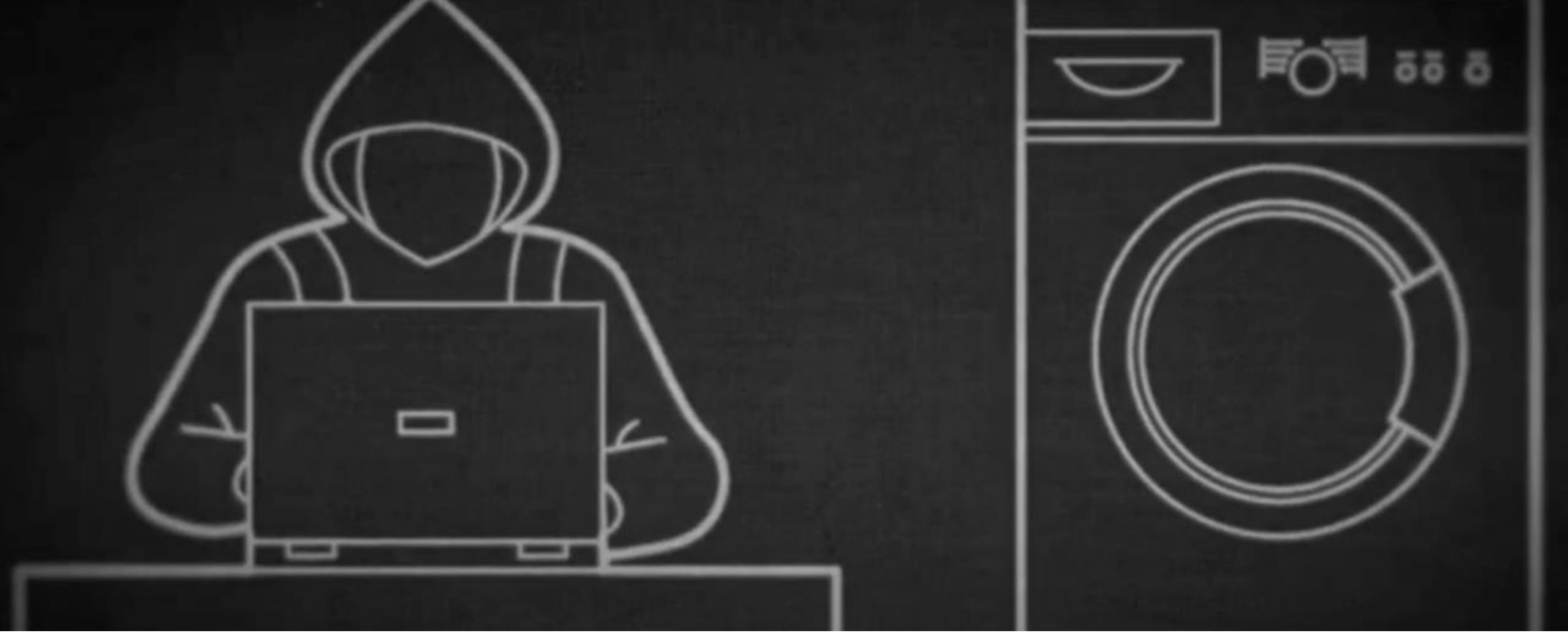
# Banking IT and FinTech

## Cybersecurity

Szabolcs Szalay

February 2025



# The Bangladesh heist

https://www.youtube.com/watch?v=-IZDNAkna5c

### Fraud and insider threats

- Internal and external threats
- Retail and nonretail threats
- Insider threats
- Market abuse and misbehavior

### Cyber breaches

- Confidentiality
- Integrity
- Systems availability

### Financial crimes

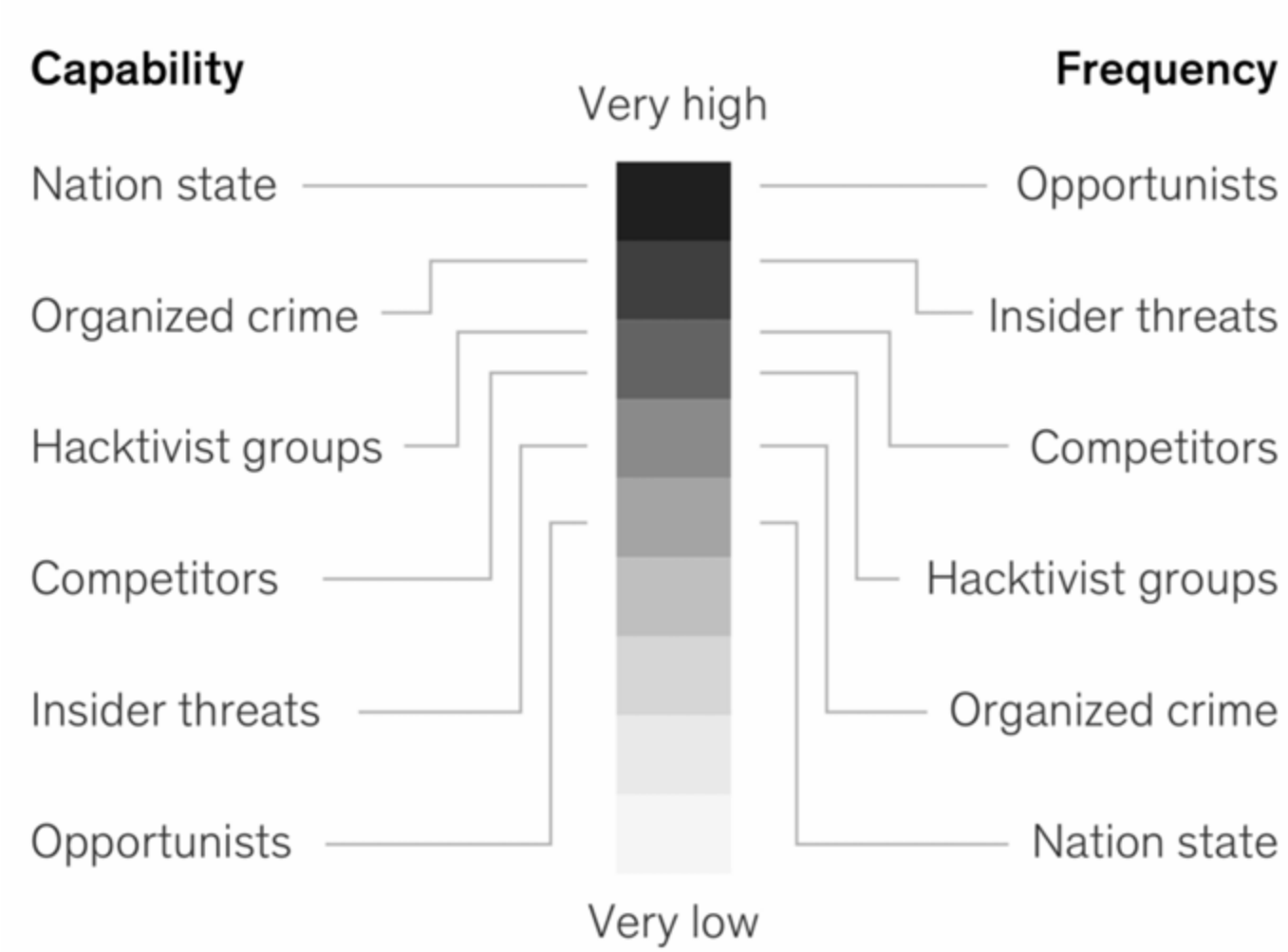
- Money laundering
- Bribery and corruption
- Tax evasion and tax fraud

### Example: cyberattack on a central bank

- Bank employee's SWIFT[1] credentials stolen with the help of insiders
- Malware surreptitiously installed on the bank's computers to prevent discovery of withdrawals
- Funds routed from bank's account at a branch of another country's central bank to a third bank (on a weekend to ensure staff absence)
- Withdrawals were made at the third bank through multiple transactions that were not blocked until too late
- Attacks may have been linked to a known sanctioned entity

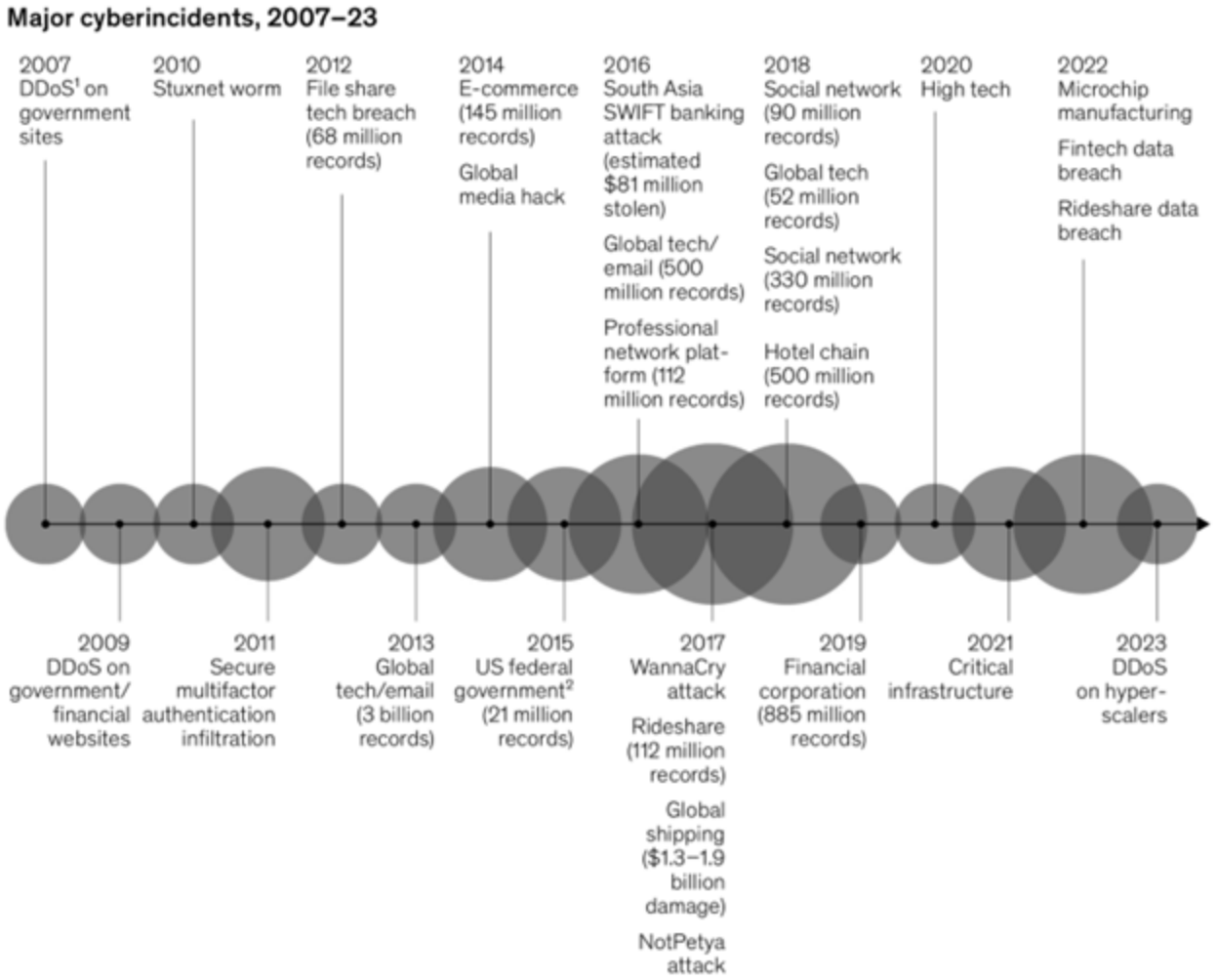
# Crime categories are converging

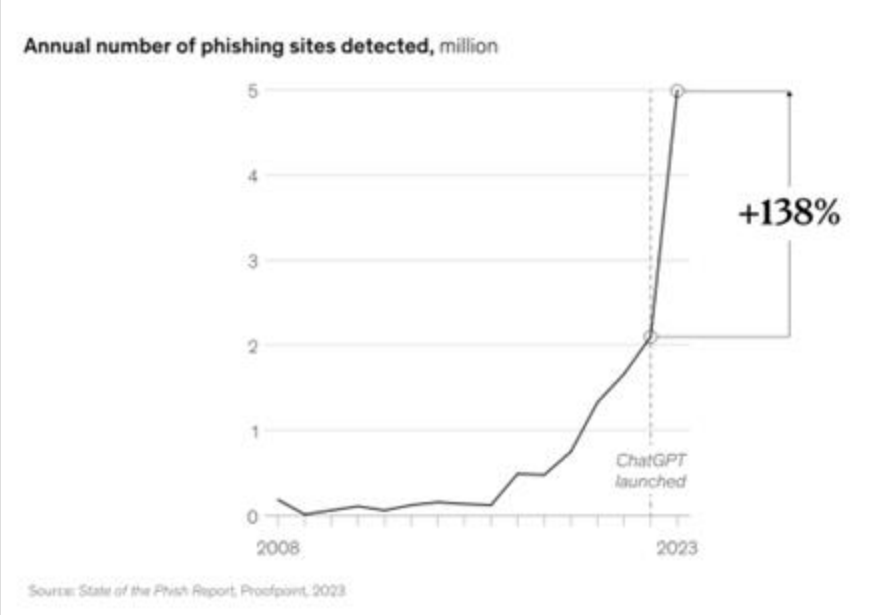
# Proliferation of cybercriminals


Source: McKinsey; illustration by DALL-E

# Frequency and severity of attacks increasing

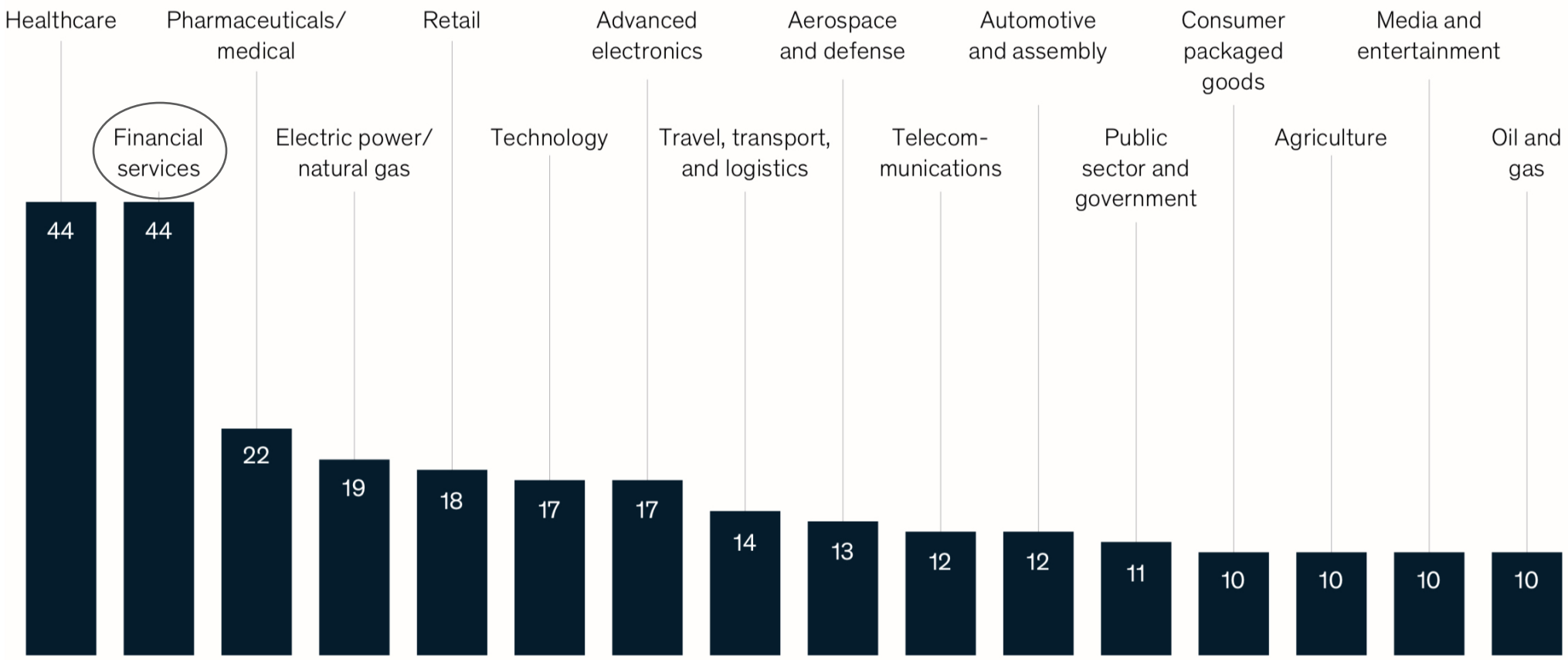



Source: McKinsey

# Financial services are trustworthy businesses

**Respondents choosing a particular industry as most trusted in protecting of privacy and data,** % (n = 1,000)




Source: McKinsey Survey of North American Consumers on Data Privacy and Protection, 2019

# Many potential fraud attack opportunity in a customer journey

## (retail bank example)

| | Open an account | Change account | Make a payment | Make a deposit |
|---|---|---|---|---|
| **Customer-initiated actions** | Customer opens a new account or adds another account through online, mobile, branch, or ATM channels | Customer updates existing account, eg, adding a beneficiary or changing address | Customer pays self or third party through wire, credit or debit card, or online transaction | Customer makes a transfer or deposit into their account |
| **Attack channel** | | | | |
| ATM | • Identity theft<br>• Synthetic ID<br>• Employee-generated account<br>• Malware | • Malware | • Card skimming or trapping<br>• Fake PIN pad<br>• Cash trapping<br>• Shoulder surfing<br>• Duplicate card<br>• Malware<br>• Transaction reversal | • Money laundering or terror financing<br>• Malware (balance multiplier) |
| Cards and e-commerce | | • Account takeover<br>• Address change<br>• Secondary card<br>• Malware | • Card-not-present fraud<br>• Card skimming<br>• Malware<br>• Cyberattack | |
| E-banking and wire | | • Addition of false beneficiary<br>• Account takeover<br>• Malware | • Cyberattack<br>• Malware<br>• Employee-driven transaction | |
| Branch | | • Account takeover | • n/a | |

Source: McKinsey

**1. Spear phishing**
Employee in targeted organization receives email with the Carbanak backdoor as an attachment

**2. Backdoor executed: credentials stolen**
Upon opening attachment, employee activates the Carbanak backdoor

**3. Machines infected in search for admin PC**
Carbanak searches network and finds admin PC; embeds and records

**4. Admin PC identified, clerk screens intercepted**
Attacker watches admin screen to mimic admin behavior for the bank's cash-transfer systems

**5. Balances inflated and inflated amount transferred**
Attackers alter balances, pocket extra funds ($1k account enlarged to $10k, then $9k transferred)

**6. ATM programmed to dispense cash**
Attackers program ATMs to issue cash to waiting accomplices at specific times

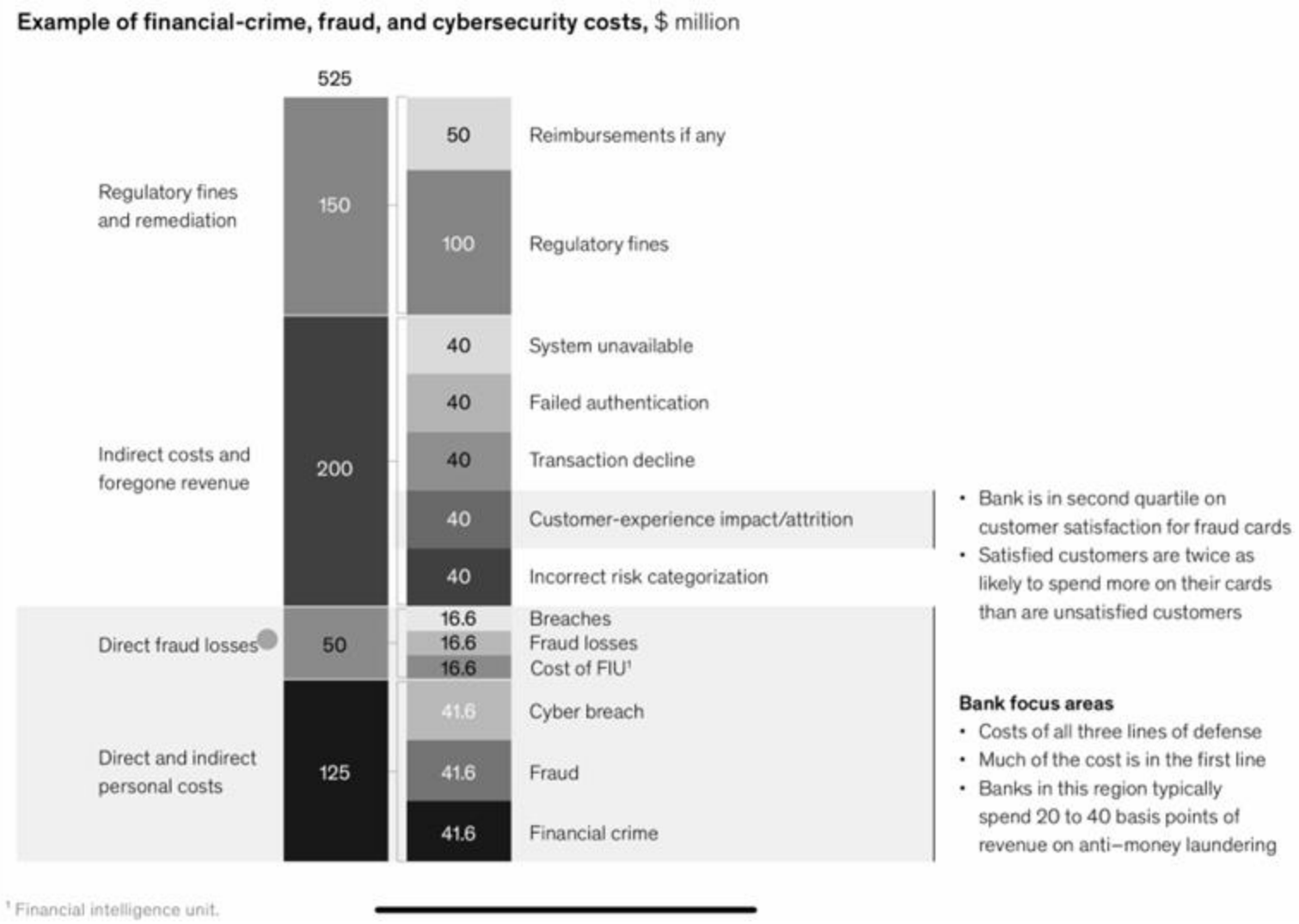
**7. Cash moved through channels by wire transfers, e-payments**
Attackers use online and e-payments to receiver banks to transfer extracted funds

# The Carbanak attack

## One of the most sophisticated and successful cyber heists in banking history

Source: McKinsey

# Banks often underestimate the total cost of financial crime




Source: McKinsey

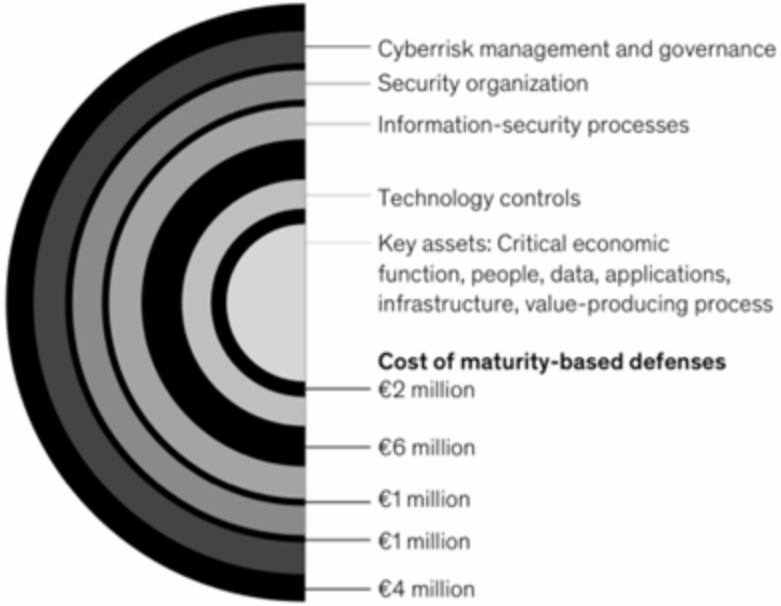
# Best practice: risk-based approach to controls

**Cyberrisk dashboard,** example


Source: McKinsey

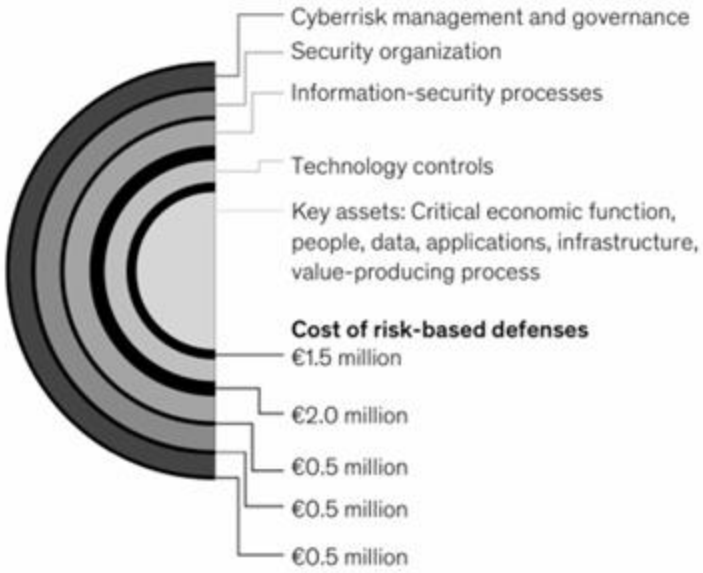
# Risk based approach is more budget conscious

**Maturity-based approach:** Builds highest level of defense around everything.




Total cost
**€14 million**

**Risk-based approach:** Optimizes defensive layers for risk-reduction and cost. Critical assets are highly protected, but at less expense and in ways that improve productivity.



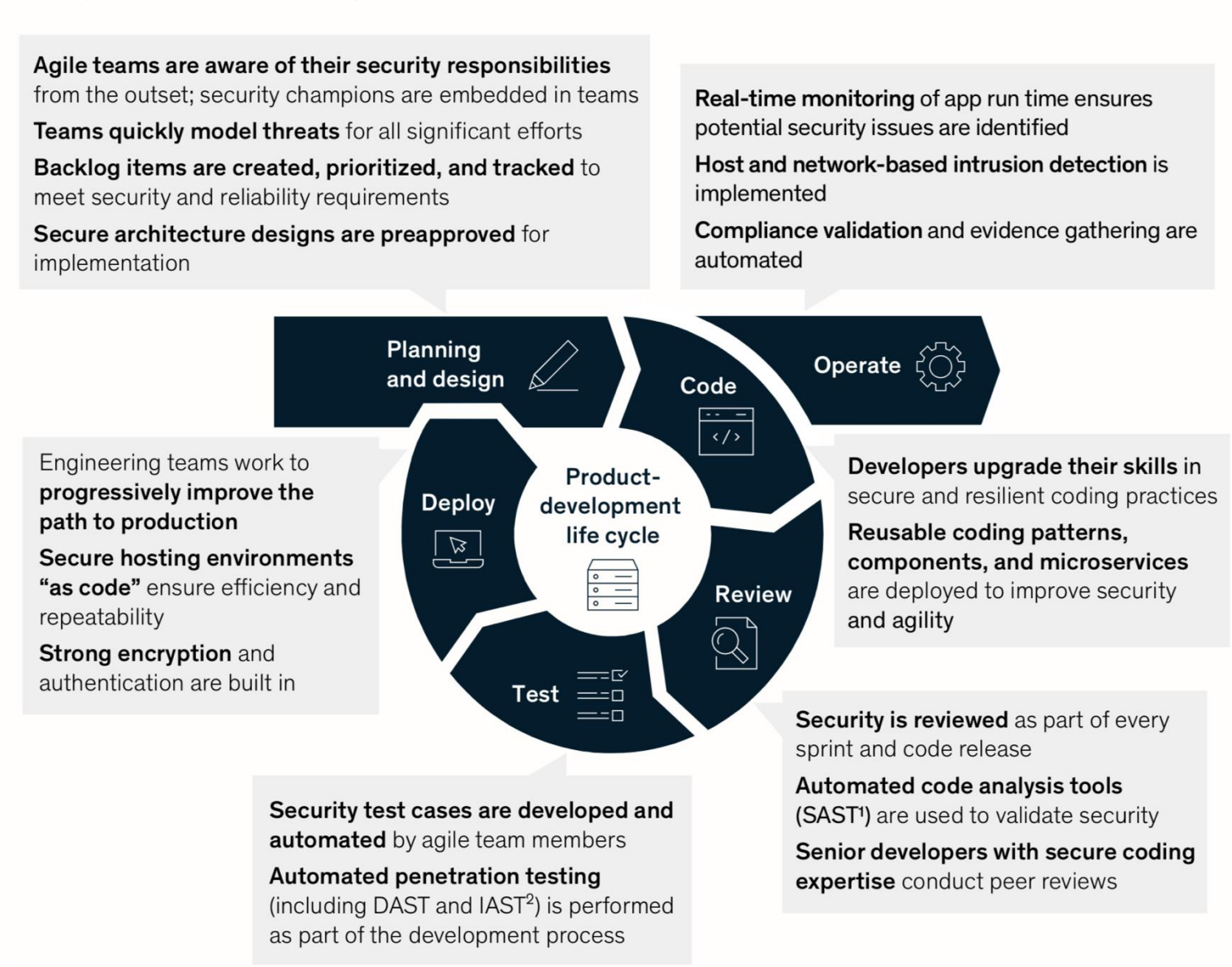

Total cost
**€5 million**

Note: Costs are illustrative but extrapolated from real-world examples and estimates.

Source: McKinsey

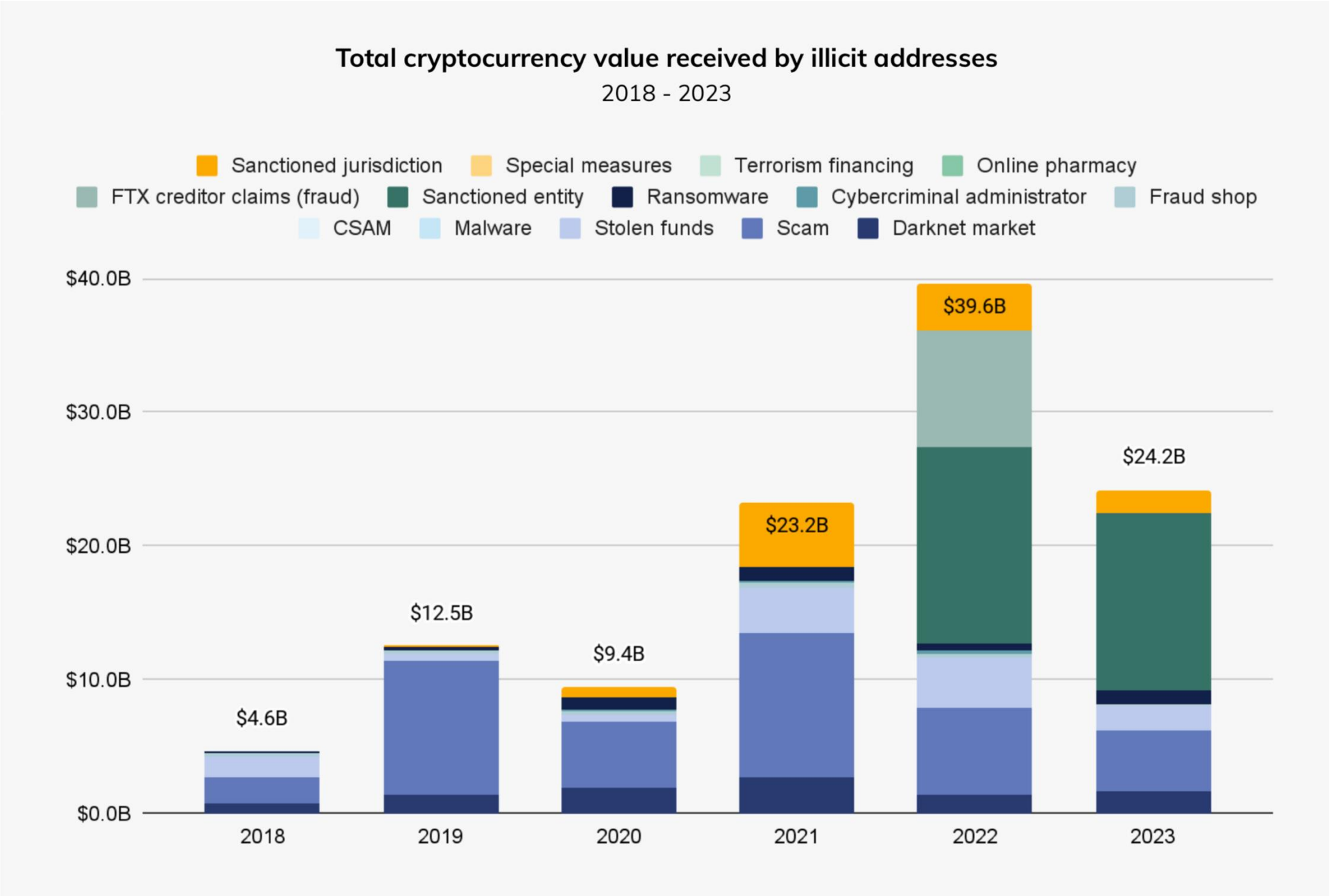
# DevSecOps

Security is integrated into every step in the product development life cycle.

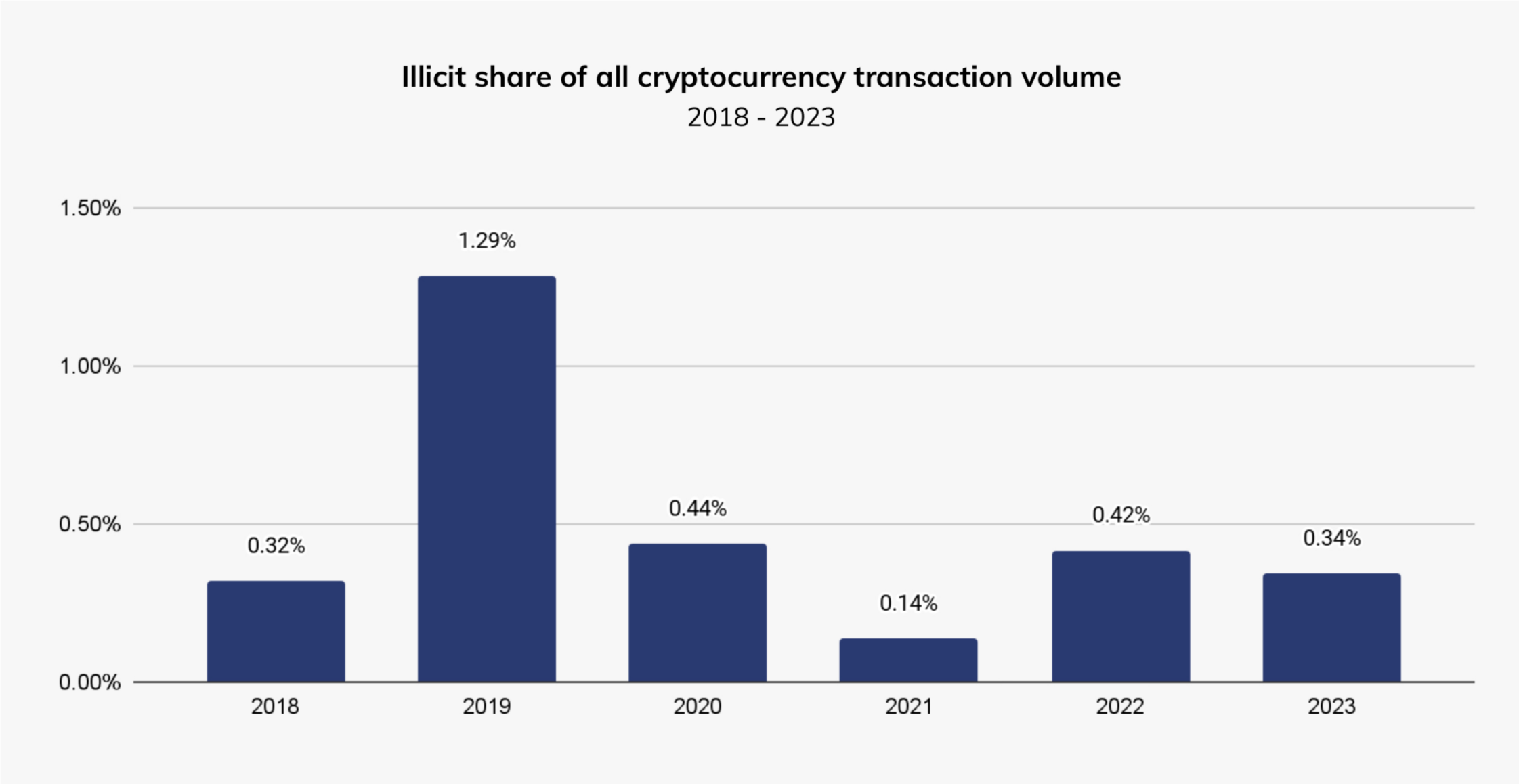



Source: McKinsey

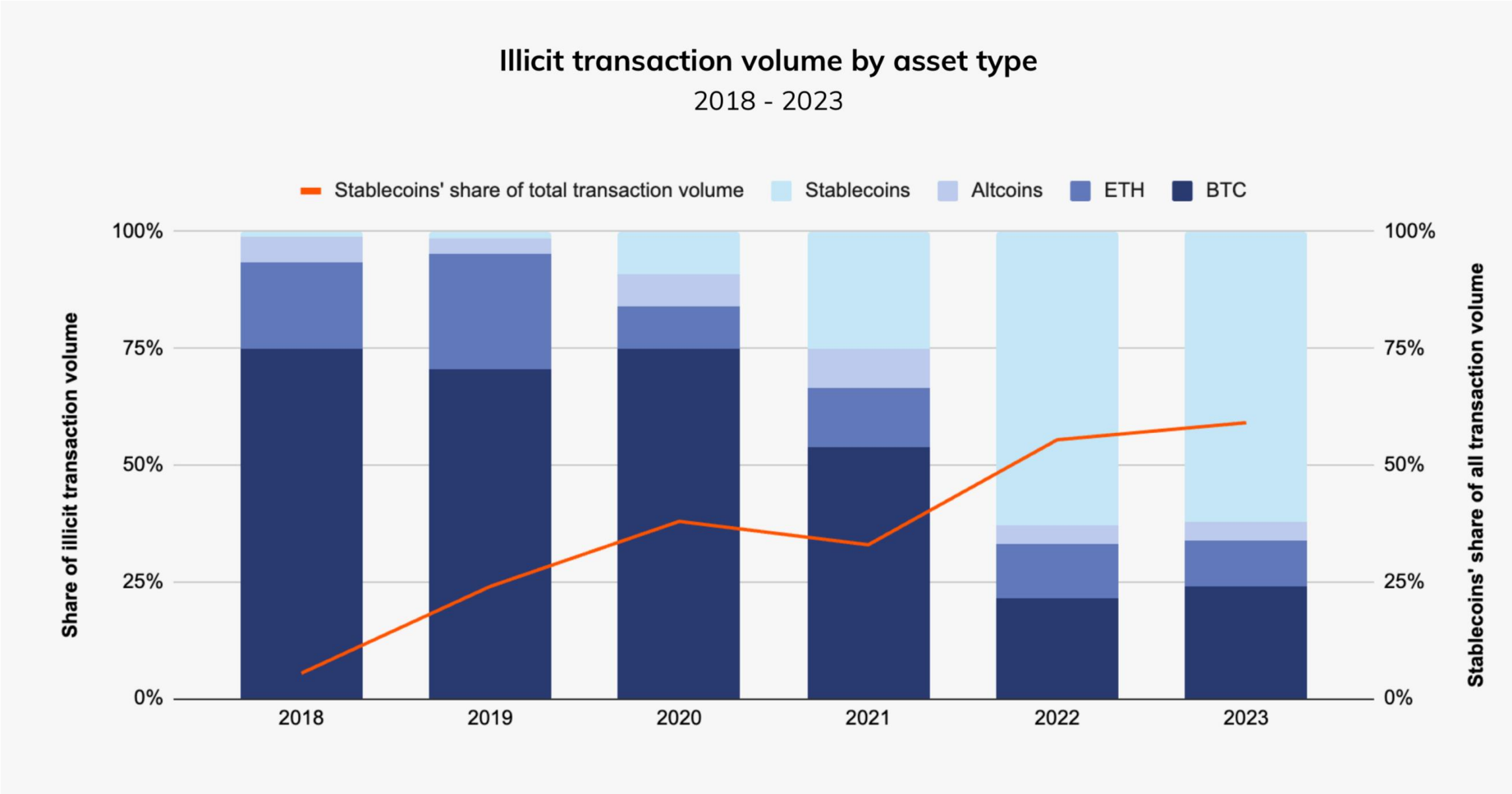
# Coming next: Zoom into crypto crime…




Source: Chainalysis



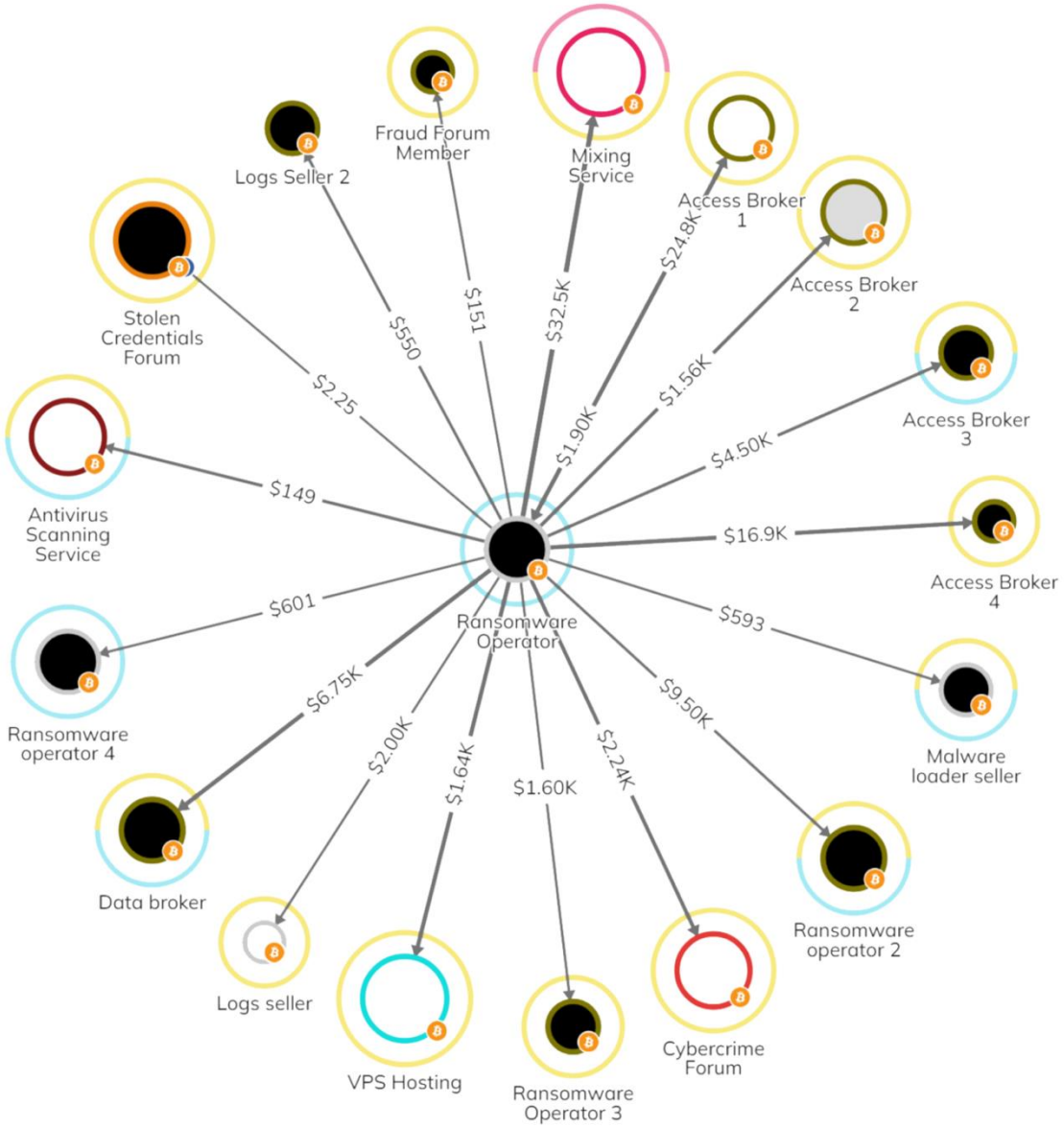

Source: Chainalysis



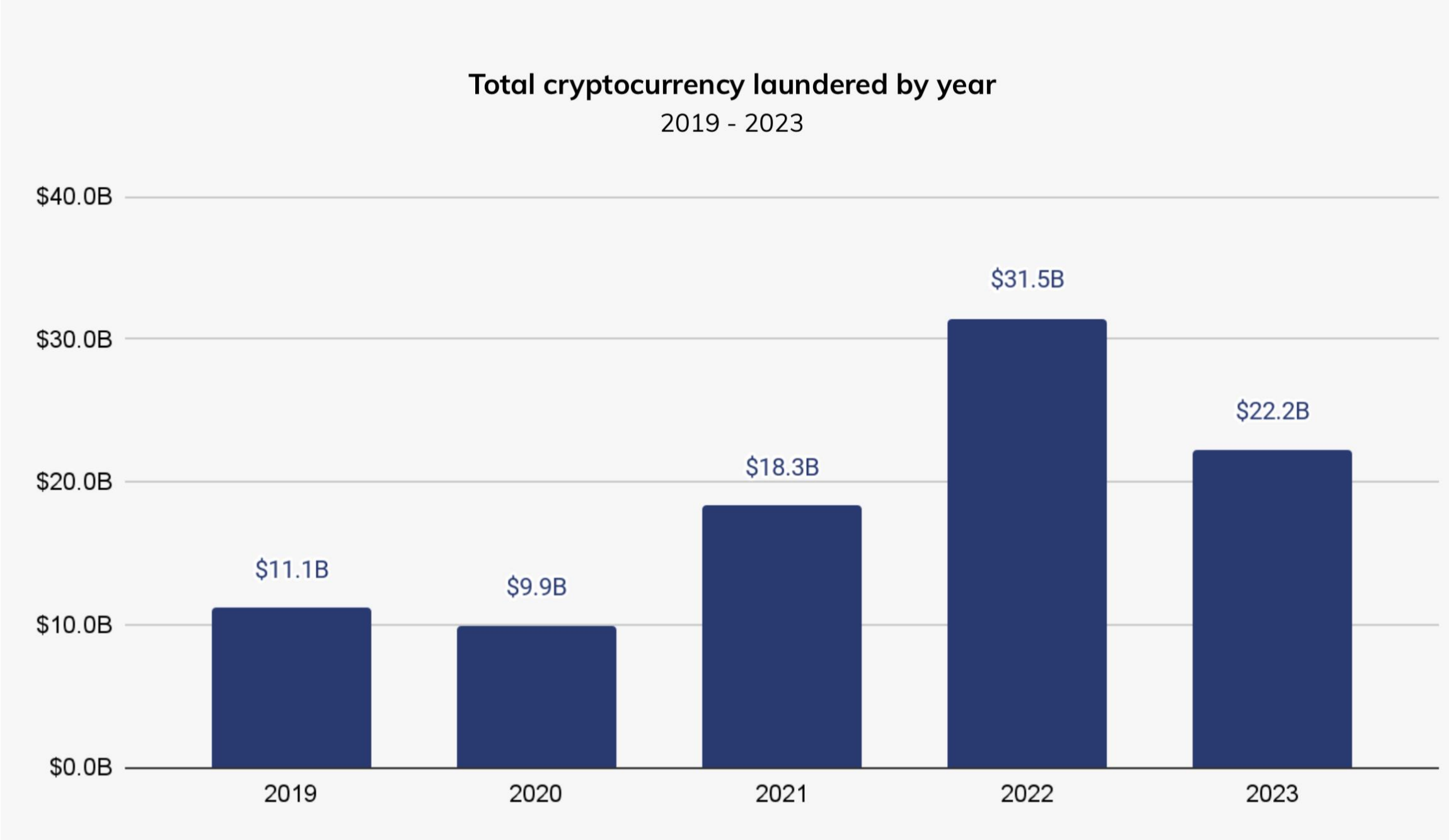

Source: Chainalysis

# The spread of Ransomware-as-a-Service (RaaS)

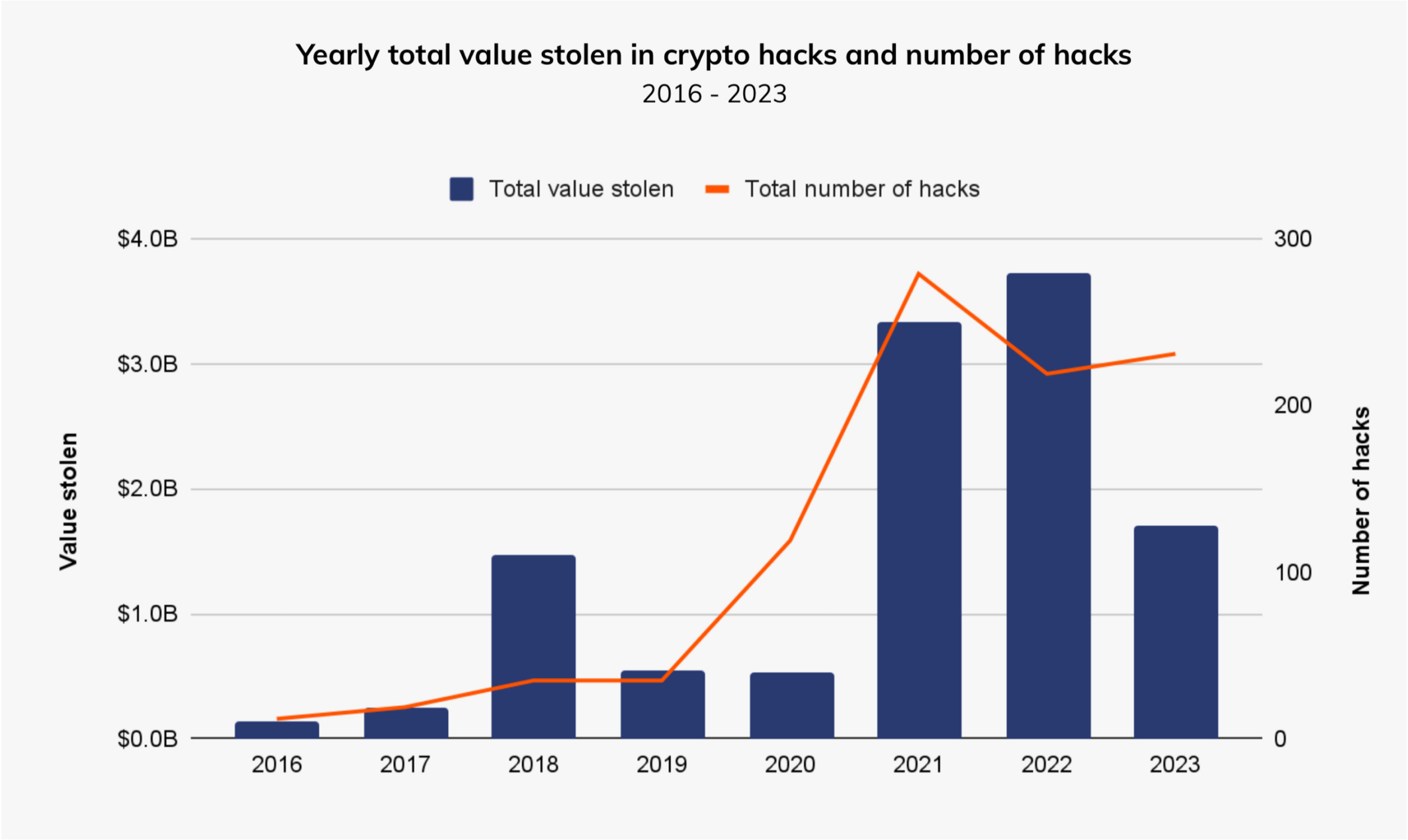
The Reactor graph on the right size shows a ransomware operator sending funds to several initial access brokers and other purveyors of tools useful for ransomware attacks



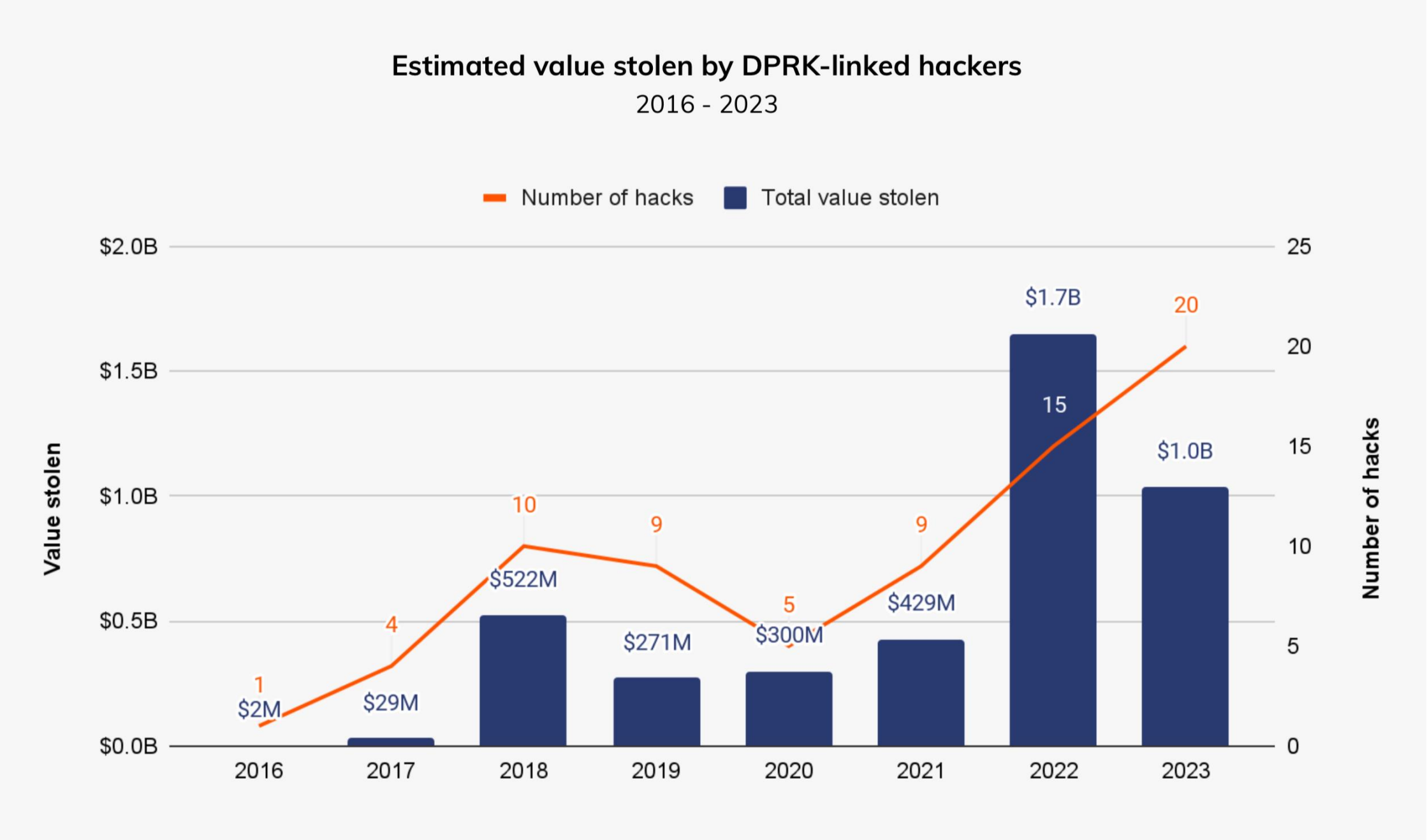

Source: Chainalysis




Source: Chainalysis

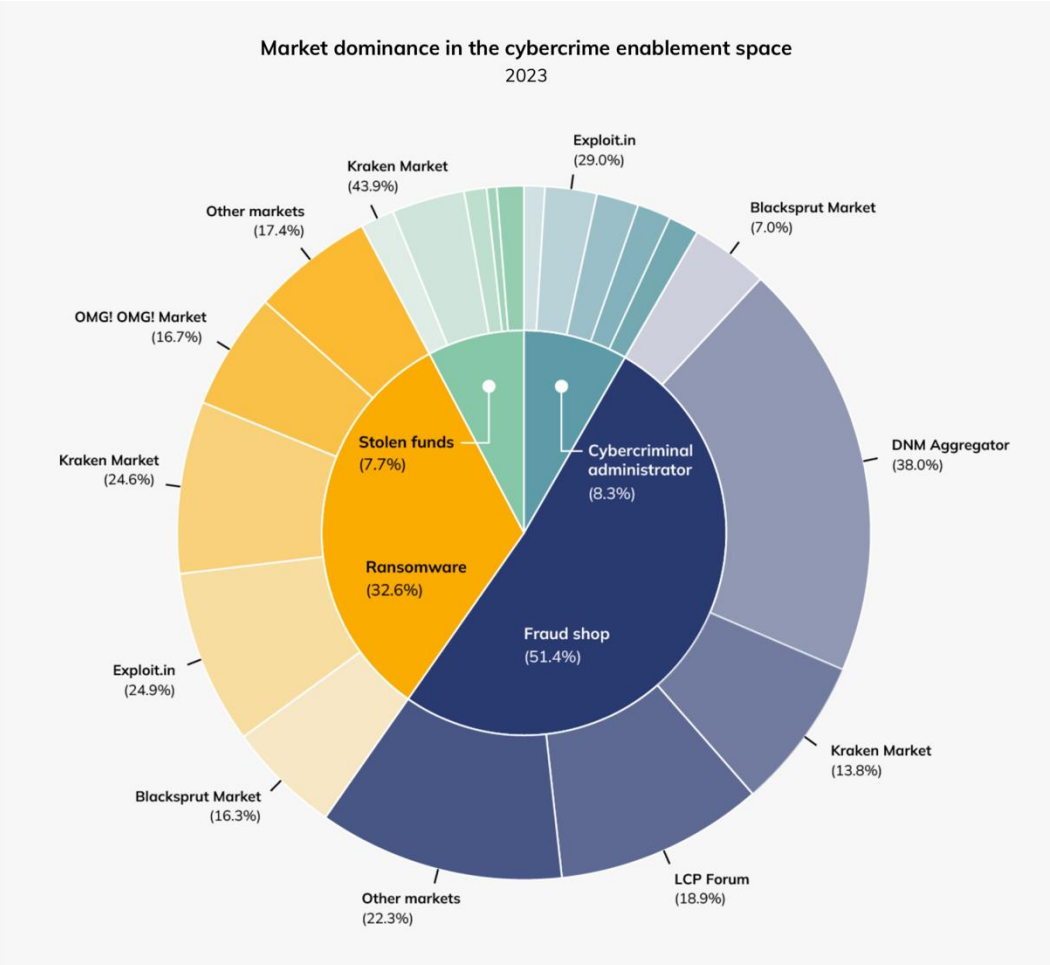


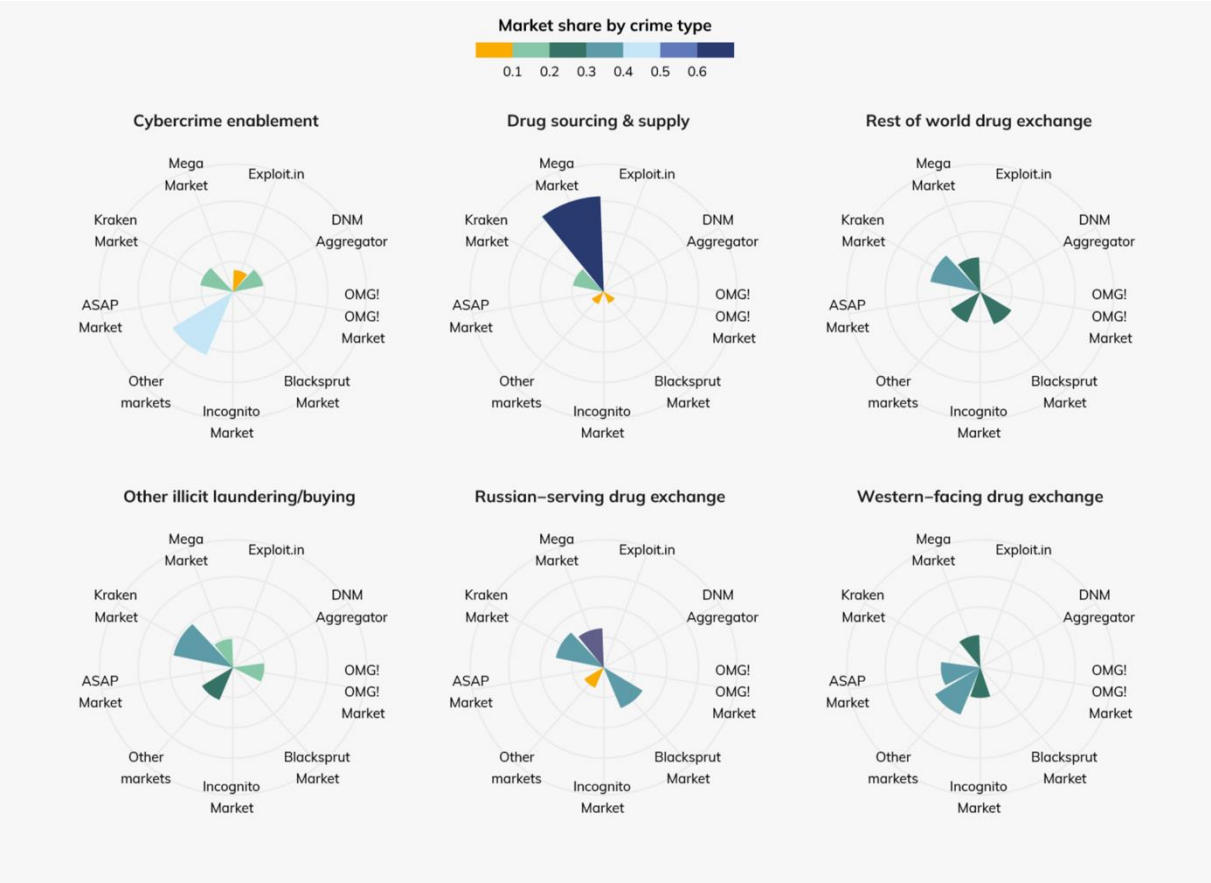

Source: Chainalysis




Source: Chainalysis

# Honey pot for the class' data analysts ☻




Source: Chainalysis

# Thank you

Szabolcs Szalay

February 2025