The "New Normal" State of Cybersecurity

LESSONS LEARNED DURING THE PANDEMIC

About me

Bogdan BOTEZATU

- 20 years of fighting cybercrime in different roles
- 14 years under the Draco sign as Director of Threat Research @ Bitdefender
- Builder of decryptors and removal tools before it was cool

Bitdefender

Addressing the Challenge:

HARD TO STAY ON TOP OF EVOLVING THREATS

Advanced Threat Intelligence

Continuously built into prevention technologies, analytics, and MDR operations

35 billion Daily threat queries from hundreds of millions of sensors worldwide

400+ Threats discovered every minute (criminals, nation-states, malicious actors)

20 Ransomware decryptors provided free to the market

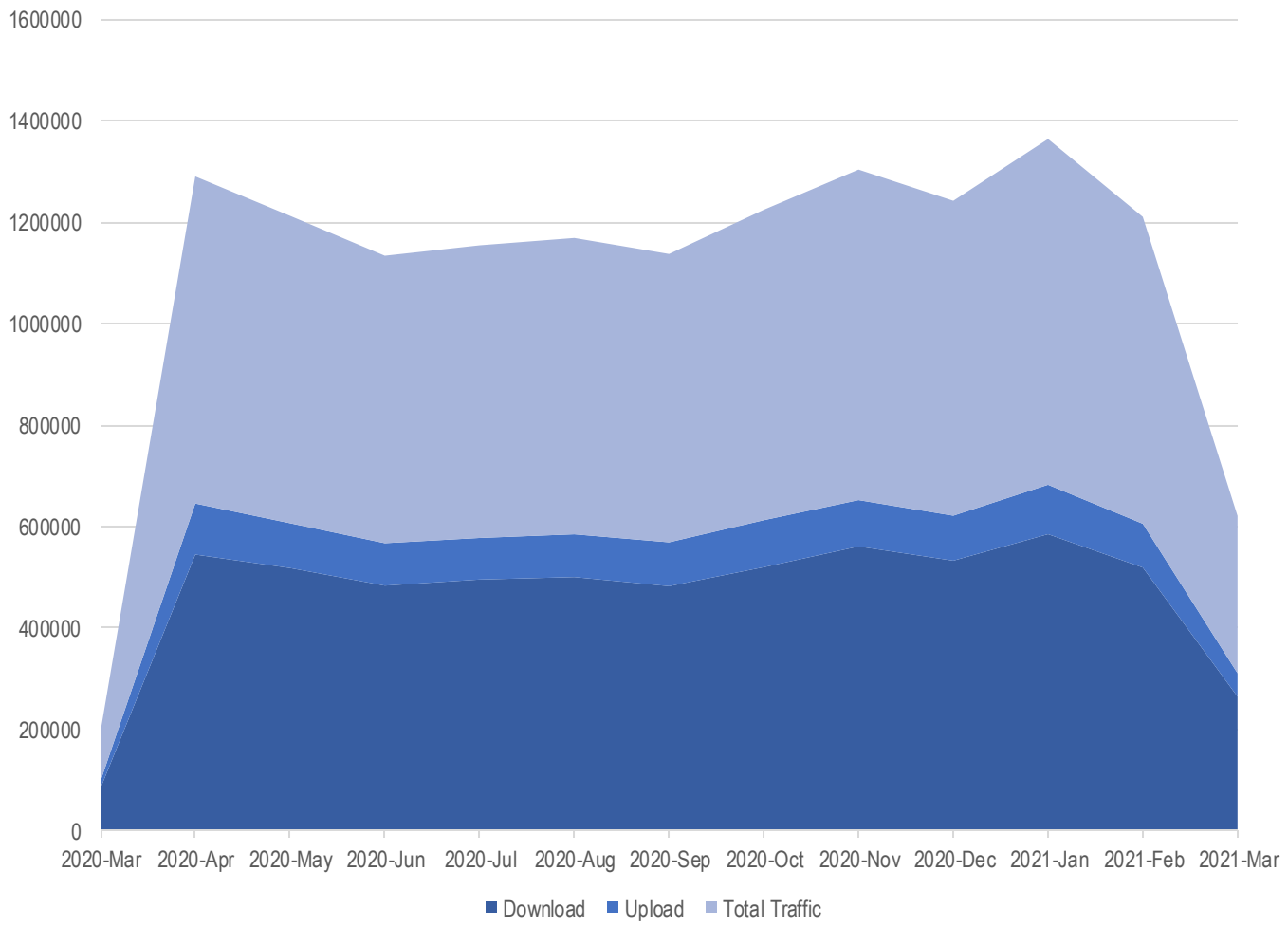
$billions Helped law enforcement take down major cybercrime groups with estimated worth in the billions

285 Elite security researchers, threat hunters and security analysts. Close collaboration on incident response with law enforcement; Working with leading academics on quantum computing and cryptography

400+ R&D employees focused on cloud, emerging technology, IoT research and machine learning

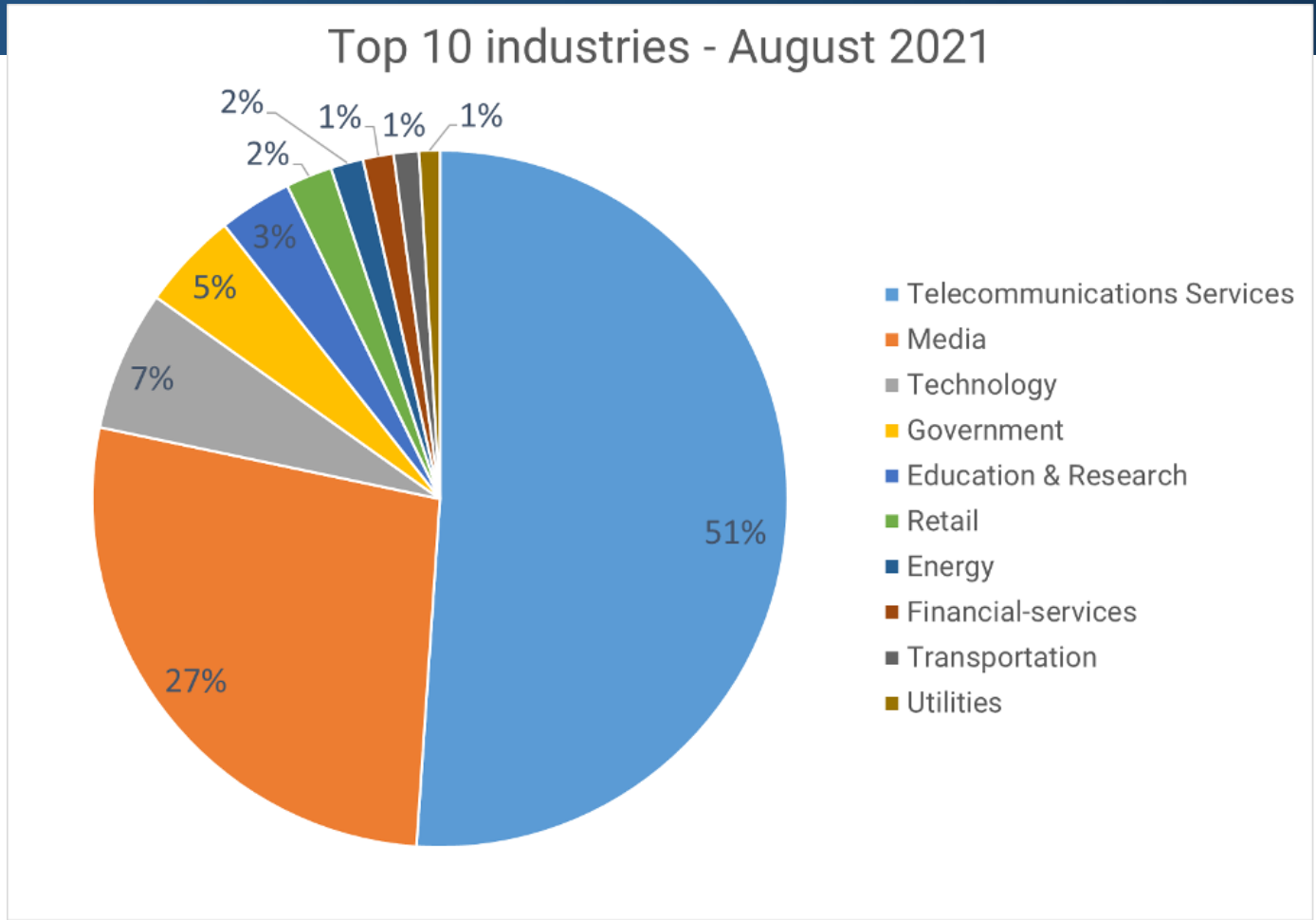
Pandemic threat landscape

- 4 out of 10 Covid-themed emails are spam
- 46 percent increase in the number of IoT suspicious incident reports
- 55.73 percent of IoT network threats involve port-scanning attacks
- GoLang becoming a popular programming language for IoT malware
- Significant increase of RDP bruteforce attacks and phishing targeted at employees
- Attackers focus more on social engineering, less on malware sophistication



Ransomware during the pandemic

- **485 (c) / 715 (b) percent increase** in year-over-year ransomware attacks
- New vectors include **supply chain attacks** to reach larger pools of victims
- Ransomware becomes a real threat to national security (Darkside vs. Colonial Pipeline)
- Most ransomware attacks go unreported unless featured in the media*



Challenges

Ransomware is a mature business with proven return of investment:

- Darkside – $4.4 million in one run
- RagnarLocker - $4.5 million in one run
- GandCrab – 2 BILLION USD in 18 months

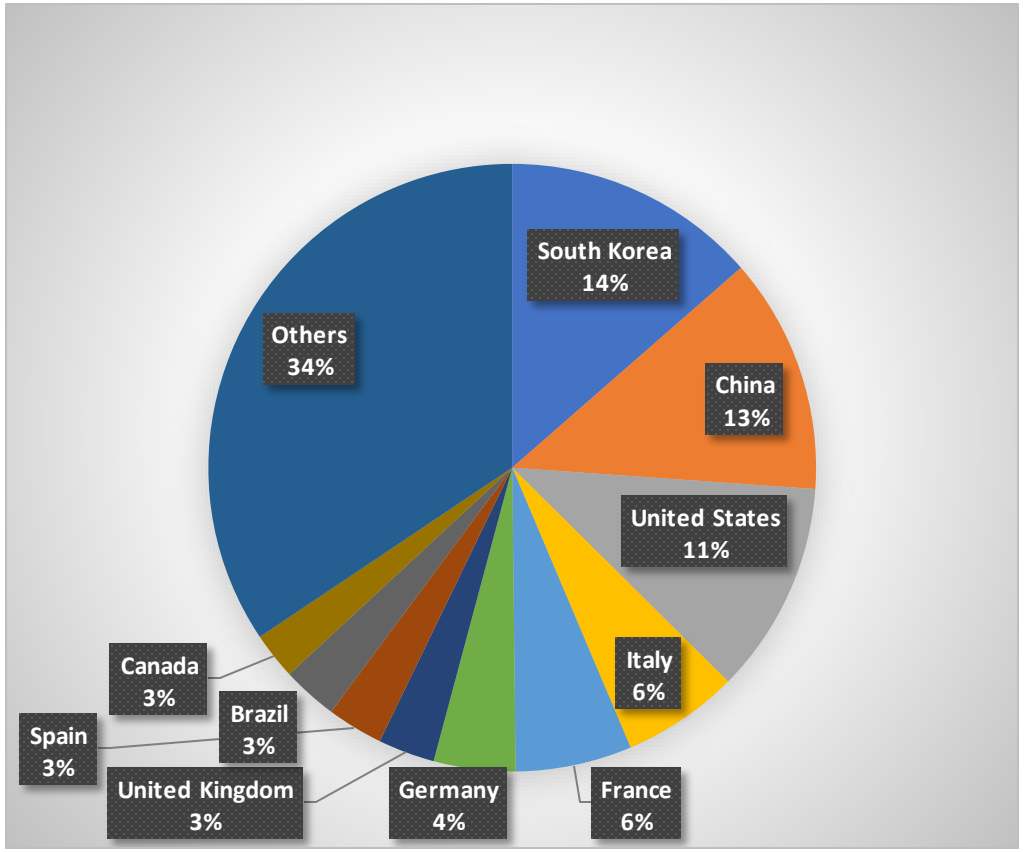
New contenders show up to fill the gaps left behind by big players

Rebranding of “rockstar” groups who so far avoided arrests

- GandCrab -> REvil
- Ryuk -> Conti
- DarkSide -> BlackMatter

Opportunities

- Collaboration with Law Enforcement Agencies is effective and helps curb down on ransomware attacks
- Bitdefender helps users decrypt data for free – more than **1,400** victim-companies in 84 countries saved - #GoldDust
- That's **more than 500 MILLION** US dollars in unpaid ransom
- Weaken operators by cutting off supplies
- Internal struggle between affiliates
- Establish a positive mindset: a decryptor will be available soon, so **#DONTPAY** the ransom.



draco@bitdefender.com