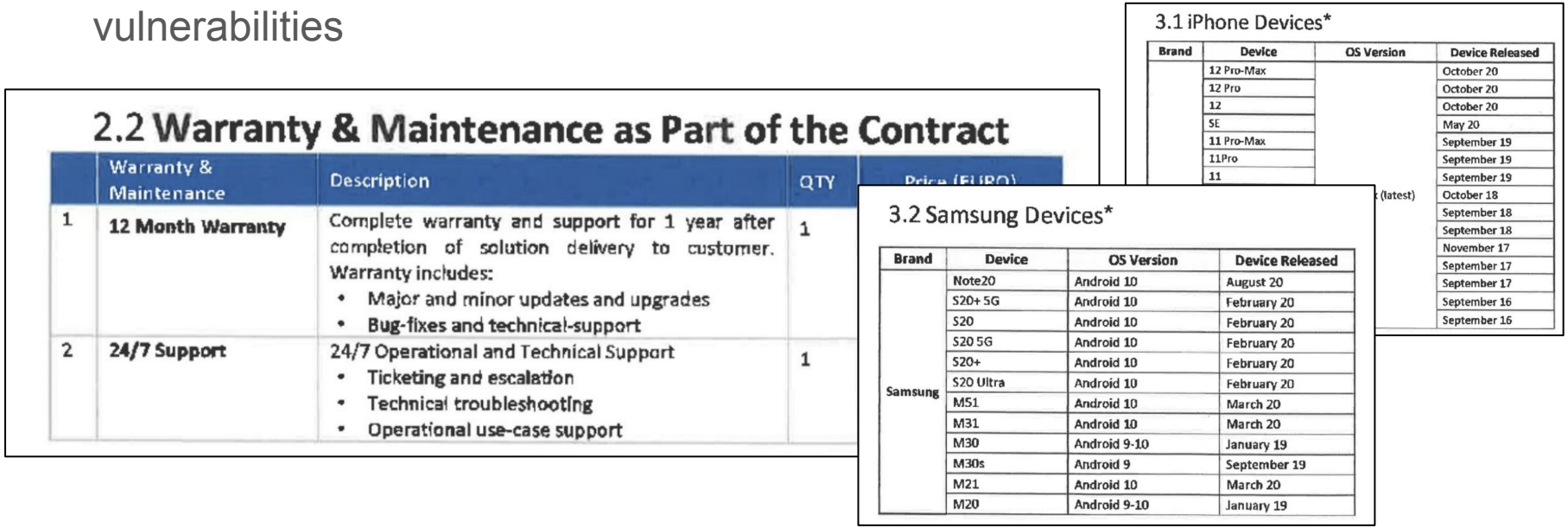
iOS example - defence in depth



End to end companies - side notes

Service Level Agreement (SLA)

- In the offensive cyber industry, SLA means that the company has the ability to infect and install the agent on the target device -> chains / exploits / vulnerabilities



2.2 Warranty & Maintenance as Part of the Contract

	Warranty & Maintenance	Description	QTY	Price (EURO)
1	**12 Month 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	
2	**24/7 Support**	24/7 Operational and Technical Support • Ticketing and escalation • Technical troubleshooting • Operational use-case support	1	

3.1 iPhone Devices*

Brand	Device	OS Version	Device Released
	12 Pro-Max		October 20
	12 Pro		October 20
	12		October 20
	SE		May 20
	11 Pro-Max		September 19
	11Pro		September 19
	11		September 19
		(latest)	October 18
			September 18
			September 18
			November 17
			September 17
			September 17
			September 16
			September 16

3.2 Samsung Devices*

Brand	Device	OS Version	Device Released
Samsung	Note20	Android 10	August 20
	S20+ 5G	Android 10	February 20
	S20	Android 10	February 20
	S20 5G	Android 10	February 20
	S20+	Android 10	February 20
	S20 Ultra	Android 10	February 20
	M51	Android 10	March 20
	M31	Android 10	March 20
	M30	Android 9-10	January 19
	M30s	Android 9	September 19
	M21	Android 10	March 20
	M20	Android 9-10	January 19

Sources of revenue

- Different types of end-to-end companies:
  - Companies that sell to the five-eyes (Australia, Canada, New Zealand, the United Kingdom, and the US).
  - Companies that sell to five-eyes and Schengen (EU).
  - Companies who sell to “Western countries”.
  - Companies who sell to countries that are not part of the US sanction list.
- End-to-end companies’ core revenue stream is based on the last category.
  - “Western countries” have internal research and operation capabilities - willing to pay less
  - Rest of the world - need access to the technology they can’t develop internally - pay more, a lot more

Supply Chain

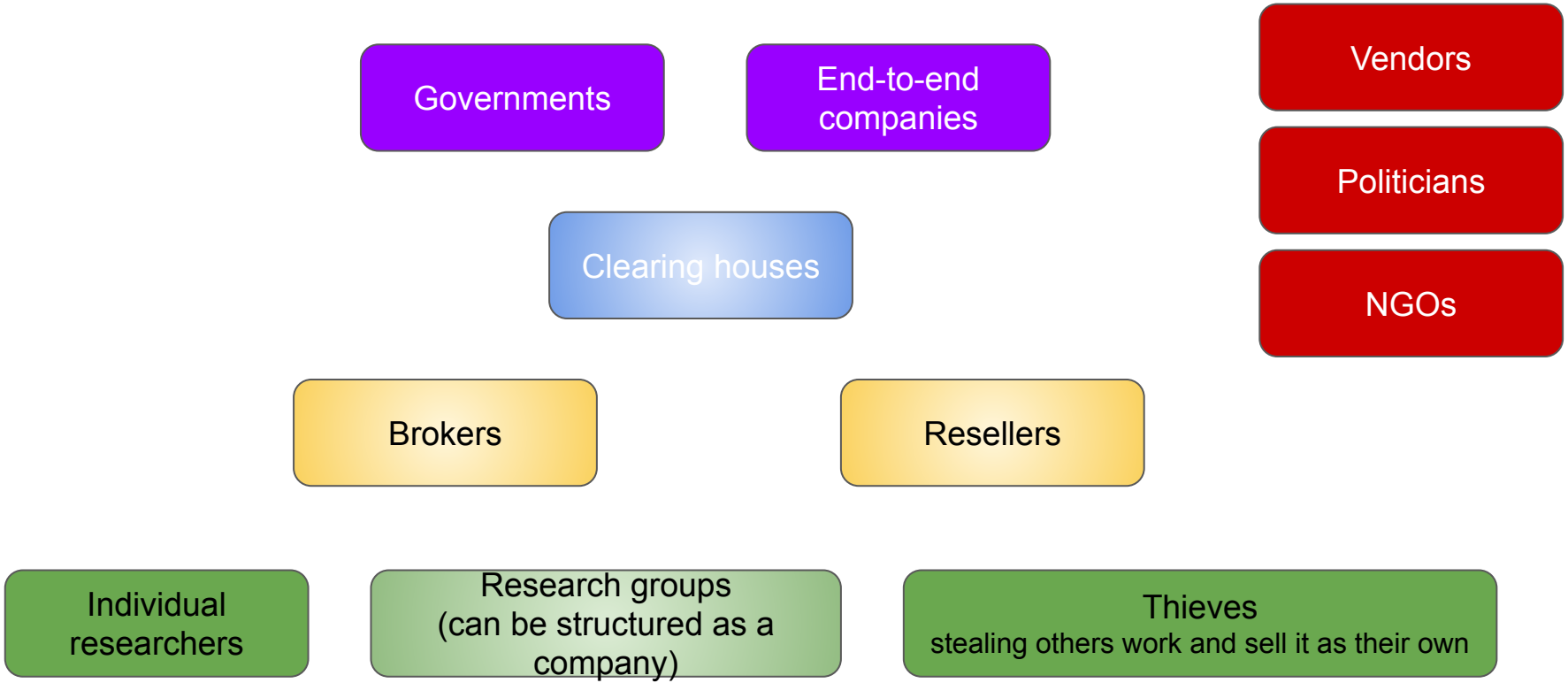
Exploits vs. vulnerabilities

Supply chain will only get paid by milestones if the vulnerability is not patched, the exploit is working and updated to the latest production version

- Acceptance, 30/60/90/120 days
- The burden of maintaining the exploit is transparent to the end client.
- Write a new exploit from scratch

The bust
2020–2021

Dominante entities in this phase



Regulation, media and NGOs

Regulations

- Tightening regulations on exporting products and knowledge (i.e. vulnerabilities and exploits).
- Limiting end-to-end companies from marketing and selling their products in certain regions without the regulator’s approval.
- Companies were added to the US sanctions list.
- Vendors launched lawsuits against end-to-end companies that violated their terms and conditions.

Cyber warfare + Add to myFT

Cyberweapon manufacturers plot to stay on the right side of US

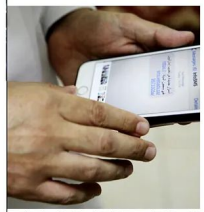
Contrasting fates of Israeli spyware-makers Paragon and NSO reveal how American support is crucial in $12bn industry

Mehul Srivastava in London

Report: Israel nixed QuaDream's spyware deal with Morocco, leading to firm's closure

Haaretz says the Defense Ministry cracked down on company's sales of cellphone hacking software overseas, following global fallout from similar NSO Group activity

By TOI STAFF



poor shows Associated Press journalists a screenshot of a spoof Ajman, United Arab Emirates, August 25, 2016. (AP Photo/Jon

LAW AND JUSTICE | GERMANY

Germany charges executives for selling spyware to Turkey

7 hours ago

Four former executives have been charged with illegally selling software to Turkey's secret services so it could spy on the country's opposition. The suspects are from the Munich-based FinFisher which develops spyware.

German authorities have filed charges against four suspects from a firm over allegations that they sold surveillance software to **Turkey's intelligence services**, Munich prosecutors said on Monday.

Prosecutors say the suspects intentionally violated licensing requirements for dual-use goods by selling **surveillance software** to non-EU countries.

The accused — from the Bavarian-based FinFisher — have been charged with commercial violations of the German trade and payments act in three separate cases.

US blacklists Israeli firm NSO Group for use of spyware

By Sean Lyngaas, CNN Business

Updated 11:57 AM EST, Mon No

WASHINGTON, Nov 3 (Reuters) - The U.S. Commerce Department added Israel's NSO Group and Candiru to its trade blacklist on Wednesday, saying they sold spyware to foreign governments that used the equipment to target government officials, journalists and others.

Designations of Persons Operating in Russia's Technology and Electronics Sectors

Russia's defense industry is reliant on imported micr
domestically and imported from abroad. Today, Trea
Russia's technology and electronics sectors, includin
tech equipment used by Russia's defense entities.

OFAC today designated the following persons pursua
technology sector of the Russian Federation econom

- **0Day Technologies**, a Moscow-based cybersecu
nation citizens' personally identifiable informati

LAW AND JUSTICE

German prosecutors investigate spyware maker

Samantha Early

09/05/2019

Munich prosecutors have launched a probe into a company accused of illegally selling spy software, German media report. The FinFisher product was reportedly used against opposition protesters in Turkey.

End to end companies

Service Level Agreement (SLA)

- The technology and the level of mitigations implemented by vendors reached maturity.
- Disruptions to the ability of end-to-end companies to uphold the SLA.
- Companies struggling to maintain theirs SLAs led to three main issues:
  - Revenue collection
  - Losing clients to competitors
  - Pressure on the internal research team for solutions
- “In the wild” affect multiple companies in parallel - the use of the same items / techniques

End to end companies - Internal research team

- Proof of Concept (PoC) to “production ready” chains
  - Huge maintenance burden
  - Less time to focus on vulnerability research
    - Only a small percentage of the research team is capable of finding new vulnerabilities
- Strategy shift in the hiring policy
  - Stopped hiring the new generation of researchers
  - Stopped hiring researchers based on “street credit”
- End-to-end companies had struggled to uphold SLA
  - pressure on the internal team / procurement team
  - researchers try to warn that research takes time

Increasing vulnerability prices

The true cost of chains increased dramatically for two main reasons:

- The number of vulnerabilities needed to create a working chain increased (i.e. from RCE and LPE to a combination of multiple vulnerabilities and techniques).
- Finding vulnerabilities and exploiting them got harder and harder.
- In the wild - items were burned faster than they can be produced

Due to regulations and vulnerability export control laws, end-to-end companies had to open entities in many countries to accommodate the transactions with researchers leading to additional costs

Bankruptcy

L3Harris reportedly drops bid for Israeli spyware following U.S. concerns

Jul. 11, 2022 9:50 AM ET | **L3Harris Technologies, Inc. (LHX)** | By: Carl Surran, SA News Editor

The American defense firm L3Harris has ended talks with blacklisted Israeli spyware company, NSO Group, to buy the firm's hacking tools following intelligence and security concerns raised by the Biden administration, according to people familiar with the matter.

MOTHERBOARD
TECH BY VICE

Hacking Team Founder: 'Hacking Team is Dead'

The company's former CEO posted a bizarre obituary on LinkedIn
ing the infamous surveillance firm is "definitely dead."

By Lorenzo Franceschi-Bicchierai

But the demand is here to

The defense ministry's licensing restrictions have sounded the death knell for several smaller shops of hackers and researchers. Nemesis, an Israeli cyber firm that had managed to keep a low public profile, shut down in April. Ace Labs, a spinoff of the billion-dollar tech giant Verint, closed up shop and fired all its researchers earlier this month.

ISRAEL

Wayout and Convexum step back from Israel's struggling NSO Group

artment of Commerce's Bureau of Industry and
st in November last year, the Israeli cybersecurity
increasing financial difficulty, prompting its IoT
-drone subsidiaries to distance themselves. [...]

Set up e
notificat
these to

Berkele
Group

Spyware Vendor FinFisher Claims Insolvency Amid Investigation

- Munich firm accused of helping governments hack activists
- Inquiry into alleged export controls violations ongoing

By Ryan Gallagher
March 28, 2022 at 4:00 PM GMT+9

A loan with a face value of over $300 million that NSO issued in 2019 was trading in November at an all-time low bid of 70 cents on the dollar. It was quoted Monday at a bid of 50 cents on the dollar, according to people familiar with the prices.

Israel's Pegasus Spyware Maker Takes Drastic Measures to Survive Global Scandal

- Maker of Pegasus phone-hack tool has cut jobs and hike
- Firm, now blacklisted in US, is trying to pacify debt holde

By Eliza Ronalds-Hannon and Davide Scigliuzzo
November 4, 2022 at 11:00 PM GMT+9

Embattled spyware maker NSO Group is taking drastic steps to pacify creditors holding around $400 million in debt as it waits out a worldwide political scandal that still threatens its survival.

Blacklisted in the US on accusations its Pegasus phone-hacking tool was used by foreign governments to spy on dissidents, the Israeli company has cut 15% of its workforce and raised prices by about 20% to stem a cash bleed that was expected to run into the tens of millions of dollars this year, according to a person with knowledge of the matter.

Moody's

Search ratings, research, analysis, and more...

HOME | TRENDING | REPORTS | SECTORS & REGIONS | RATINGS & ASSESSMENTS | TOOLS & DATA | EVEN

Moody's
INVESTORS SERVICE

Print | Export PDF

Rating Action: Moody's downgrades NSO to B3 with negative outlook

25 May 2021

Frankfurt am Main, May 25, 2021 -- Moody's Investors Service ("Moody's") has today downgraded the corporate family rating (CFR) to B3 from B2 and the probability of default rating (PDR) to B3-PD from B2-PD of NorthPole Newco S.a r.l. (NSO), the top entity of the restricted group of Israeli-based cyber security and intelligence software provider NSO Group. Concurrently, Moody's has downgraded to B3 from B2 the instrument rating of the $300 million senior secured first lien term loan B1 (TLB1) and €176.96 million senior secured first lien term loan B2 (TLB2) facilities both maturing in March 2025 and the $30 million senior secured revolving credit facility (RCF) maturing in March 2024. The outlook on all ratings remains negative.

RATINGS RATIONALE

Analysis

Israeli cyber is shrinking: from 18 to 6 spy manufacturers within a year

The closure of QuaDream is further evidence of the shrinking of the world-leading Israeli cyber
Israeli companies that were active
in the last year also due to the re
Ministry of Defense. At the same
co

Israel News | National Security & Cyber

Israeli Spyware Maker QuaDream Closes, Fires All Employees

The company, which specializes in software to hack iPhones for governments, halts operations in Israel following investigative report

Save | Zen Read

Bankruptcy

End-to-end companies encountered numerous challenges, including escalating costs, declining revenue, unable to uphold SLA, researchers quitting, increased regulations, and more.

Some of the end to end companies struggled to cope with these difficulties and were unable to effectively manage the financial strain and went bankrupt.

Supply Chain

There would be pain

Supply Chain

- Tightened regulations around vulnerability/exploit export - led some researchers to pivot away from the industry
  - Exporting became illegal altogether in some places
- Higher barrier to enter the field of vulnerability research
  - Cost of devices
  - IDA
  - Emulation (Corellium for example)
  - Without vulnerabilities, researchers can’t search for the next part in the chain.
- Addressable market shrinked
  - Bankrupt end to end companies + regulation
- Clients will not buy parts of the chain unless they have the rest of the pieces
  - Or they are confident enough that they can buy/find them in a short period

Supply Chain

- Products that are in demand were prioritized to the main vectors which are mobile
  - Researchers tried to pivot to mobile without success and ended up leaving the industry.
- Researchers tried to limit the use of their vulnerabilities and exploits by companies
  - Protect the item
- Individual researchers started to group together and created research companies
  - No longer able to achieve the same level of output as they did in the past
- Researchers that worked in end to end companies left to research groups or started their own venture

Brokers

Brokers

- Governments and end to end companies started to work openly in the industry
- High markups
- Misled researchers by claiming to have sold the item only once, when in reality, they sold it multiple times without informing the researchers
- Limited pool of vulnerabilities and exploits that circulated among a wide range of brokers
    - Clients became hesitant to purchase these vulnerabilities and exploits

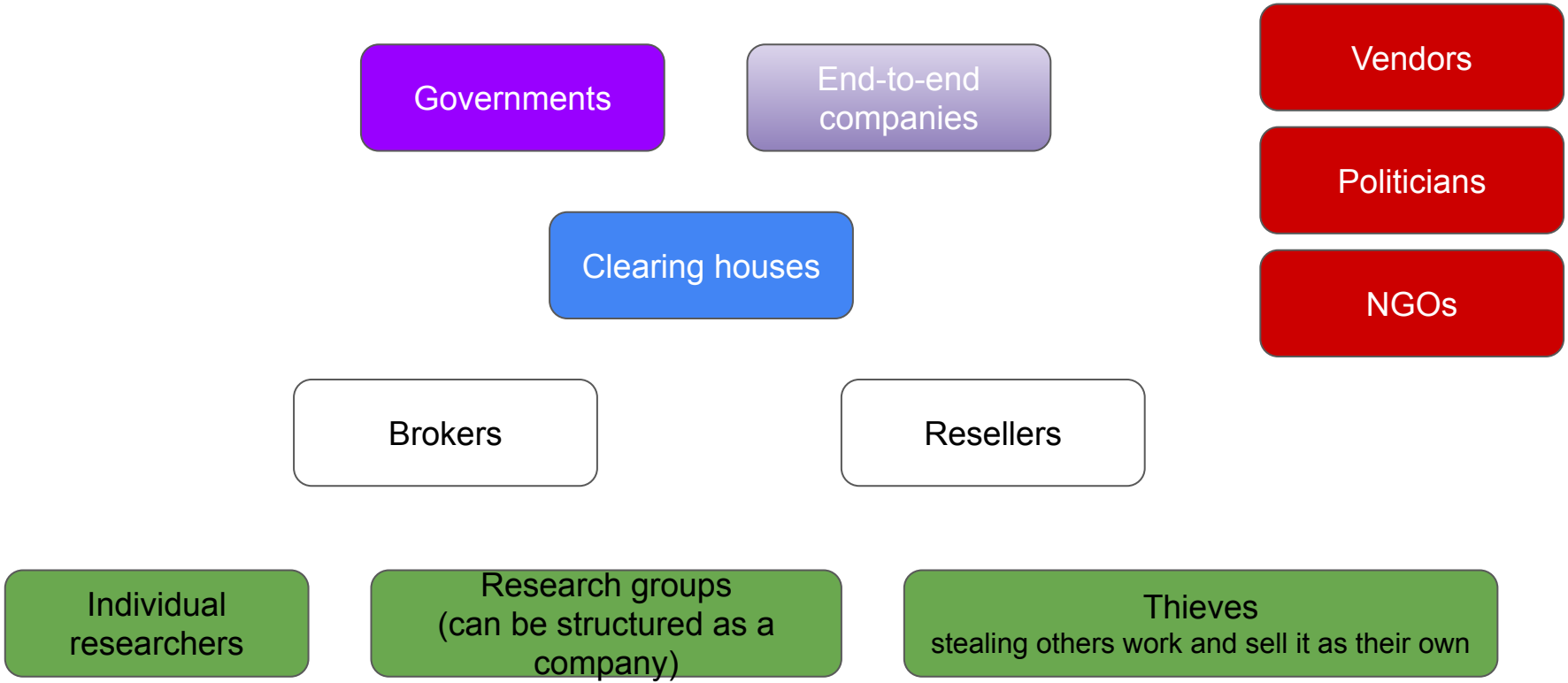
1. Item name : XXX - Preauth RCE
2. Vendor Homepage: XXX
3. Vulnerable Software: XXX
4. Asking Price and availability of exclusive acquisition : XXX
5. Affected OS: *unix
6. Vulnerable Target application versions and reliability. If 32 bit only, is 64 bit vulnerable?
List complete point release range.
_____
7. Tested, functional against target application versions, list complete point release range. XXX (Latest)
Explain _____
8. Does this exploit affect the current target version?
[x] Yes
[ ] No
9. Targets can be found with google dork/shodan/censys?
[x] Yes
[ ] No
10. Privilege Level Gained
[ ] As logged in user (Select Integrity level below for Windows)
[ ] Web Browser's default (IE - Low, Others - Med)
[ ] Low
[ ] Medium
[ ] High
[x] Root, Admin or System
[ ] Ring 0/Kernel
[ ] Other

Main takeaways

- Harder to find vulnerabilities and maintain full chians
- The offensive cybersecurity industry shrinked
  - Bankrupt end to end companies
- Regulations on both end to end companies and vulnerability export increased
  - The US sent message to the world by adding end to end companies to the sanction list
  - L3 - NSO merger canceled
- The roles of brokers and resellers went obsolete
  - Governments and end to end companies started to work openly
- Researchers started to group together

The adjust in the supply side 2022-2024

Dominante entities in this phase



Regulation, media, NGOs and politicians

Regulation, media, NGOs and politicians

Journalists and NGOs targeting end-to-end companies, their clients, operations and targets.

NGOs worked with people that were targeted with end to end companies solutions.

NGOs works closely with the vendors to analyze victims phones.

Politicians started to publicly speak about the harm of using end to end services against non-criminal targets.

Companies were added to the US sanctions list.

End to end companies

End to end companies

- Despite the reduced number of end-to-end companies, they continue to compete with each other in the market and are having a hard time keeping their SLA.
- More companies went bankrupt or pivot away.
- Harder to get the regulator approval for selling the services to new clients
- Only a handful of end to end companies operates in the industry.

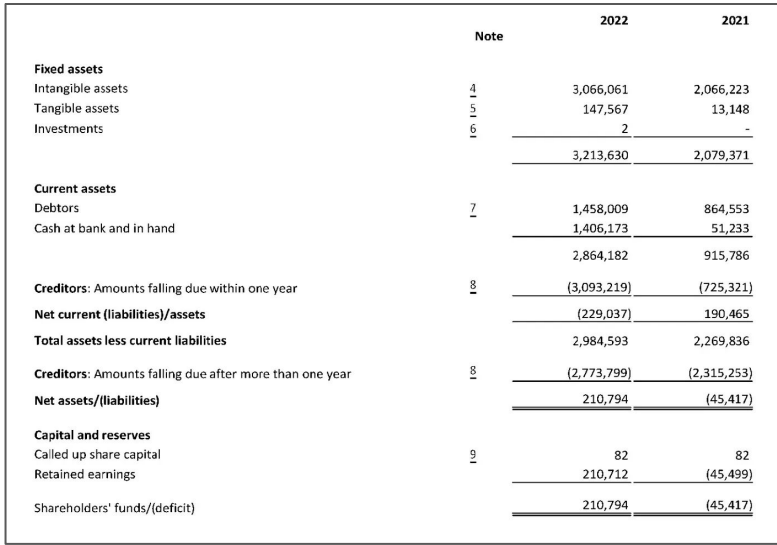
Reshape of the supply chain

Supply chain - from individuals to research groups

- As technology mature, finding vulnerabilities became increasingly challenging -> the solution, research companies.
  - Longer time to provide the same output they had in the past.
  - Needed a team and six months to achieve the same outcome.
- Researchers that used to work for end to end companies started their own research teams / joined research groups
  - Wanted to make more money
  - No need to work on others work (“PoC to production”)
  - Focus on research

Supply chain - Research groups

- The researchers who left the end to end companies, usually already had vulnerabilities in mind based on the experience of their older work
  - Quick way to get paid once you opened a company
- Small research groups are usually in the magnitude of up to 8 researchers with a revenue of a few million USD a year.



	Note	2022	2021
Fixed assets			
Intangible assets	4	3,066,061	2,066,223
Tangible assets	5	147,567	13,148
Investments	6	2	-
		3,213,630	2,079,371
Current assets			
Debtors	7	1,458,009	864,553
Cash at bank and in hand		1,406,173	51,233
		2,864,182	915,786
Creditors: Amounts falling due within one year	8	(3,093,219)	(725,321)
Net current (liabilities)/assets		(229,037)	190,465
Total assets less current liabilities		2,984,593	2,269,836
Creditors: Amounts falling due after more than one year	8	(2,773,799)	(2,315,253)
Net assets/(liabilities)		210,794	(45,417)
Capital and reserves			
Called up share capital	9	82	82
Retained earnings		210,712	(45,499)
Shareholders' funds/(deficit)		210,794	(45,417)

Supply chain / brokers

Control over transaction: difficulty of finding vulnerabilities + shorter lifespan = the need of greater control over transactions

Forcing brokers to pivot from the traditional role of gatekeepers to agents.

- The broker does not see the item, only creates the environment to the transaction
- Compensation based on success

Supply chain - Not all 

Pushback from end-clients as vulnerabilities patched quicker

Researchers couldn't maintain the exploit or the vulnerability got patched before the last milestone

High risk in high risk environment

Supply chain / end clients

Paid R&D: Research group need to be self-sponsorship for an extended period before discovering a sellable vulnerability.

In an industry already characterized by high risks and rewards, research teams sought to mitigate their risks by pursuing paid R&D projects.

Under this arrangement, potential clients would offer a base salary along with a success bonus.

From the client's perspective, small capital risk throughout the project's duration. In return, if the research team successfully identifies and exploits a vulnerability, the client gains exclusive access to it.

The rise of the “Clearing houses”

The rise of the “Clearing houses”

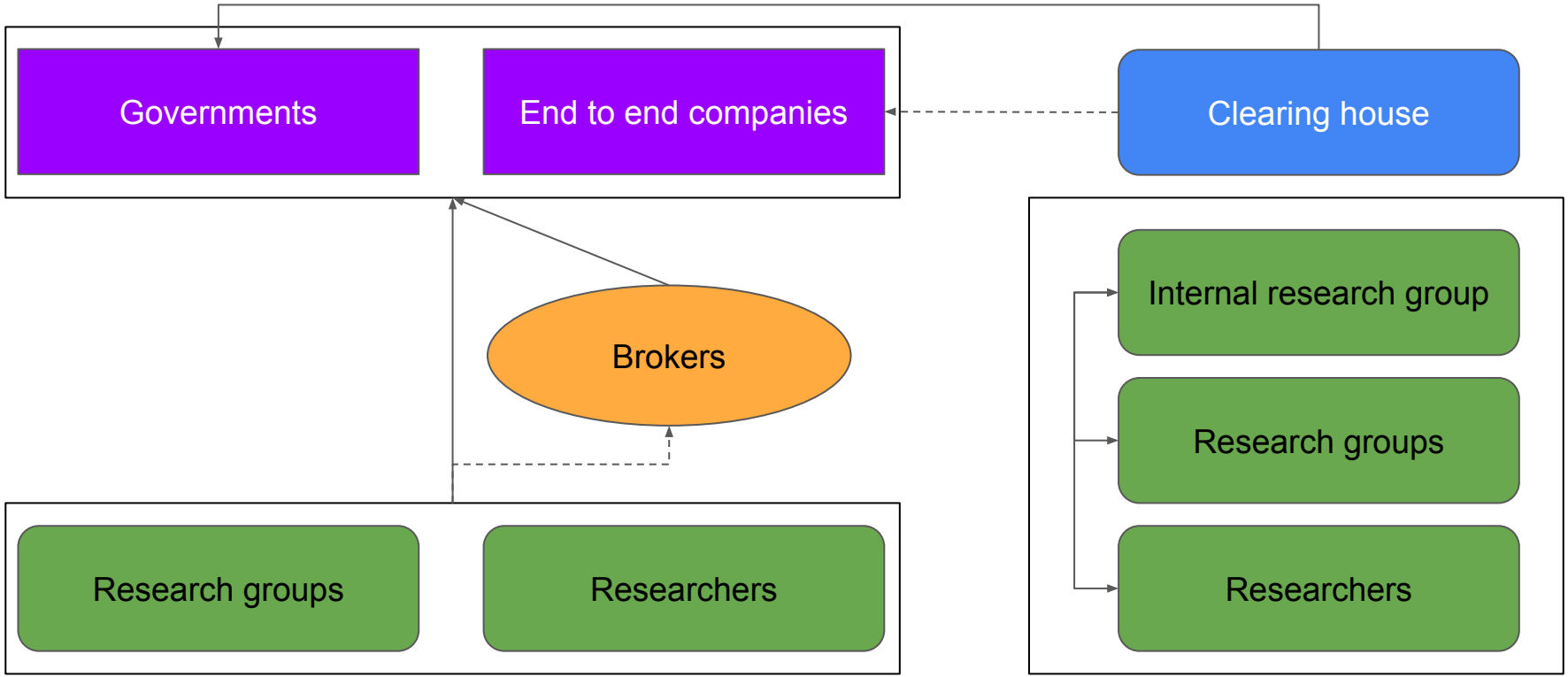
Clearing houses are a new type of entity focusing only on vulnerability research.

- Strong brand name within the industry.
- Own internal research team where they hire high-end or capable researchers to work exclusively for them and exclusively on vulnerability research.
- Secure an exclusive supply-chain of researchers work and vulnerabilities or exploits by investing in paid R&D projects.
- Buys vulnerability from the market exclusively and improve them to be “production ready”.

The rise of the “Clearing houses”

- Share infrastructure, vulnerabilities, exploitation techniques and more with the researchers within the company and researchers that work exclusively with the company
- Compensate researchers and their supply chain, mostly based on success bonuses which are significantly higher than market rates and relatively low base salary
- Work, mostly, with governments
- Prioritization of capabilities over maximizing profits
    - Work with reliable clients that won’t burn the items - opsec
- Don’t need to maintain SLA

Clearing houses role in the supply chain



The rise of the “Clearing houses”

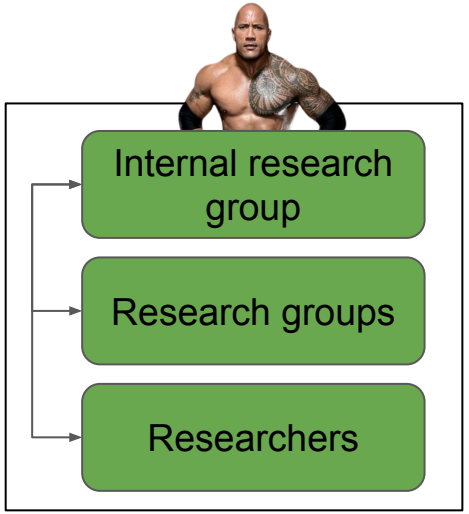
- Replacing some of the end-to-end liquidity in the market
  - End-to-end companies face additional challenges - competing with Clearing houses
- Clearing houses employee quite a lot (I would say more than 15) researchers and exclusive supply chain.
- Their magnitude is usually within the tens of millions USD.

Income Statement 3, Income Statement		
A) Production value		
1) sales and performance revenue	16,880,414	14,641,447
2) changes in inventories of work in progress, semi-finished and finished products	0	(270,000)
3) variations in work in progress under order	0	0
4) additions of fixed assets for internal works	0	0
5) other income and receipts		
contributions for the financial year	452,579	0
Other	485	82,781
Total other income and receipts	453,064	82,781
Total production value	17,333,478	14 454 228
B) Production costs		
6) raw materials, consumables and of goods	166,422	133,474
7) for services	12,125,792	8,929,938
8) for use of property of third parties	104,786	61,098
9) for staff		
a) wages and salaries	621,029	24,479
b) social security contributions	115,193	5,544
c) end-of-relationship treatment	48,553	1,190
d) pension and similar treatment	0	0
e) other costs	380	0
Total personnel costs	785,155	31,213
10) depreciation and amortization		
a) depreciation of intangible assets	2,331	691
b) depreciation of tangible fixed assets	21,310	2,424
c) other write-downs on fixed assets	0	0
d) write-downs on loans and advances and cash	0	0
Total depreciation and amortization	23,641	3,115
11) changes in inventories of raw materials;subsidiaries, consumer and goods	0	0
12) provisions for risks	0	0
13) other provisions	0	0
14) miscellaneous operating charges	402,532	11,118
Total production costs	13,608,328	9,169,956
Difference between value and production costs (A - B)	3,725,150	5,284,272
C) Financial income and charges		
15) income from participating interests		
from subsidiaries	0	0
by affiliated undertakings	0	0
by parent undertakings	0	0
by undertakings under the control of parent companies	0	0
Other	0	0
Total income from participating interests	0	0
16) other financial income		
(a) claims on fixed assets of controlled undertakings	4,225	0
by affiliated undertakings	0	0
by parent undertakings	0	0

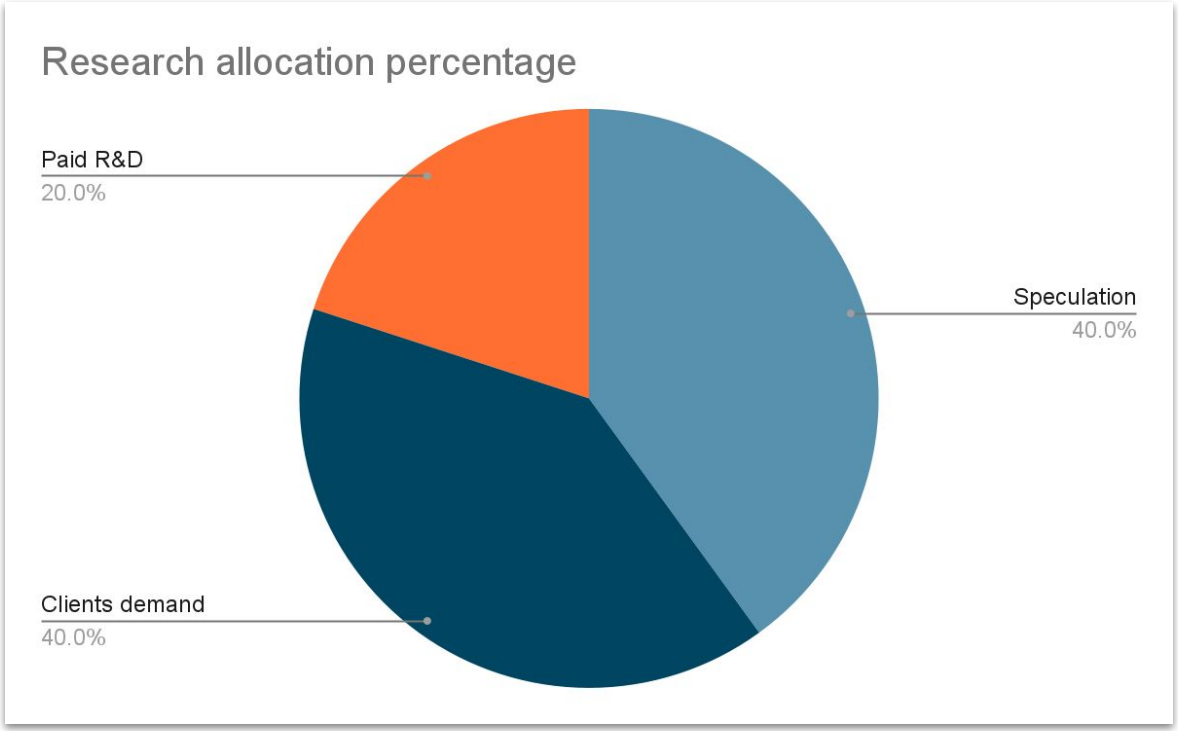
Clearing houses -  the risk

The clearing house management need to play a risky game

- Anticipate the clients demand
- Create teams that can work together
- Allocate researchers to specific research projects
- Develop expertise in new vectors
- Secure funds from end-clients in paid R&D
- Speculation / reinvestment in future research projects
- Make sure the researchers are happy + make profit
    - Agree on the terms before a sale - the clearing house is “holding the bag”



Clearing houses



Main takeaways

The significant technological and security advancements made by vendors had a profound impact on the supply side.

The supply chain had to reinvent itself in order to adopt to the new environment

- Research groups
- Clearing houses
- Paid R&D
- Working exclusively with end client

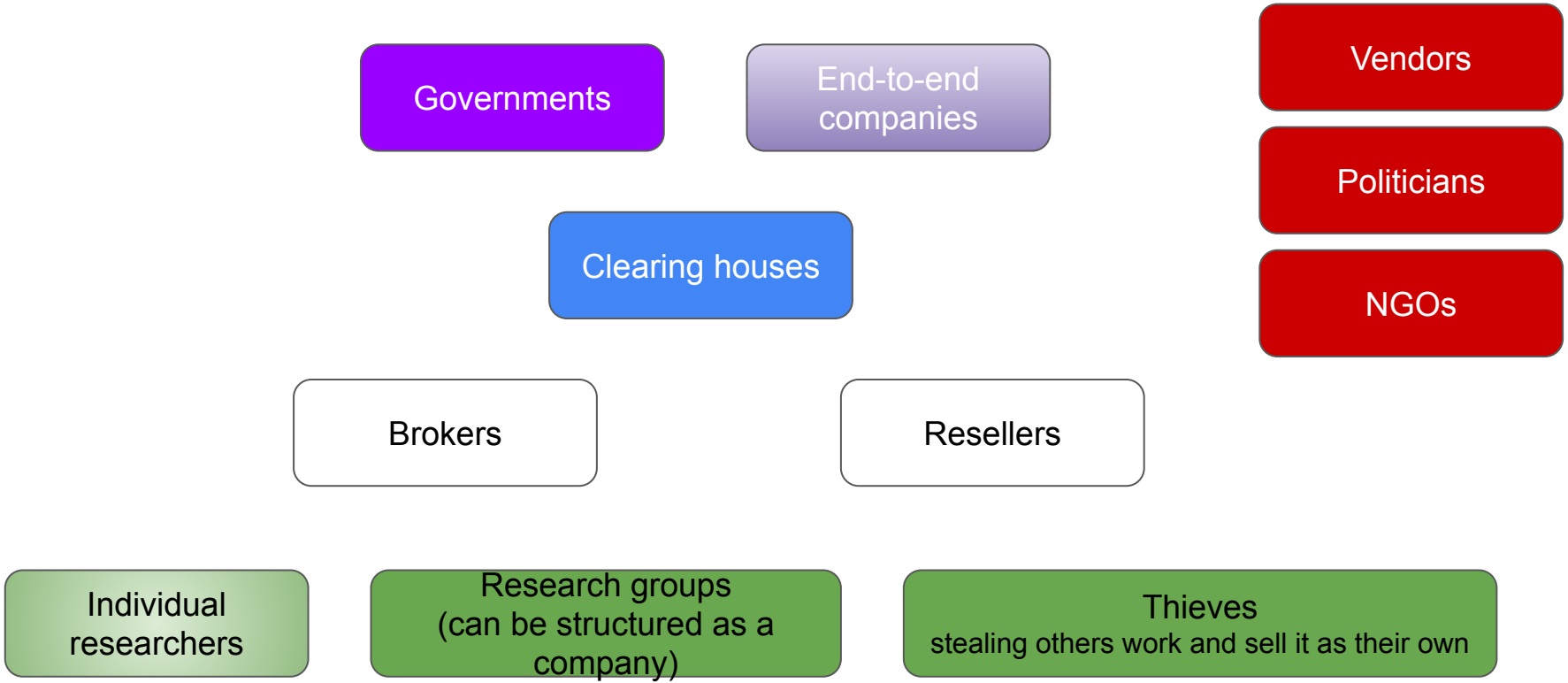
Brokers - a thing of the past

It worked, the supply chain was able to meet (~) demand and adopt

The unknown 2024+

The year of the moat

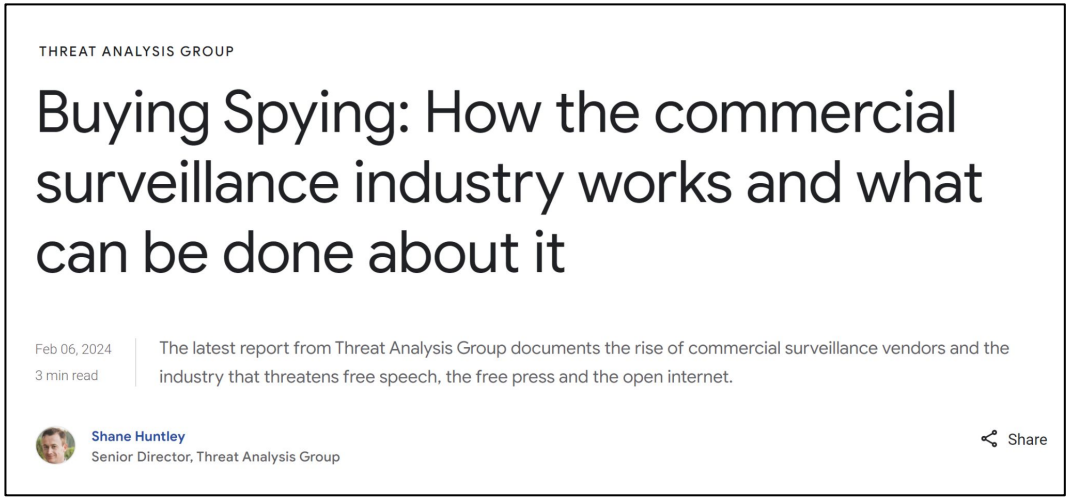
Dominante entities in this phase



Vendors, regulation, media, NGOs and politicians

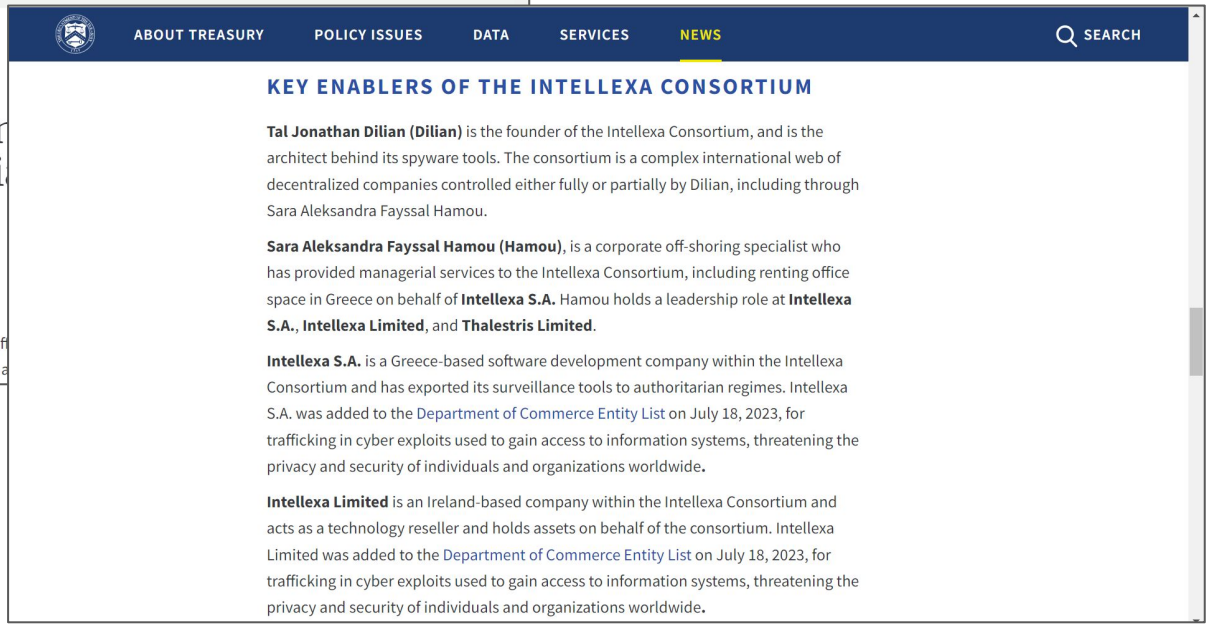
Vendors, regulation, media, NGOs and politicians

Crackdown on end-to-end companies and enabling new policies and tools that can impact greatly on the offensive cybersecurity industry as a whole



Disrupt the offensive cybersecurity industry operations

Vendors, regulation, media, NGOs and politicians



Disrupt the offensive cybersecurity industry operations

Business

US restricts exports to Canada's Sandvine over Egypt censorship

By **Karen Freifeld**

February 27, 2024 3:31 AM GMT+9 · Updated 13 days ago

WASHINGTON, Feb 26 (Reuters) - The U.S. on Monday placed Canada-based Sandvine Inc on a trade restriction list for allegedly helping the Egyptian government target human rights activists and politicians.

Disrupt the offensive cybersecurity industry operations

Featured Article

Spyware startup Variston is losing staff — some say it's closing

The Barcelona-based startup's malware has been used to target iPhones, Android devices and PCs

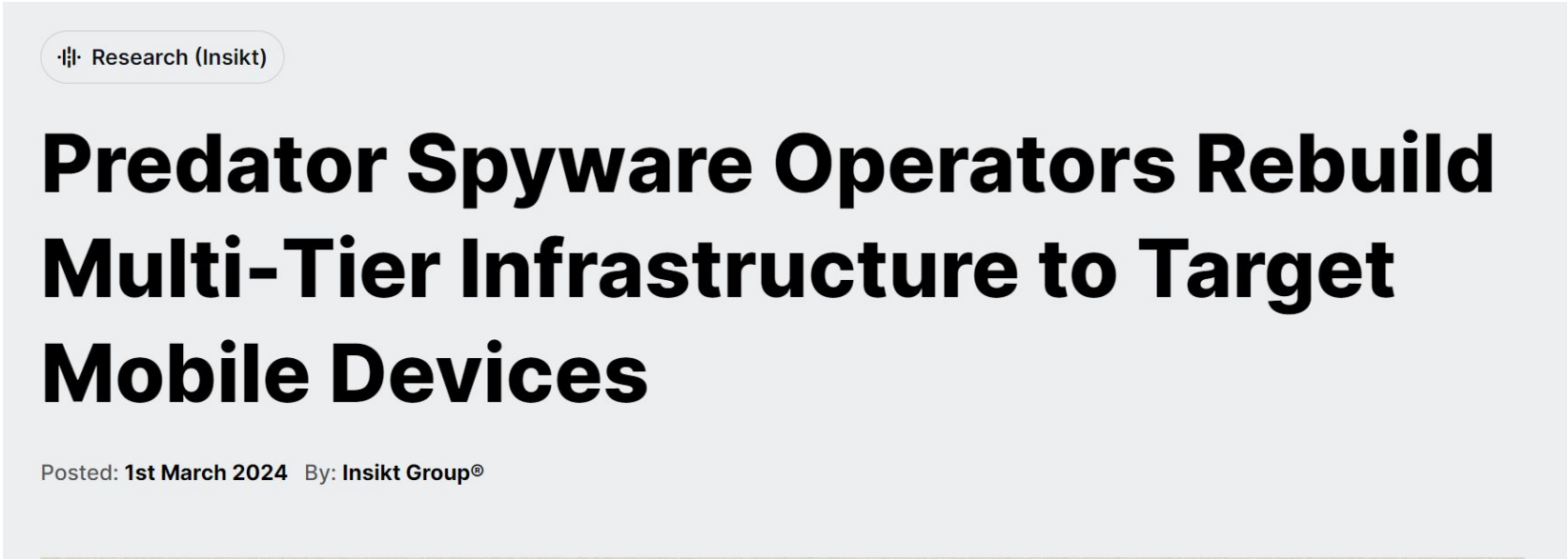
Lorenzo Franceschi-Bicchierai @lorenzofb / 5:05 AM GMT+9 • February 16, 2024 Comment

Court orders maker of Pegasus spyware to hand over code to WhatsApp

Israeli company NSO Group is accused in lawsuit by Meta's messaging app of spying on 1,400 users over a two-week period

NSO Group's Pegasus spyware is capable of extracting information from a target's phone without their permission or knowledge. Photograph: Amir Cohen/Reuters

Disrupt the offensive cybersecurity industry operations



Disrupt the offensive cybersecurity industry operations

RON WYDEN
OREGON

CHAIRMAN OF COMMITTEE ON FINANCE

221 DIRKSEN SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-5244

United States Sena
WASHINGTON, DC 20510-370

February 29, 2024

The Honorable Joseph R. Biden, Jr.
President
The White House
1600 Pennsylvania Avenue, N.W.
Washington, D.C. 20500

Dear President Biden:

I write to request that you address the grave threats posed by wir
practices, which are not regulated, but should be. Surveillance c
foreign government customers have exploited lax security in U.S
for at least a decade to track phones anywhere in the world. Auth
abused these tools to track Americans in the United States and jo
threatening U.S. national security, freedom of the press, and inte

Surveillance technology companies sell access to phone compan
which their foreign government customers can enter any phone r
associated with it, wherever it is in the world. In contrast to spyw
services do not interact with the target's phone. Instead, they tric

Executive Order 14093 so that the same restrictions that you created for spyware companies also apply to firms that sell phone company hacking services.

Fifth, to ensure that foreign surveillance companies are not able to benefit from the U.S. financial system, including investments from the U.S, the Departments of Treasury and State should impose Global Magnitsky sanctions. Specifically the government should sanction the major players in this industry, including Circles, Cognyte, the Rayzone Group and Defentek. The government should also investigate for potential sanctions FlowLive and Inno Networks, two foreign telecommunications companies that press reports have alleged are fronts for surveillance companies.

Sixth, to encourage allied countries to take similar steps to regulate the sale of phone company hacking services, BIS and the Departments of State and Defense should support efforts at the Wassenaar Arrangement — a multi-country forum for collaboration on export controls — to regulate phone company hacking services. On January 15, 2024, the Swiss government informed my office that it submitted a proposal along these lines, in response to reporting in May 2023 from an international consortium of news organizations into a Swiss company enabling such surveillance, which the press linked to the murder of a journalist in Mexico. I also request that you provide me with a copy of the Swiss proposal.

Thank you for your attention to this important matter. If you have any questions about this request, please contact Chris Soghoian in my office.

Sincerely,

NEWS

UK and France push for international agreement on spyware

The UK and France are hosting diplomats, big tech companies and civil society groups, in a two-day conference in London targeting the proliferation of spyware tools and 'hackers for hire'

By **Bill Goodwin,** Computer Weekly

Published: 06 F

REUTERS® World Business Markets Sustainability Legal Breakingviews Technology Investigatio

Society & Equity | Data Privacy | Human Rights | Data Privacy

Britain, France lead 35 nation agreement on controlling spyware, mercenary hackers

Reuters

February 7, 2024 5:47 AM GMT+9 · Updated a month ago

GOV.UK

Home > Government > Cyber security

Press release

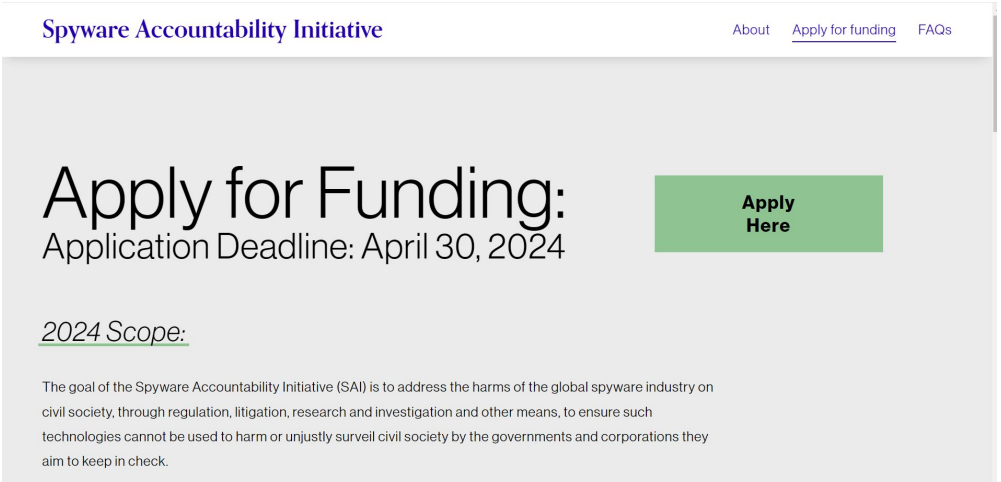
Deputy Prime Minister hosts first global conference targeting 'hackers for hire' and malicious use of commercial cyber tools

In a speech today, the Deputy Prime Minister, Oliver Dowden, has called on governments and businesses to address the proliferation of commercial cyber intrusion tools and services by developing better safeguards and oversight.

Disrupt the offensive cybersecurity industry operations

Biden administration indicts and sanctions Chinese hackers accused of sweeping espionage campaign against US targets


By Sean Lyngaas and Evan Perez, CNN
4 minute read · Updated 1:24 PM EDT, Mon March 25, 2024



Disrupt the offensive cybersecurity industry operations

Featured Article

Investors' pledge to fight spyware undercut by past investments in US malware maker

Cyber investors announced commitments to fighting spyware, but at least one firm previously invested in an exploit maker

Lorenzo Franceschi-Bicchierai @lorenzofb / 10:47 I

THE WHITE HOUSE

MENU

MARCH 18, 2024

Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware

BRIEFING ROOM › STATEMENTS AND RELEASES

Vendors, regulation, media, NGOs and politicians

New regulations from the US that allows to denied visa from anyone who is part of the offensive cybersecurity industry

Vendors starting to call names and provide detail attribution to exploits used by the end to end companies

Politicians launched investigations on misuse of end to end services

For the first time, individuals were added to the US sanction list

US politicians recommend to add new offensive cybersecurity companies to the sanction list

The judicial system forces end to end companies to give sensitive information to vendors

It’s just April, right?

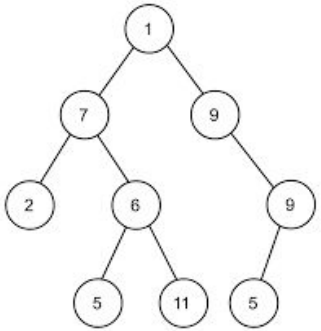
Vendors, regulation, media, NGOs and politicians - What can we learn?

The US is signals to the offensive cybersecurity industry that they need to to pick a side - “western VS non-western”

We might see an EU version of US sanctions and policies to restrict the offensive cybersecurity industry

The regulators are creating tools and policies that can be used on other type of entities that are not end-to-end companies in the industry (i.e supply chain, brokers)

Everything can change, but for now, let’s assume that this regulation trend will continue



The ripple effect

End to end companies

End to end companies

- End to end companies needs to make a decision with whom they will work
- Option #1: working with non-western countries
  - High probability to get into the sanction list
    - Isolation from crucial vendors
    - Hard to move money around (all transactions should be in a non-USD currency / SWIFT etc)
  - Individual and executives can be added to the sanction list
  - Employees can be denied entrance to the US
  - End to end clients might face deterioration in relations with the US / EU

End to end companies

- Option #2: working with western countries
  - Low(er) revenue stream
  - Limited demand for end to end solution
  - Limited space to grow
  - Strict(er) SLA
  - Unfair game - US based end to end companies have the advantage

End to end companies

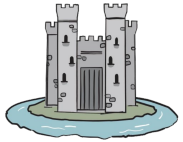
Either way, end to end companies revenue will decrease

The regulators will limit their licenses to sell the technology to specific regions

Some end to end companies will go bankrupt

End to end companies will push for lower prices for vulnerabilities

Difficulty to keep employees / researchers

End to end companies with a  :

- There are companies that only worked in the past with Western governments.
- End to end companies that worked with non-western countries can pledge to only work with Western governments moving forward.
- To be affiliated with a government that can “protect” the executives, employees, and supply chain from being added to the sanction list (but not the company itself).
- If your strategy is to work with “non-western” countries, congratulation, you can hike prices, by a lot.
    - Just make sure that the operation is close-loop in sponsored country.

Sanctions - baby steps

The US regulator added specific companies to the list, knowing that the companies could bypass the sanctions quite easily through shell companies and third parties.

If the US regulator wants to stop a company as a whole, they can do it by adding executives to the sanction list.

The regulator chose to not add some individuals to the sanction list, in most cases, due to “government protection” to those individuals.

Supply chain
Defense position

Total addressable market

Only a handful of end to end companies still operates in the market

New regulations limits the number of potential clients even more

Governments mostly work with clearing houses (aggregators) and their availability to research groups is limited

Supply chain

Many new research groups in the market

Many researchers that looking for a job

Individual researchers

Will going to be impact the most.

Work with limited number to clients.

Their clients are mostly end to end companies.

High risk compensation structure (i.e found item - getting paid).

Limited resources to allocate for client relationship / creating new relationships.

Individual researchers

Too small to engage governments directly.

If the main client will go bankrupt -> free flot.

Focus on one specific target - Time to market (in a few slides).

Research groups and clearing houses

Shifting their strategy - defensive position, saving resources.

Firing // not renewing contracts to researchers who didn't perform well.

Focus on paid R&D and pre-purchase items.

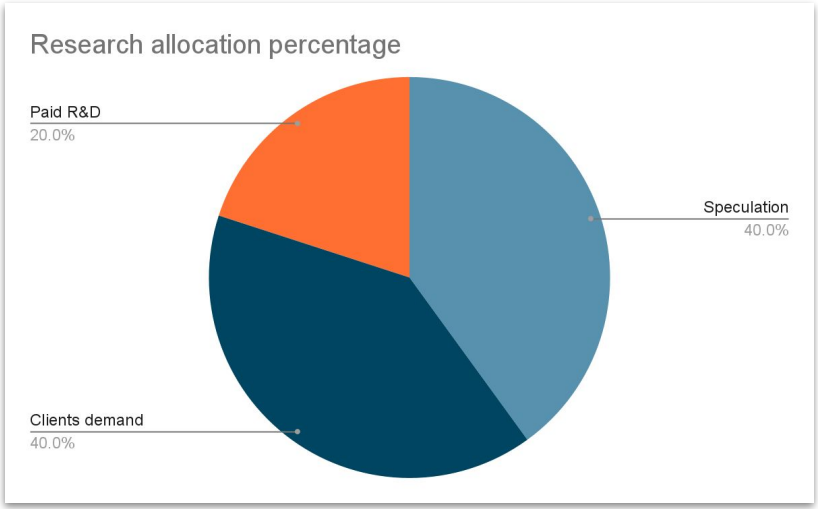
Decrease speculation projects.

"Sanction proof" revenue stream - prioritization of governments.

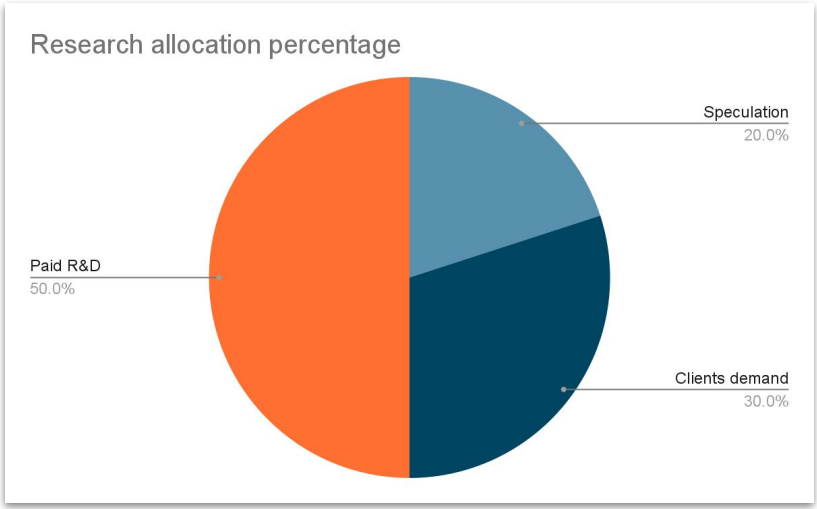
Diversify research projects - boutique research (BB / 0clicks / IM).

Clearing houses research allocation demand VS speculation

The adjust



The unknown



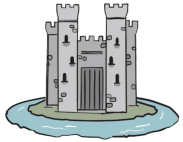
Time to market / feeding the beast

When the total addressable market shrinks, the supply side competition is fierce.

First come first serve:

- If there is demand to an item and there are at least two supply chain entities that have a solution to the demand, the first to sell will “take over the market”.
- In worst case, the supply chain is holding an item they can’t sell.
- In a better scenario, they could sell their item as a redundancy (worst terms).

Supply chain



- Connection to western governments (revenue protection from sanction).
- Paid R&D.
- Pre-purchase items (not paid R&D).
- Good enough relationship to prioritize you over potential market flood.
- To be affiliated with a end client that can “protect” you from sanctions (western end to end company / government).
- Invest in high demand (and high risk) research projects (i.e 0clicks / IM etc).
- Enough resources in reserve to withstand 2024

Market flood in the short term - opinion

Supply chain understands that we step into a new phase where they need to maximize their profits and save resources.

Will try to sell their inventory as fast as possible to reposition themselves for paid R&D / pre-purchase items.

When a few supply chain groups will do it, the market will be flooded with items which in turn will hurt the other supply chain entities in the market.

It’s a race. And it’s already started…

Main takeaways

- End to end companies will have to “pick a side” - either working only with the US/EU or to only work with the rest of the world
  - Some End to end companies will go bankrupt
  - Some End to end companies will be put on the US and EU sanction list
- Individual people in the offensive cybersecurity industry will be put on the US and EU sanction list -> already happened (!!)
- Over supply - In the next year we are going to see a lot of researchers and research groups trying to sell their inventory on the market
- The supply chain is going to experience a second shock wave - this time is from the demand side
  - Some of the clearing houses and research groups will go bankrupt
  - There are more high-end researchers that are looking for a job than ever before

Main takeaways

- There are going to be researchers with items in hand that they can’t sell
  - Prices for vulnerabilities and exploits will decrease
- Due to export control regulations - governments will have to stop operations outside their own country (i.e research hubs / shell companies)
- Clearing houses and research groups will take less risk and reduce research speculation (i.e pivoting to research on items that sold upfront)
- Clearing houses and research groups will not maintain chains - back to the item era
- Clearing houses and research groups will pivot away from traditional 1click solutions (mostly on the speculation side)

The opportunity

New clearing houses - timing the market

Uncertainty creates opportunities

If you have the resources (North of 15M USD) and the right positioning (i.e “sanction proof”) - 2024 can be the year that you can lock-in:

- High-end researchers
- Exclusive supply chain

Governments

Governments have shell companies / companies that are sponsored by a specific government that act as research hubs in different places.

They keep appearance of legitimate companies which focus on vulnerability research.

Make sure the new regulations will not affect operations

Governments - Option #1:

Keep the operation as is (i.e appearance of legitimate company)

Talk with your sponsor government and allocate (a lot more) resource to buy more than usual items from the market to secure long-term supply chain

Take advantage of the current market situation and hire new researchers

Governments - Option #2:

Tell the world who is sponsoring you!

If you are sponsored by western government and researchers can know about it, they will come to you!

Hire best-in-class researchers in better terms

Secure long term supply chain which you didn’t have access before

Will I still be here in 2025?
I don’t know, I don’t think so.
I hope so.