LEONARDO

The cyber threats evolution through the experiences gained by Leonardo with its customers

The British Chamber of Commerce for Italy
LO SMART WORKING, DA ECCEZIONE A NUOVA NORMALITÀ:
la Cybersecurity, le Nuove Regole e i case studies vincenti

Antonio Berardi, Head of Cyber Security & Intelligence Lab
Cyber Security Division Leonardo

03.11.2020

Summary

- Leonardo and the Cyber Security Division
- Focus on main 2020 Cyber Threats
- Changes about work after COVID-19: the threat actors' & companies' point of view
- Analysis of the main attacks detected by Leonardo during the COVID-19 pandemic
- Use Case

Our Group

Leonardo is a global company in the **Aerospace**, **Defence** and **Security** sector with an integrated offer of high-tech solutions for both military requirements and civil applications.

Helicopters	Defence Electronics & Security	Aeronautics	Space
Helicopters Division	Electronics Division Cyber Security Division Leonardo DRS (100%) Vitrociset (100%) Elettronica (31,33%) MBDA* (25%)	Aircraft Division Aerostructures Division ATR* (50%)	Telespazio* (67%) Thales Alenia Space* (33%) AVIO (26%)

*Joint ventures
% Leonardo's share

Cyber Security Division

We design, develop and implement products, systems, services and integrated solutions for Governments, Institutions, and large enterprises and are proud of

*“ … **Being the partner** of choice of domestic and international players engaged on **mission critical applications** requiring leading edge integrated end to end **security solutions.** ”*

LEONARDO CYBER SECURITY

We are the technological partner of the italian PA for the national secure digital transformation.

We are NATO’s mission Partner for the supranational Cyber Defence.

We provide professional communication infrastructure for security operations in over 150 countries.

We protect the public and private critical infrastructures, nationally and internationally, and guarantee the security of major events.

We support the safety and the resilience of cities and we design solutions for the security and efficiency of rail and road trasports.

Cyber Security Division: The Cyber Security & Digital Competence Center

Our Cyber Security & Digital Competence Center provides advanced technologies and skilled expertise for the design of **innovative products** and **solutions.** We also support our customers **collaboration with universities** and **research centers** in the **technology transfer** and the training on **Cyber Security** and **Digital Transformation**.

Leonardo's **NEXT GENERATION SECURITY OPERATION CENTER** the enabling infrastructure for the provision of managed security services that guarantee, in real time, the cyber protection and resilience of our Customers' key infrastructures

Security Operation Center

Computer Security Incident Response Team

Intelligence operation Center

SERVICES PROVIDED 24/7, 365 days/year

150 # EXPERT ANALYSTS in cybersecurity & intelligence

+ 50,000 # SECURITY EVENTS monitored/second

+ 1,200 # SECURITY OFFENCES managed every day

20% # SECURITY OFFENCES automatically managed

+ 250 SECURITY AWARENESS generated/year

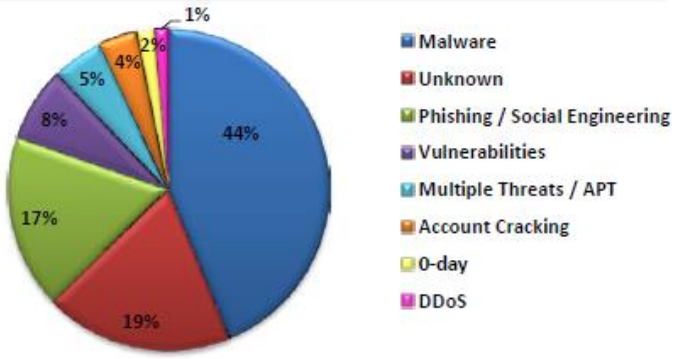
+ 3,5 M INDICATORS OF COMPROMISE monitored/year

+1,300 TAILORED INTELLIGENCE REPORTS generated/year

500 TFLOPS High Performance Computer

Main Cyber Threats: types and motivations

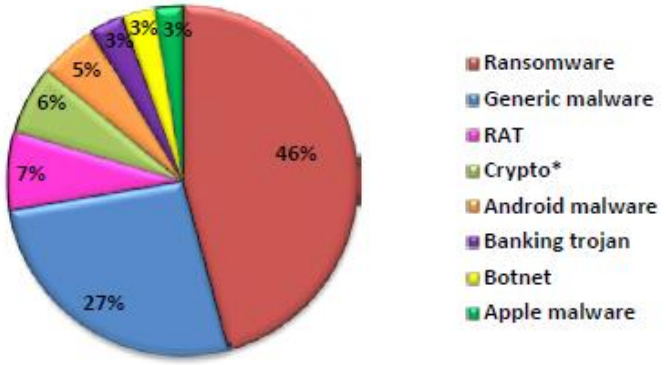
Cyber Attack distribution by types (2019)



© Clusit - Rapporto 2020 sulla Sicurezza ICT in Italia

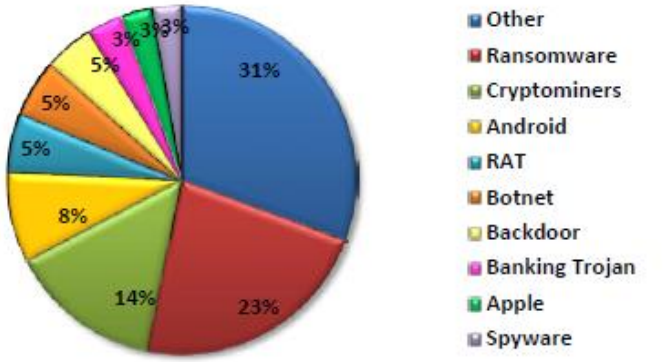
TIPOLOGIA TECNICHE DI ATTACCO	2014	2015	2016	2017	2018	2019	2019 su 2018	Trend
Malware	127	106	229	446	585	730	24.8%	↑
Unknown	199	232	338	277	408	317	-22.3%	↓
Known Vulnerabilities / Misconfig.	195	184	136	127	177	126	-28.8%	↓
Phishing / Social Engineering	4	6	76	102	160	291	81.9%	↑
Multiple Techniques / APT	60	104	59	63	98	65	-33.7%	↓
Account Cracking	86	91	46	52	56	86	53.6%	↑
DDoS	81	101	115	38	38	23	-39.5%	↓
0-day	8	3	13	12	20	30	50.0%	↑
Phone Hacking	3	1	3	3	9	1	-88.9%	↓
SQL Injection	110	184	35	7	1	1	0.0%	-
TOTALE	873	1012	1050	1127	1552	1670		

Malware distribution by types (2019)



© Clusit - Rapporto 2020 sulla Sicurezza ICT in Italia

Malware distribution by types (2020)



© Clusit - Rapporto 2020 sulla Sicurezza ICT in Italia

The main motivations of the Threat Actors behind the cyber-attacks:

- Geopolitics
- Financial
- Industrial espionage
- Hacktivism

Changes about work after COVID-19: the companies' point of view

From the beginning of 2020, Italy (and the rest of the world) is facing the COVID-19 pandemic for which no one was really prepared.

Smart Working approach has ensured the business continuity but, on the other hand, has introduced a strong exposure to cyber risks

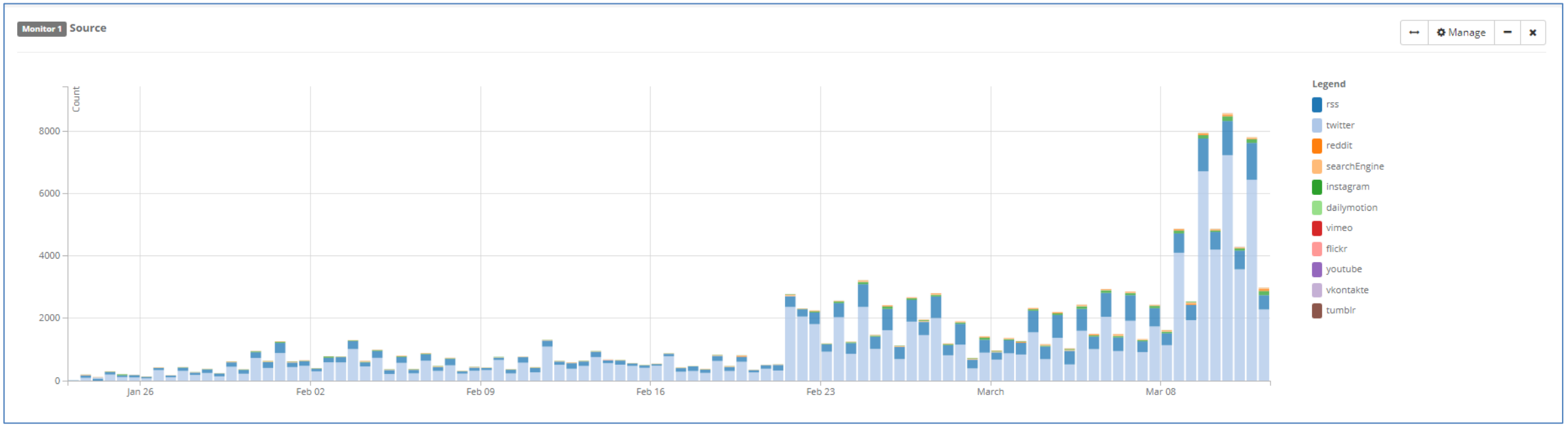
After COVID, we have operated in a context in which:

- the infrastructures were not adequately sized and protected
- people didn't have specific training about threats in this new scenario
- The processes were not suited to the new operational context

After COVID-19 pandemic, Cyber risks has enormously increased

Changes about work after COVID-19: the threat actors' point of view

The interest about **COVID-19 topic** becomes a key element in making malicious campaigns more effective

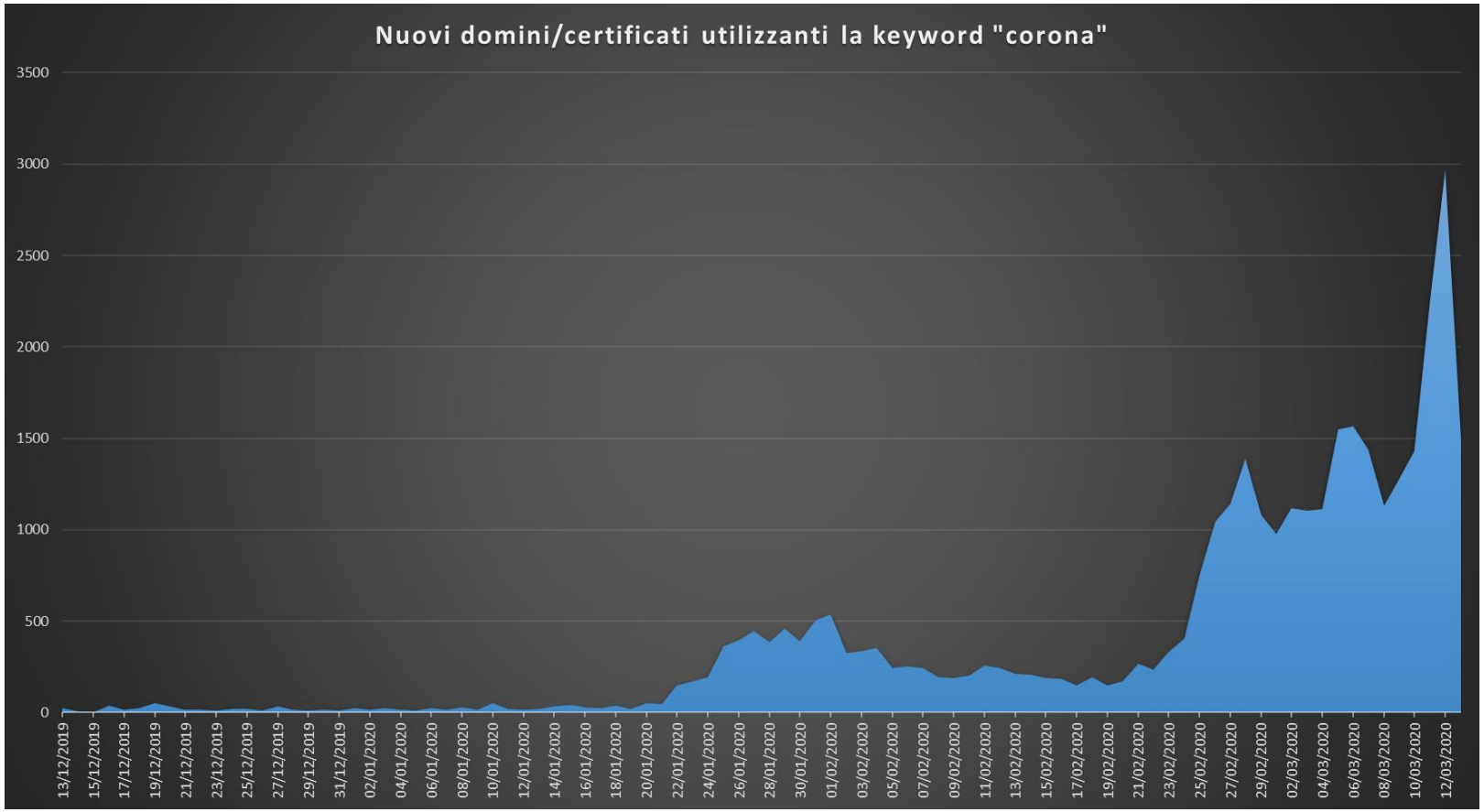


The social chatter regarding the COVID-19 theme

Source: SOC Leonardo

Changes about work after COVID-19: the threat actors' point of view

The significant increase in new **malicious COVID-19-themed sites** recorded in Q1 2020 confirms the **opportunism of threat actors in exploiting this topic**

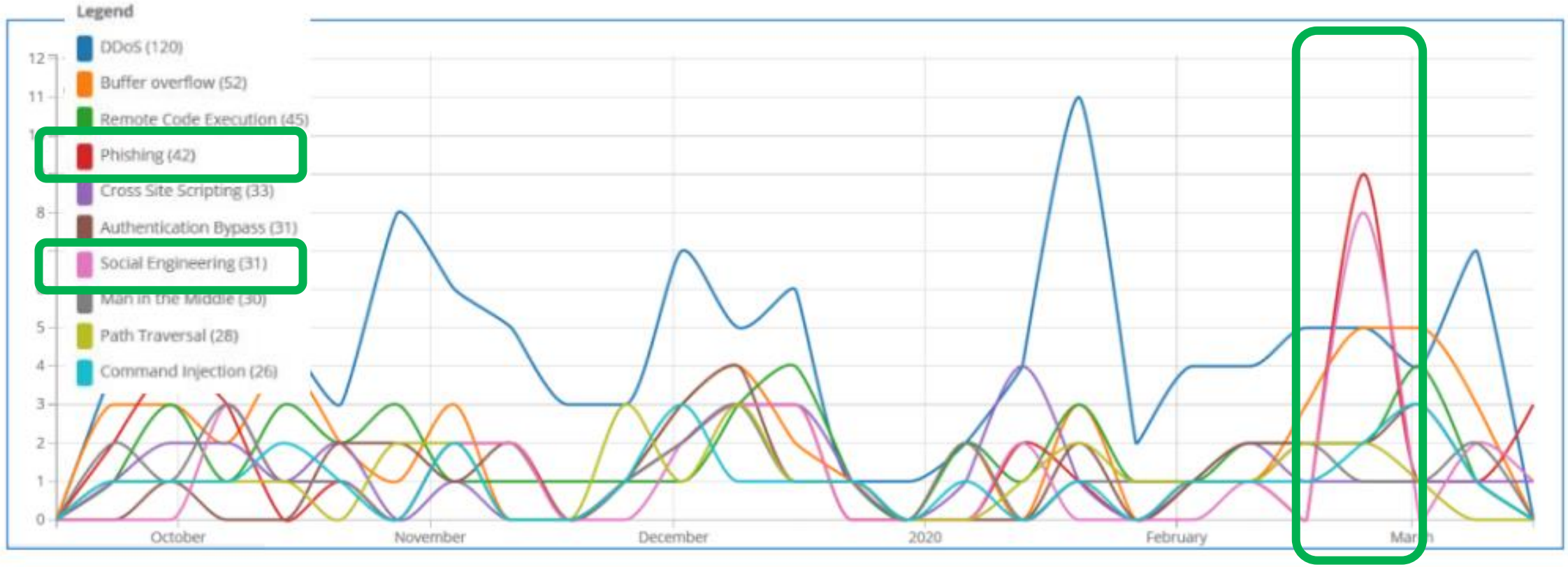


Trend of the registration of new domains using the COVID-19 subject

Source: SOC Leonardo

Changes about work after COVID-19: the threat actors' point of view

The type of **cyber-attacks also change to adapt to the emergency phase** focusing on **Phishing** and **Social Engineering**

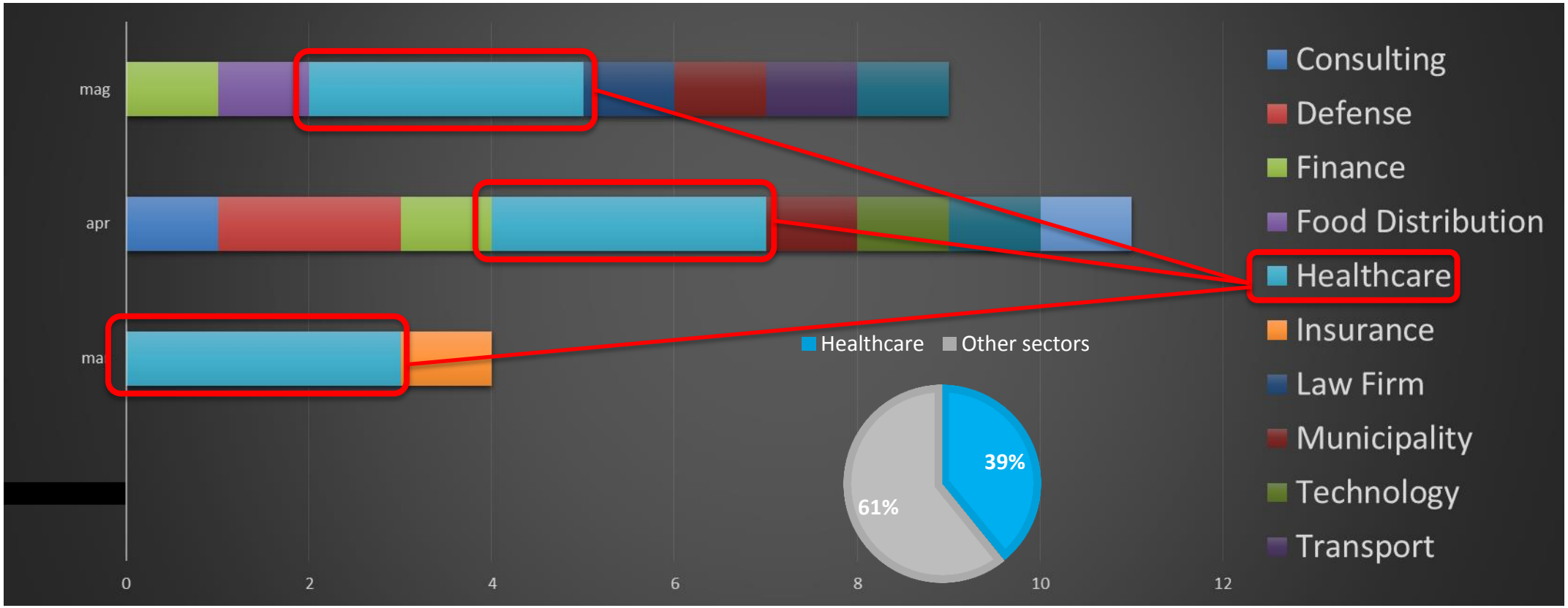


Cyber-attacks by type

Source: SOC Leonardo

Changes about work after COVID-19: the threat actors' point of view

Cyber-attacks **mainly target the healthcare sector** most exposed in the pandemic period



Ransomware attacks by industry

Source: SOC Leonardo

Analysis of the main attacks detected during the COVID-19 emergency

PIONER KITTEN (alias PARISITE, UNC757)

- *GOAL:* **Iranian state-sponsored group**
- *HISTORY:* has been operating since 2017, before known as **TunnelMaster**
- *TACTICS, TECHNIQUES, AND PROCEDURES (TTP)*: internet mass scans to find vulnerable servers
- *BEHAVIOUR DURING THE PANDEMIC*: sale of user access to compromised company networks, using the VPN vulnerabilities exploitation

Analysis of the main attacks detected during the COVID-19 emergency

CHARMING KITTEN (alias Parastoo, APT35)

- *GOAL:* Iranian **state-sponsored group**
- *HISTORY:* has been operating since 2013, links to the Islamic Revolutionary Guard Corps (IRGC)
- *TACTICS, TECHNIQUES, AND PROCEDURES (TTP)*: very active in social engineering operations through spear phishing
- *BEHAVIOUR DURING THE PANDEMIC*: sale of credentials to access compromised corporate networks, using the VPN vulnerabilities exploitation

Analysis of the main attacks detected during the COVID-19 emergency

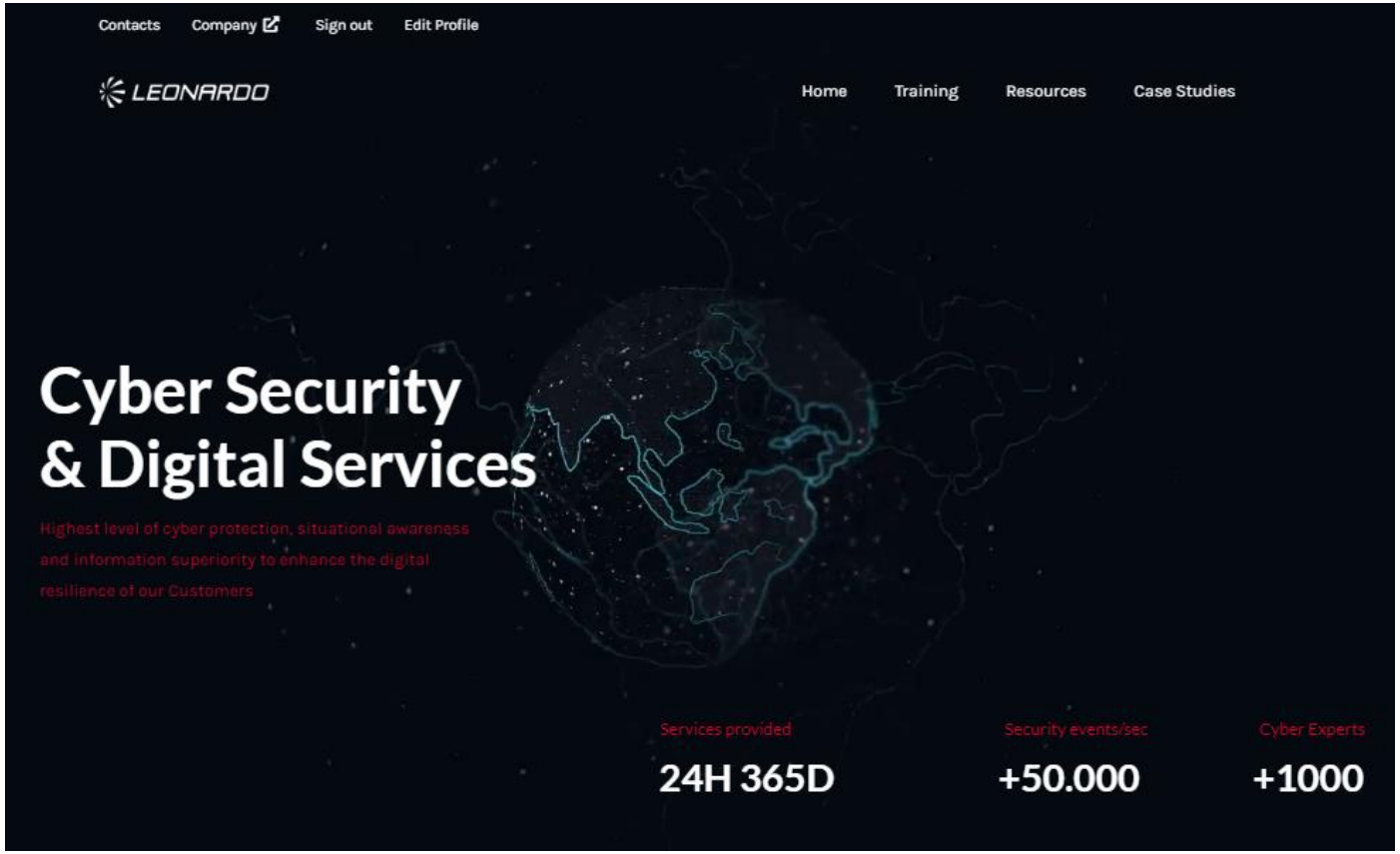
GRACEFUL SPIDER

- *GOAL:* Iranian **no-profit group**
- *HISTORY:* has been operating since 2016, links to APT Indrik Spider (Author of Dridex)
- *TACTICS, TECHNIQUES, AND PROCEDURES (TTP)*: spam emails to gain initial access to victims
- *BEHAVIOUR DURING THE PANDEMIC*: use of CL0P ransomware to attack Healthcare companies

Introduction to the Use Case – The Intelligence Process

Use Case

Smart working & Cyber Security: Leonardo COVID-19 initiatives



- Documentation on attacks and prevention measures
- Cyber awareness video learning for employees

https://lnrdo.co/cyberaccess

LEONARDO CYBER SECURITY

THANK **YOU**
FOR YOUR ATTENTION

leonardocompany.com