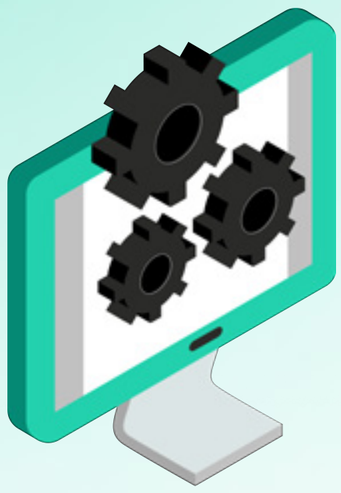
# External attack surface

and ongoing cybercriminal activity in APAC region

2022

kaspersky

# Executive summary



Cyberattack can be prevented before an attacker is inside the internal network. Threat monitoring allows you to take action and properly neutralize a threat before it can exploit any existing vulnerabilities and affect the company.

The public disclosure of PoC exploits and easy exploitation of some of the vulnerabilities have led to many attacks occurring daily in the world. China, India and Indonesia, more than any other countries in the APAC region, are at risk of being attacked through public exploits at any moment.

Right now, attackers prepare to attack, exchange data, and get money on the Darknet. Australia, India, mainland China are the most mentioned countries. Cyberattacks are being prepared against companies from these countries, data with their users is sold on Darknet forums, and malware is hidden in their infrastructure. Selling insider services is especially common in India and Pakistan.

Protection recommendations are unique to each company. They depend on the stage of the attack and on the information, the attacker has. Maybe changing password or limit access to several network services will be enough. Or maybe your data has already been lost and is found in one of the available on the Darknet market databases. Then an investigation is needed to understand the reason for what happened.

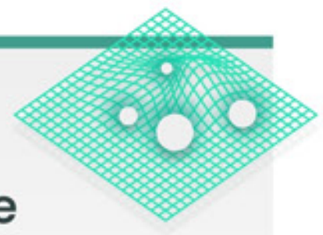
To continue our previous **Digital Footprint Intelligence Report** performed in 2020 for the Middle-East region, the Security Services Analyst team announces research for APAC region. The research results were collected in 2021 within the Digital Footprint Intelligence service that helps organizations and even countries to keep an eye on possible external threats and stay informed about potential cybercriminal activities, including ones being discussed the Darknet. Details on the results and how the service can improve the country-scale cybersecurity can be requested through the following email address: **dfi@kaspersky.com.**

# Introduction

## Digital Footprint Intelligence

Digital Footprint Intelligence is an intercrossing of external attack surface analysis, Darknet monitoring and threat intelligence to provide enriched and actionable notifications.

### External attack surface

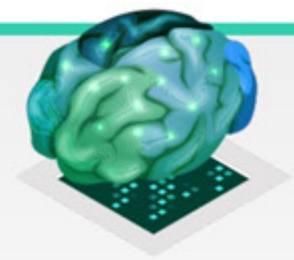


- Identification of infrastructure, human and business assets
- Threat assessment for identified attack surface to perform an attack and impact business

### Darknet monitoring

- Identification of malicious activities with attack preparation
- Identification of already executed attacks
- Identification of attack impact

### Threat intelligence



- Monitoring of active threat actors
- Enrichment of external attack surface and Darknet notifications with TTPs of threat actors

## Scope of the report

We present this report about external threats for a selection of countries from APAC region in 2021. The sole purpose of the report is to create an awareness about security threats, and demonstrate effective approaches to risk mitigation for widespread attacks with high business impact.
**Here are the main figures and anonymized statistics to show the existing and possible threats.**

## 15 countries and territories

From APAC region

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Australia | Hong Kong | Malaysia | Singapore | Bangladesh | India | Japan | South Korea |
| Pakistan | Viet Nam | Indonesia | Philippines | Thailand | Taiwan | Mainland China | |

**>4,700** organizations

**161,068** **IP addresses** with available services[1]

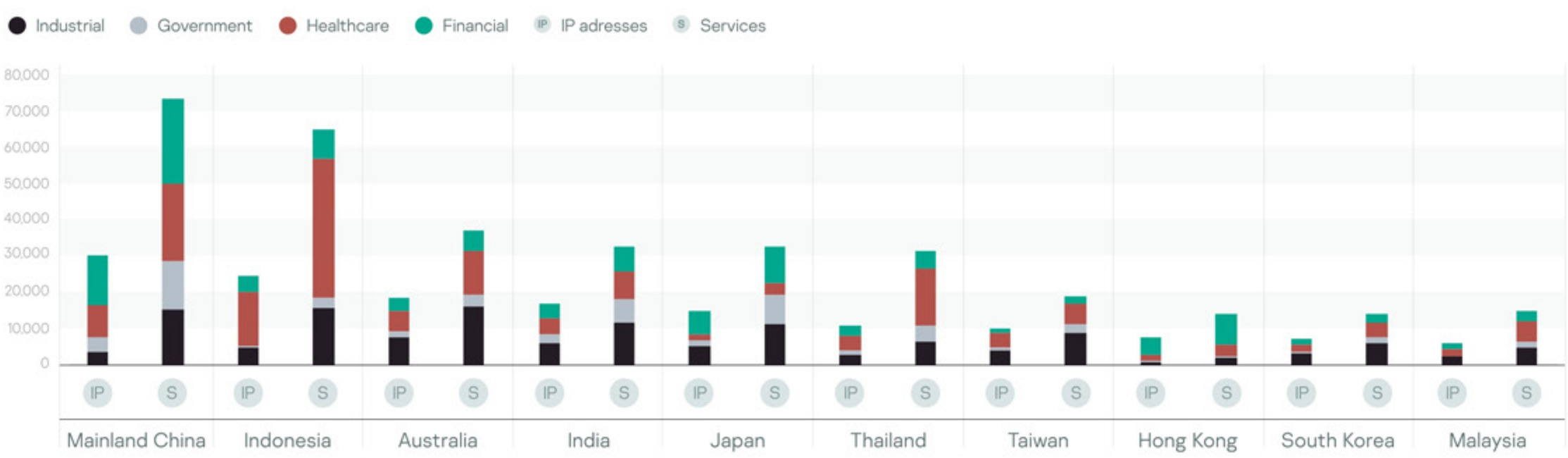
**390,497** **Services**[2]

**Financials**
51,904 IP's
88,987 Services

**Healthcare**
14,273 IP's
46,995 Services

**Industrial**
45,076 IP's
113,117 Services

**Government**
54,442 IP's
140,036 Services




1. Real number of IP addresses belonging to the organizations in scope is much bigger, but we don't count IP addresses without public service (TCP or UDP port)
2. Service is a publicly available application (e.g. Web app, API, remote management interface, etc.)

# Adversaries exploitation capabilities

Rapidly growing share of adversaries' initial access approach is exploitation of 1-day vulnerabilities. Complicated business processes are forced to leave services on the perimeter, which in turn increases the external attack surface. With the help of public sources and specialized search engines we collected information on 390,497 services available from public networks and analyzed them for key security issues and vulnerabilities.

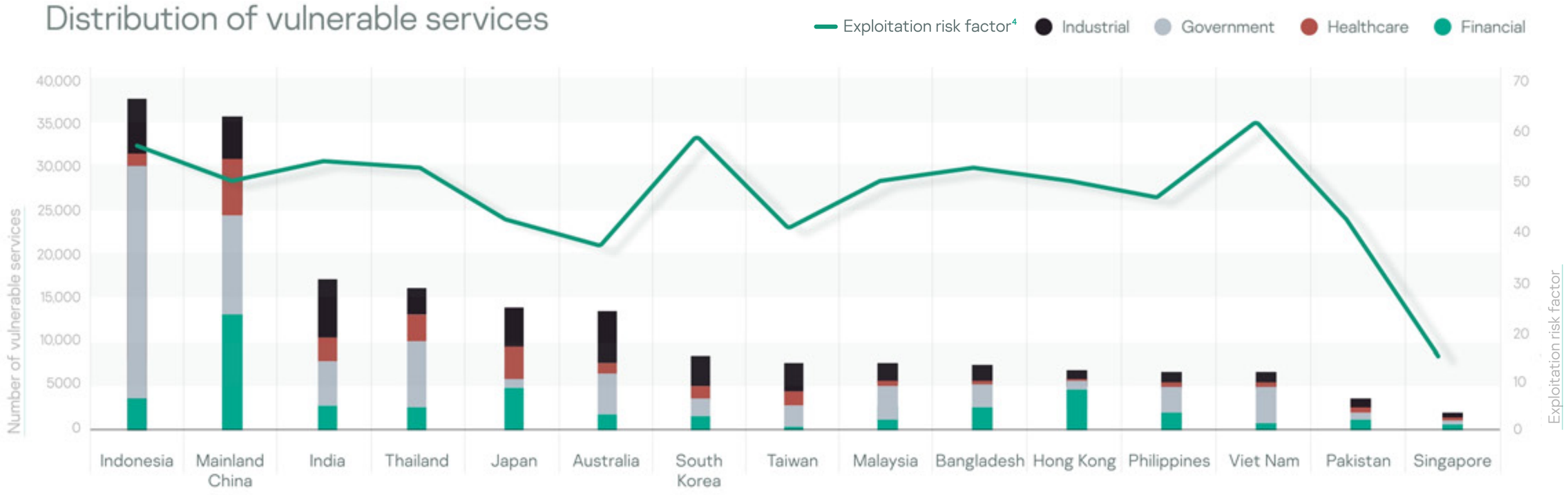
Maturity of an institution is not measured by number of unpatched services, but by the presence of critical vulnerabilities with high impact. There are numerous resources that can help with vulnerability prioritization, but we should seek threat intelligence context, like in Known Exploited Vulnerabilities Catalog. Another great source of actionable data on critical vulnerabilities is analysis of incident response reports, e.g. IR Analyst Report.

**103,058**[3]

**Services with software without security patches**

- Almost every fifth of the vulnerable services contained more than one vulnerability, thereby increasing the chances of an attacker performing a successful attack.
- All industry sectors in all countries have issues with application of security updates for publicly available services.
- Government institutions (major personally identifiable information (PII) processors and providers of critical services for citizens) are potential incident-generators by huge margin.
- Singapore has low number of vulnerabilities and outstanding low ration between the amount of services and the sum of vulnerabilities in them.

Distribution of vulnerable services




**1,073**

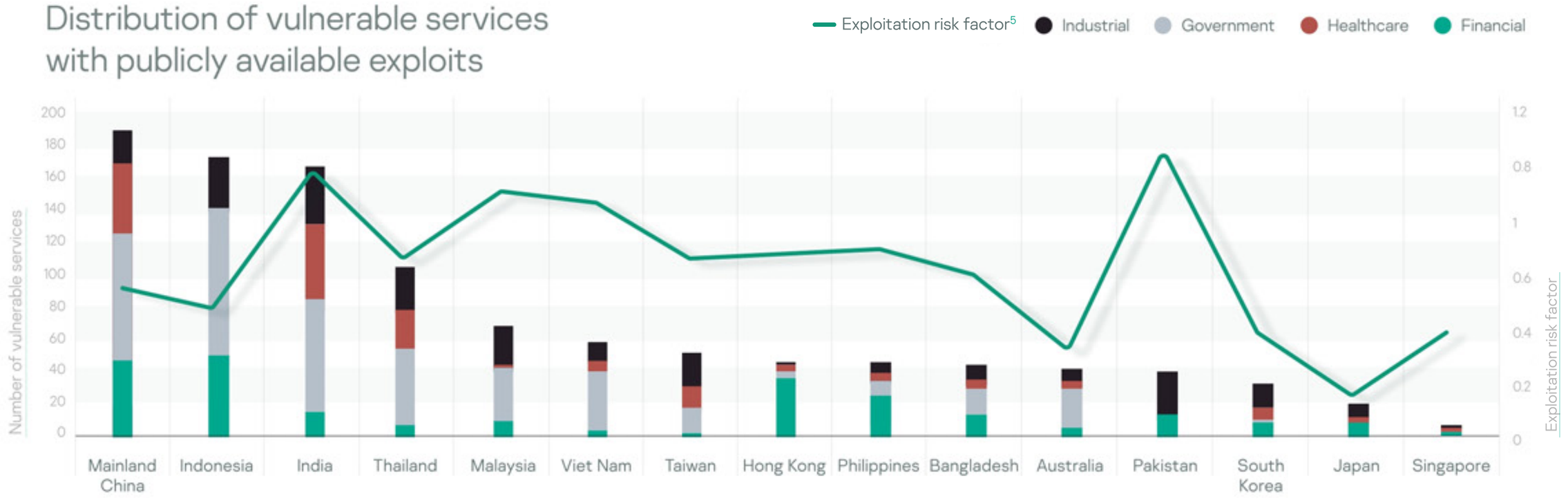
**vulnerabilities with publicly available exploits**

Not all vulnerable services are the same - the same service can be affected by several vulnerabilities at once.

Moreover, for thousands of identified vulnerabilities, it is enough for an attacker to find an exploit on the Internet and run the script.

Philippines, Pakistan, Malaysia, India and Taiwan have bigger share of exploitable vulnerabilities in comparison with other countries and territories.

Distribution of vulnerable services with publicly available exploits




3. The actual number of services running outdated software exceeds this value. However, due to the passive nature of research (data was collected without direct interaction with research targets), some of the widely used critical vulnerabilities can't be identified and/or verified, and some of the findings might be outdated
4. The ratio of detected vulnerabilities number to services available on the perimeter
5. The ratio of detected one-day vulnerabilities number to all vulnerabilities

# Adversaries exploitation capabilities

From our practice in incident response handled by Global Emergency Response Team (GERT) and CISA advisory adversaries use a well-known list of vulnerabilities to exploit organization defenses. For the last year the most interesting vulnerabilities (ProxyShell/ProxyLogon) were related to Microsoft Exchange Server.

### Most affected countries to ProxyLogon:

(for companies from the scope)

**Indonesia**
In Industrial

**Thailand**
In Government bodies

**Philippines**
In Healthcare

**China, Philippines**
In Financials

### Most affected countries to ProxyShell:

(for companies from the scope)

**China**
In Industrial

**Viet Nam**
In Government bodies

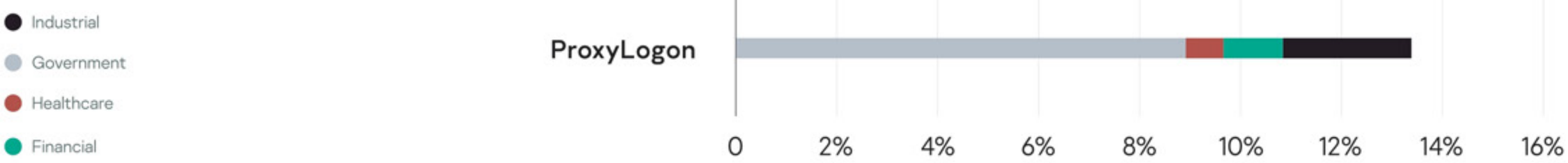
**China**
In Healthcare

**China**
In Financials

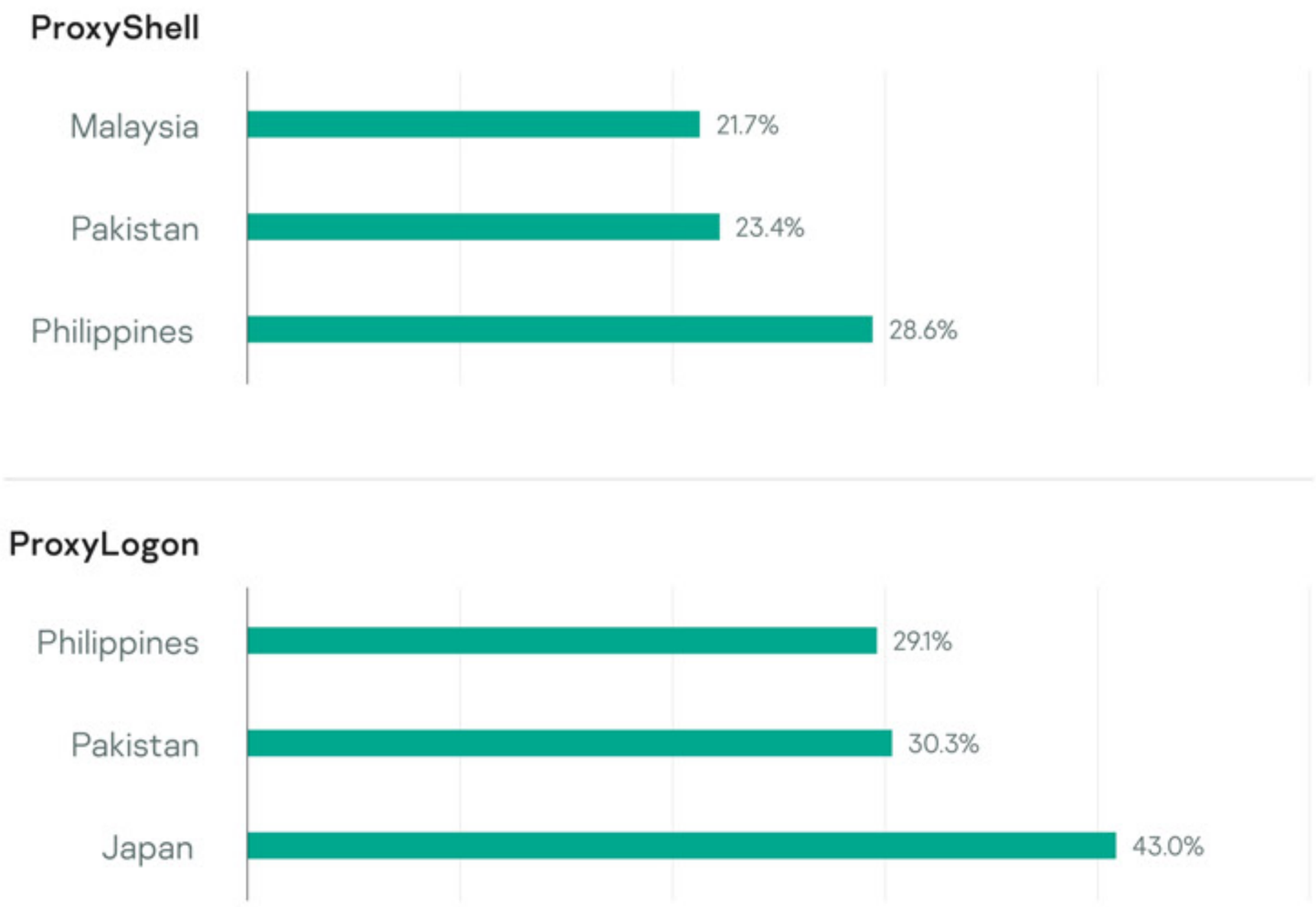
If we review the situation in the whole APAC region (including other industries), we see that every 10th encountered vulnerability on the external perimeter resources was ProxyShell. The most affected country by ProxyShell was Philippines (28,6% of vulnerable services). As for the Proxylogon's greatest impact, 43% of vulnerable services were exposed to it. The best defense against these vulnerabilities is to keep public faced systems updated with the latest patches and product versions. You should also avoid direct access to Exchange Server from the Internet.

## Share of services vulnerable to ProxyShell and ProxyLogon in the whole APAC region

Share of vulnerable services on Regions (%)




Share of vulnerable services on Country (%)



# Adversaries account-based capabilities

Available network services of organizations might provide an attack opportunity for the adversary even without being vulnerable. Great share of attacker's initial accesses leading to cybersecurity incidents are related to services with remote access or management features (RDP[6], SSH[7], VNC[8], etc.). Attackers can take advantage of credentials brute force, but it's a security-event-wise noisy one. Another approach is acquiring valid credentials from the start by contacting initial access brokers (IABs) who basically offer these data for sale on the Darknet.

Usually these valid credentials were gathered from infected devices by using stealers as Vidar or REDLINE. Security verdict is straightforward: if you have similar service and rely on password-based authentication only - you are either already compromised or will be in the nearest future.

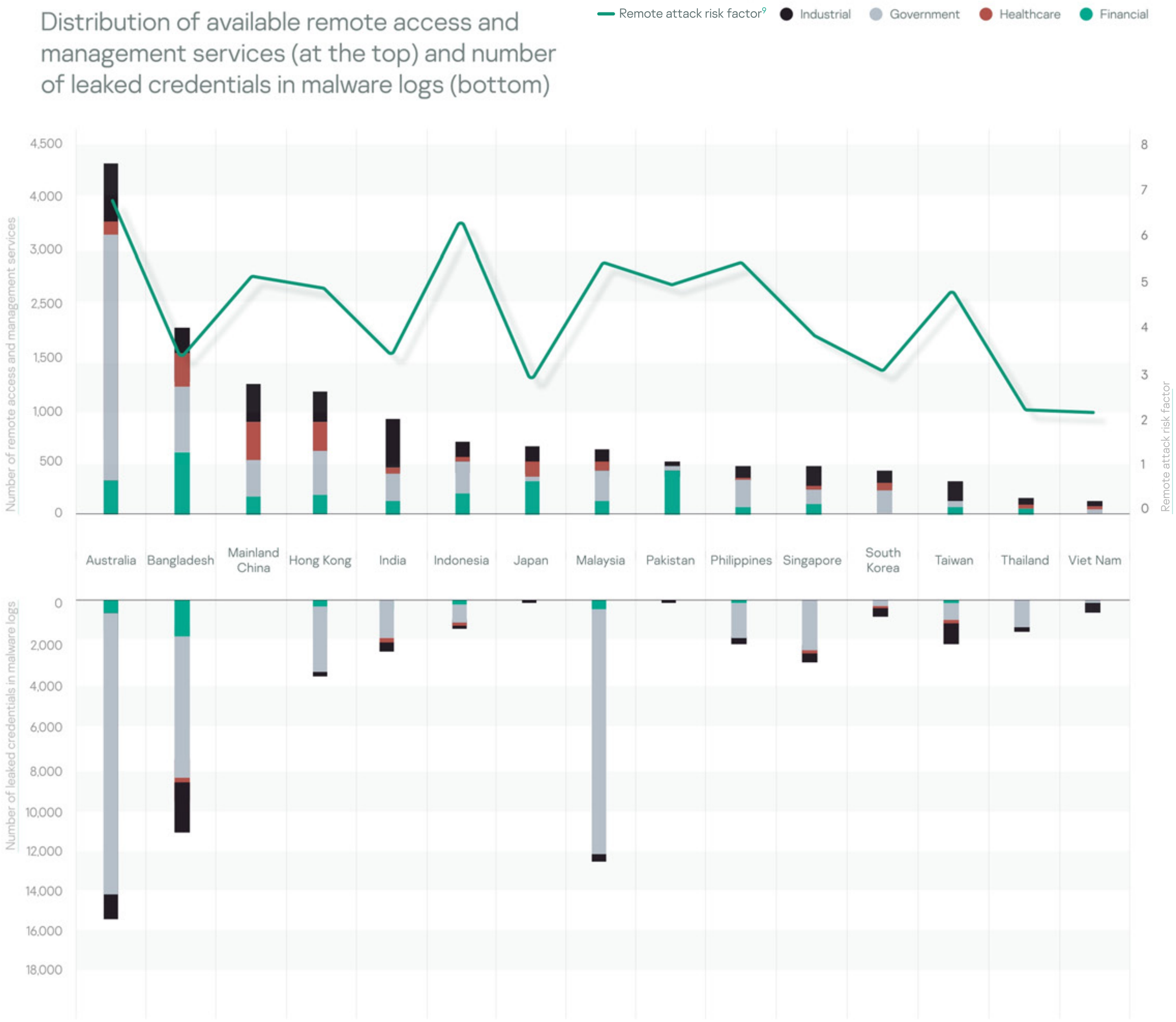
**16,003**

**remote access and management services are publicly available**

Indonesia, India, Bangladesh, the Philippines, and Viet Nam provide the maximum facilities for an attacker to gain remote access.

Government institutions are serving more than 40% of attack surface for brute force attacks and credential leaks reuse.

Distribution of available remote access and management services (at the top) and number of leaked credentials in malware logs (bottom)




6. Microsoft Remote Desktop Protocol
7. Secure Shell
8. Virtual Network Computing
9. The ratio of remote access and management services number to services available on the perimeter

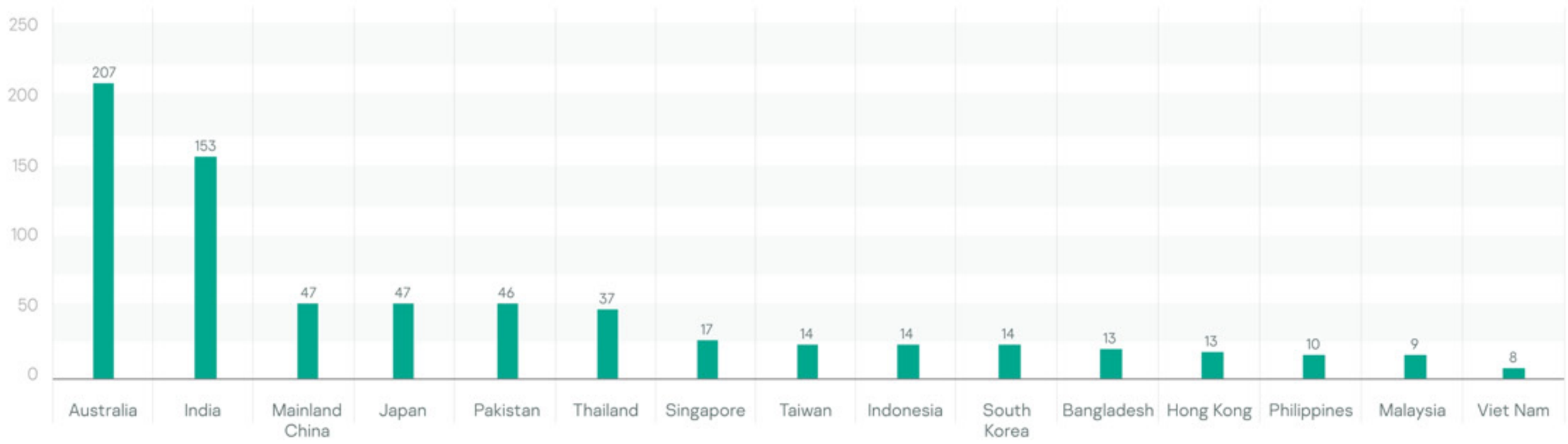
# Adversaries account-based capabilities

**1,116**
**initial access brokers deals**

Sell and buy orders demonstrate major countries of interest for adversaries: Australia and mainland China.

Initial access brokers are active in countries with the highest numbers of vulnerable software and available remote access services.

Number of IAB ads shared by countries




## Examples of initial access brokers sell orders

#1

05.06.2022

**Wolverine**
HDD-drive

User

| | |
|---|---|
| Registration: | 18.01.2022 |
| Messages: | 43 |
| Reactions: | 15 |

Selling access to the Thai branch of the corp of the industrial sector.
**VPN-RDP**

Access: **Domain Admin**

Hosts: **66**

Country: **Japan/Thailand**

Price: **$600**

Details in PM, sale through a guarantor, bargaining is appropriate.

Last edit: 05.06.2022

Complaint | Like | Quote | Reply

# Types of Darknet data

Monitoring of external sensors in our Digital Footprint Intelligence service, such as Darknet resources, C&C servers, malicious activity and public sources provides insights into cybercriminal activity through different stages of attack lifecycle. In this report we highlight Darknet analysis results only[10].

There are two major types of data found when analyzing organization's digital footprint: fraudulent activities and cyberattack footprints. While we discover numerous fraud signs, our focus in the report is on attack detection.

## Darknet data

The amount of adverts in Darknet for 2021

**40,819**
**Cyber attack footprints**

**467**
**Attack preparation**

Buy order for access to the company's resources published on the Darknet forums (accounts for access through RDP, SSH, other credentials, activity of insiders)

| | |
|---|---|
| Access buy orders | 467 |

**1,610**
**Attack executed**

Initial access brokers activity (credentials sales) on the Darknet, insider selling access to the network, malware logs with domain credentials

| | |
|---|---|
| Creditential leaks from malware logs | 674 |
| Access sell orders | 649 |
| Insider activity orders | 287 |

**38,742**
**Attack impact**

Sale of the company's databases (employees, clients, contractors), sale of the sensitive documents including top-managers mailboxes, ransomware blog post with call for disclosure of sensitive company's data

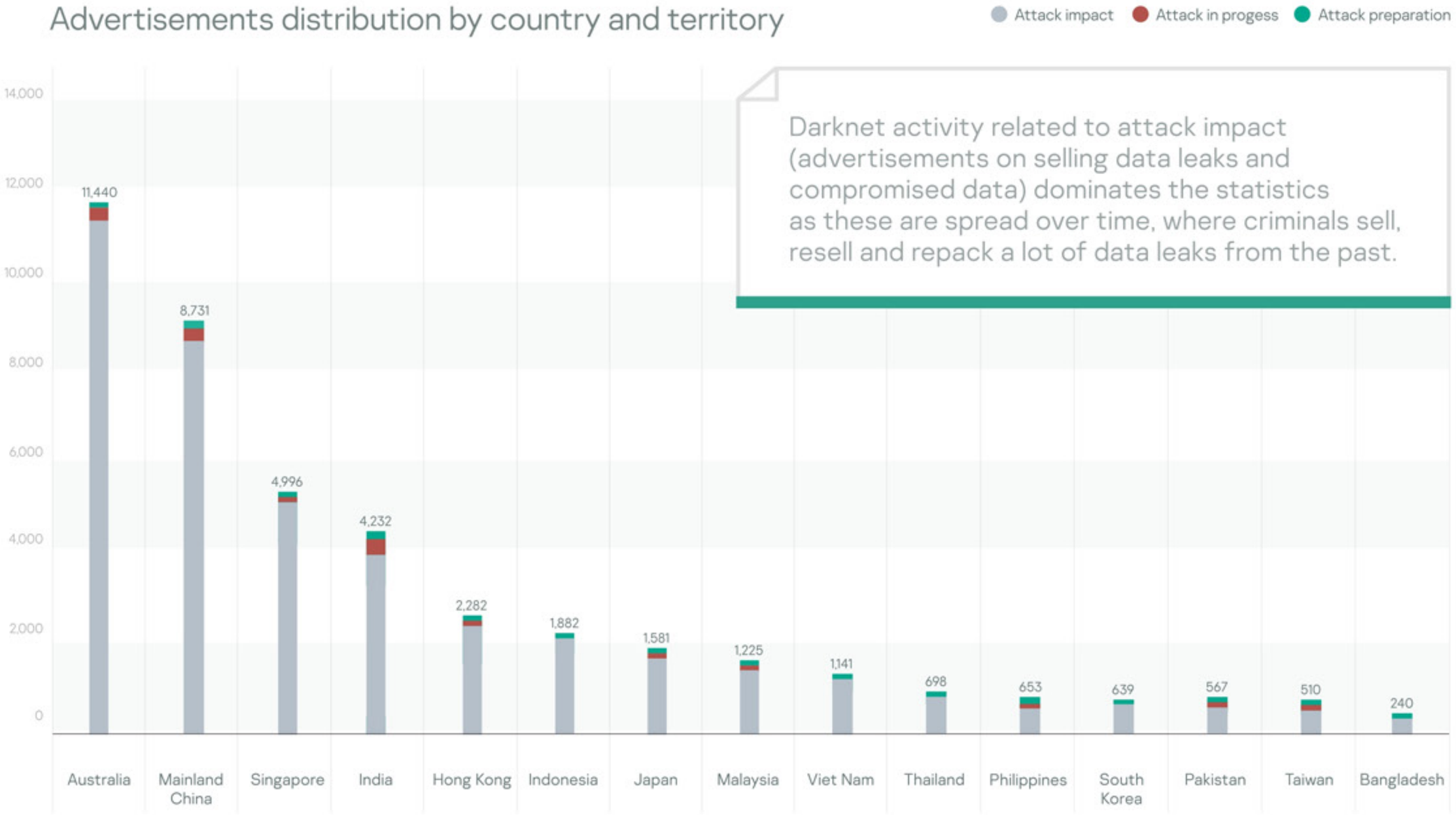
| | |
|---|---|
| Insider activity orders | 287 |
| Credit card and withdrawal | 5,865 |
| Database leaks | 32,590 |

**19,820**
**Fraudulent activities**

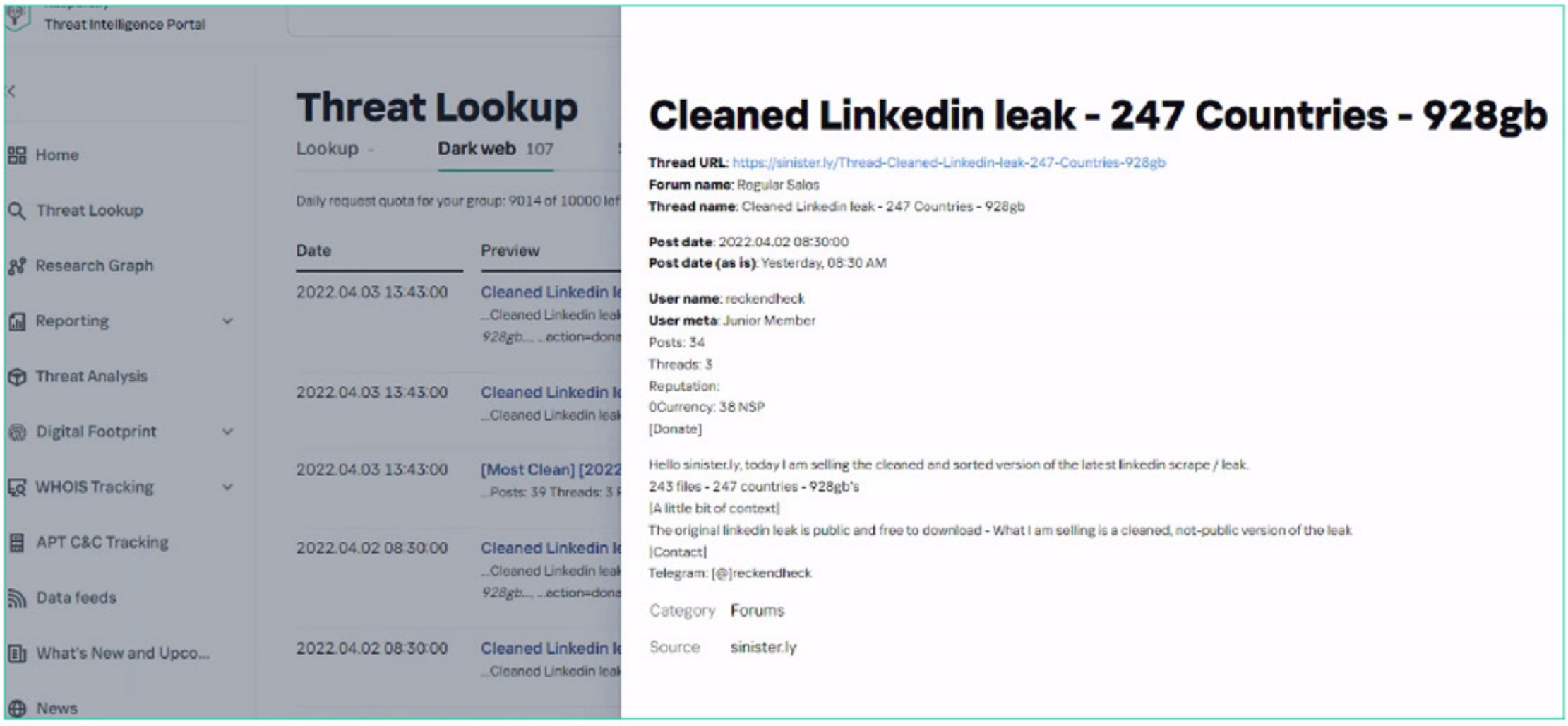
| | |
|---|---|
| Credit card and withdrawal | 5,865 |
| Document fraud service | 5,415 |
| SIM card orders | 4,605 |
| Information gathering services | 3,648 |
| Insider activity orders | 287 |

10. In total, more than 120,000 messages were found, but only half of them could be automatically categorized.

# Types of Darknet data



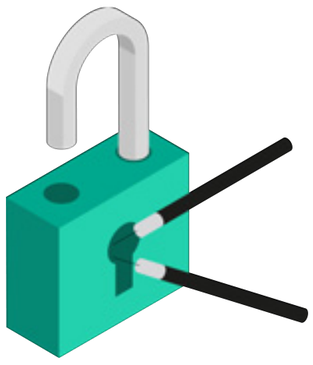

## Database selling order example




Source: Kaspersky Threat Intelligence portal

# Attack preparation

Stating interest to compromise somebody's resources usually doesn't contain useful threat intelligence data and only in a minority of cases can the topic starter (adversary) be linked to his previous attacks with actionable TTPs. Threat intelligence is the ''silver bullet" in the defenders arsenal to detect Reconnaissance and Resource Development techniques[11][12] before the attacker initiates the attack and gets initial access to the company. For mitigation negative impact it is better to be already prepared and broad action list can be taken already at this stage: personnel training, systems hardening, running compromise assessment projects.



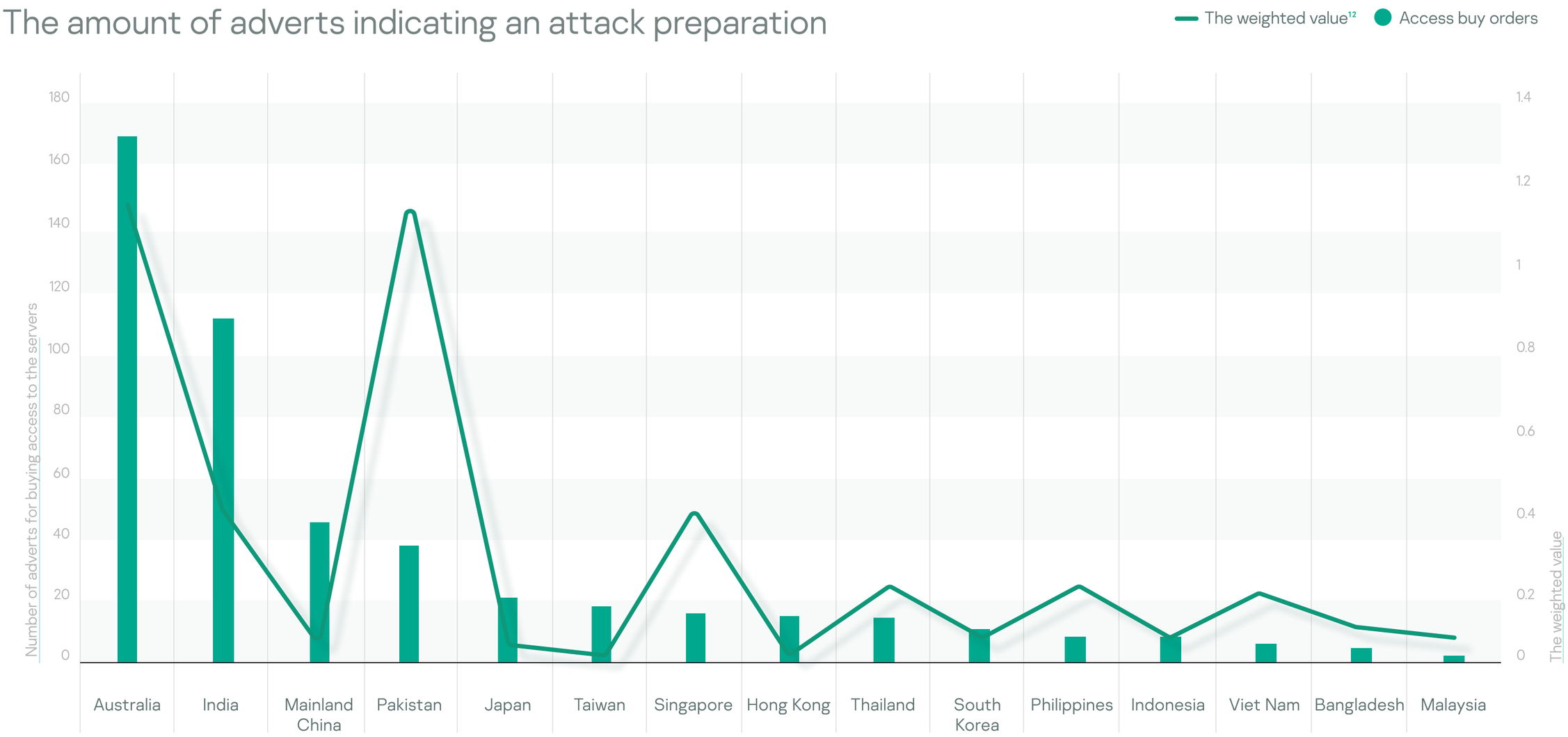
**Organizations from Australia, India, mainland China and Pakistan are the major adversaries' interest to start an attack.**

These countries were present

**in 84% of ads**

from the attack preparation category.

The amount of adverts indicating an attack preparation




Pakistan and Australia attract huge interest as seen by the number of orders weighted with their GDP[13].

Looking at the size of infrastructure, businesses, and industrialization - mainland China poses relatively low interest for adversaries. This may indicate the presence of a language barrier cybercriminal scene in the APAC region or the complications with network-level access to organizations in the country.

**Insider activity buy orders**

Request to buy insider services can lead to credentials or data leaks, source of information gathering service (e.g., PII data exfiltration by request). Those orders are the most inconclusive type of findings for remediation planning.

**Access buy orders**

Request to buy access to a single or a list of specific organizations or industries in a specific region.

11. Knowledge base of adversary tactics and techniques on https://attack.mitre.org/
12. The weighted value is the ratio of adverts number to GDP
13. We use GPD from https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?view=chart

# Attack preparation

**Examples of access buy order** #1

**GitDump**
Byte
Paid registration (**0**)

| | |
|---|---|
| Registration | 17.01.2022 (ID:124 391) |
| Publications | 5 |
| Activity | hacking |

Published 11 hours ago

look for seller account hostpoint and hosteurope and seller shell .jp i take all account and shell u have ready contact me [redacted]

i need urgent

Complaint Like Quote Reply

**Examples of access buy order** #1

**Benso**
Work
Paid registration (**3**)

| | |
|---|---|
| Registration | 28.03.2021 (ID:115 422) |
| Publications | 62 |
| Activity | hacking |

Published 17 hours ago

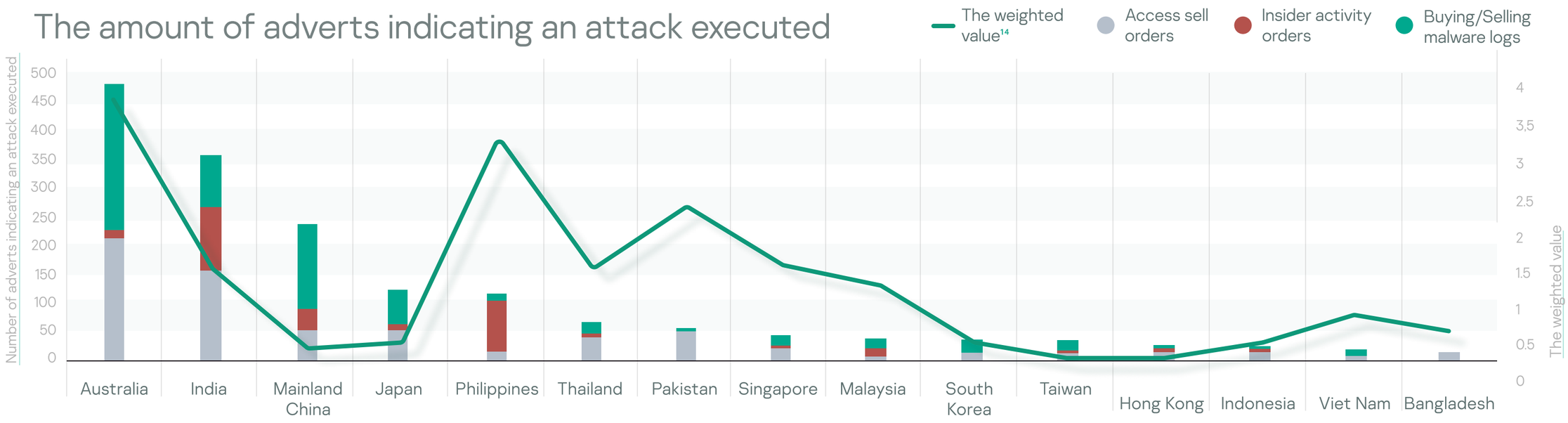
Greetings,
I will buy your access to corporate networks, interested in any type of access (RDP, VPN, cisco, citrix, etc) but RDP level access with admin privilege's is preferred, only interested in corp's with a revenue higher than 30kk. countries that will be given preference are: USA, CA, JP, EU (not interested in any other country, unless the revenue is especially high), not interested in: hospitals, government organization's, institutions for education (schools universities colleges etc),

To not waste either of our time, please write what access you have in store and your price for them, and list the foilwing details: what type of access, what level of privilege's you have, and what price range you think the access is worth.  Payments from 5k upto and beyond 20k.

Complaint Like Quote Reply

# Attack executed

The most promising findings are from attack execution stage: artifacts are stating that adversaries have capabilities or already have access to organizations' networks or services, but there is no business impact yet. While there is no clear place to start an incident investigation, there are leads as account credentials that can be effectively used for threat hunting or compromise assessment, and for easy-to-implement remediation steps: change passwords, enable 2FA, and monitor account activity with increased priority.




Australia, India, mainland China and Philippines cover 75% of detected adverts.
Potentially these ads can lead to impact phase.
Philippines, Pakistan, Singapore, Australia and Thailand organizations are most attacked when weighted with GDP.
Philippines, India and mainland China are dominating the insider services market with 82% of orders turnover.


## Initial access brokers

Sell orders for a specific organizations, or bulk orders with organizations grouped by industry and/or region. Especially appreciated access to Active Directory domain through valid credentials that can be applied to existing remote access or management service.

## Insider activity sell orders

Request to sell insider services can lead a credentials leak, source of information gathering service (e.g. PII data exfiltration by request), or data leak. The source is usually an insider's broker.

## Malware logs

Credential stealing malware (stealers) collect credentials into resalable or otherwise accessible data with account usernames and passwords. Sometimes these log files can be found freely accessible on the Surface web and Darknet.

### AN EXAMPLE OF ACCESS SELL ORDER

lnthematrix1
Byte
Paid registration (**14**)

| | |
|---|---|
| Registration | 25.06.2020 (ID:105 713) |
| Publications | 16 |
| Activity | Carding |
| Депозит | **0.002488 B** |

Posted: 11 March

Access to a windows server 2019 datacenter location Sydney Australia via RDP Inside there are 2 different people that do trading on binance exchange

Gmails already login insde both chrome and firefox . Last transaction i see they buy BTC with RelayPay on 1st of march , ammount 0.175BTC- 9500$ AUD
Also there is telegram on desktop , they are login in clicksend where they receive sms code confirmation for relaypay

Additional info they have transactions with commonwealth bank . [redacted]

Start: 2000$
Step : 200$
Blitz : 4000$

pps : 4h

Complaint | Like | Quote | Reply

14. The weighted value is the ratio of adverts number to GDP

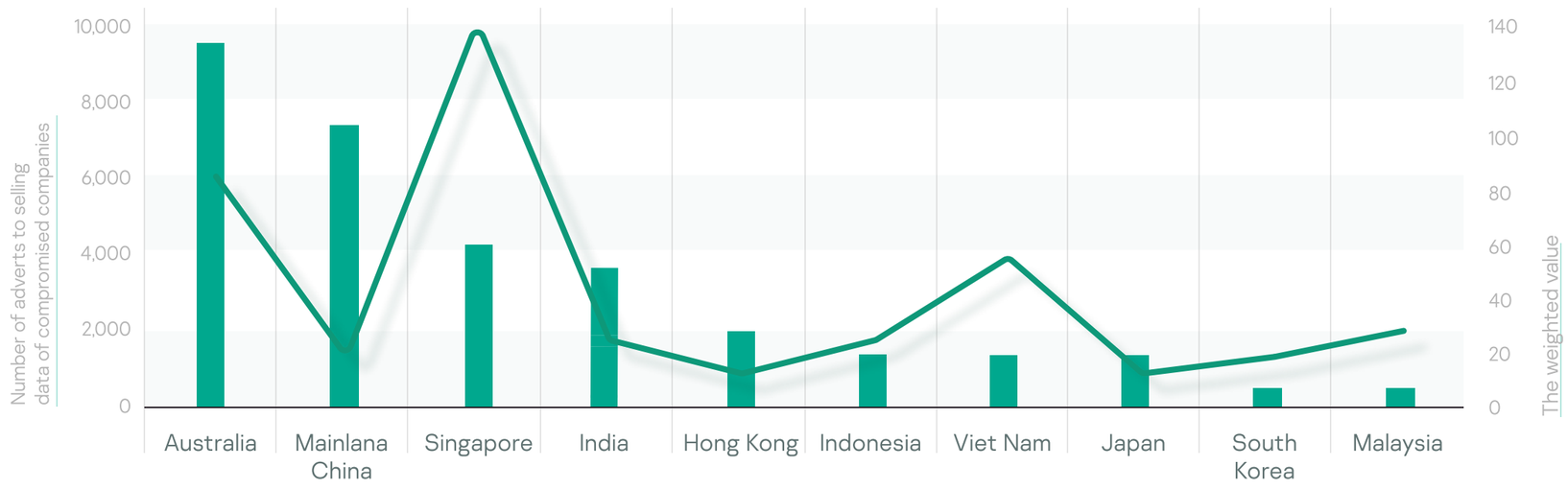
# Attack impact

While an attack has already happened - there are specific artifacts that should point to a compromised system to start incident response. It's time to investigate the attack, recover systems, takedown leaks and plan SOC development based on lessons learned from incident response.

## The amount of adverts indicating a compromised system

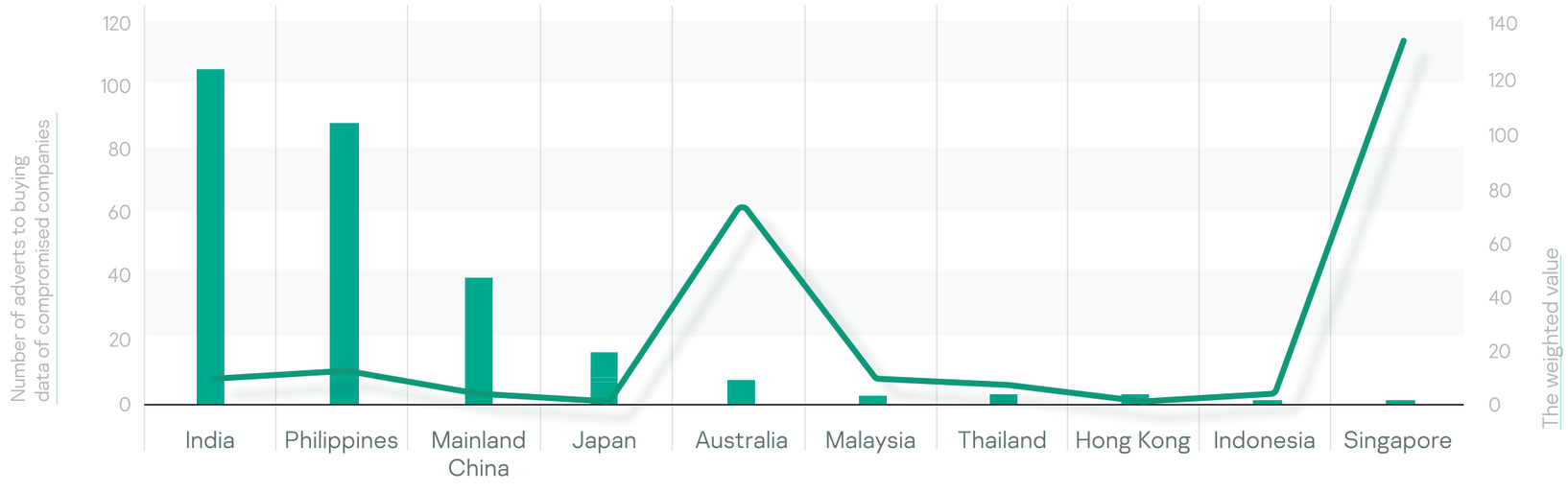
### Data leaks

Confidential data leak initiated by an insider.




### Insider activity orders

Sale or free access to any type of organization's internal data, including, but not limited to databases, confidential documents, PII, credit cards, VIP information, financial data and many others.



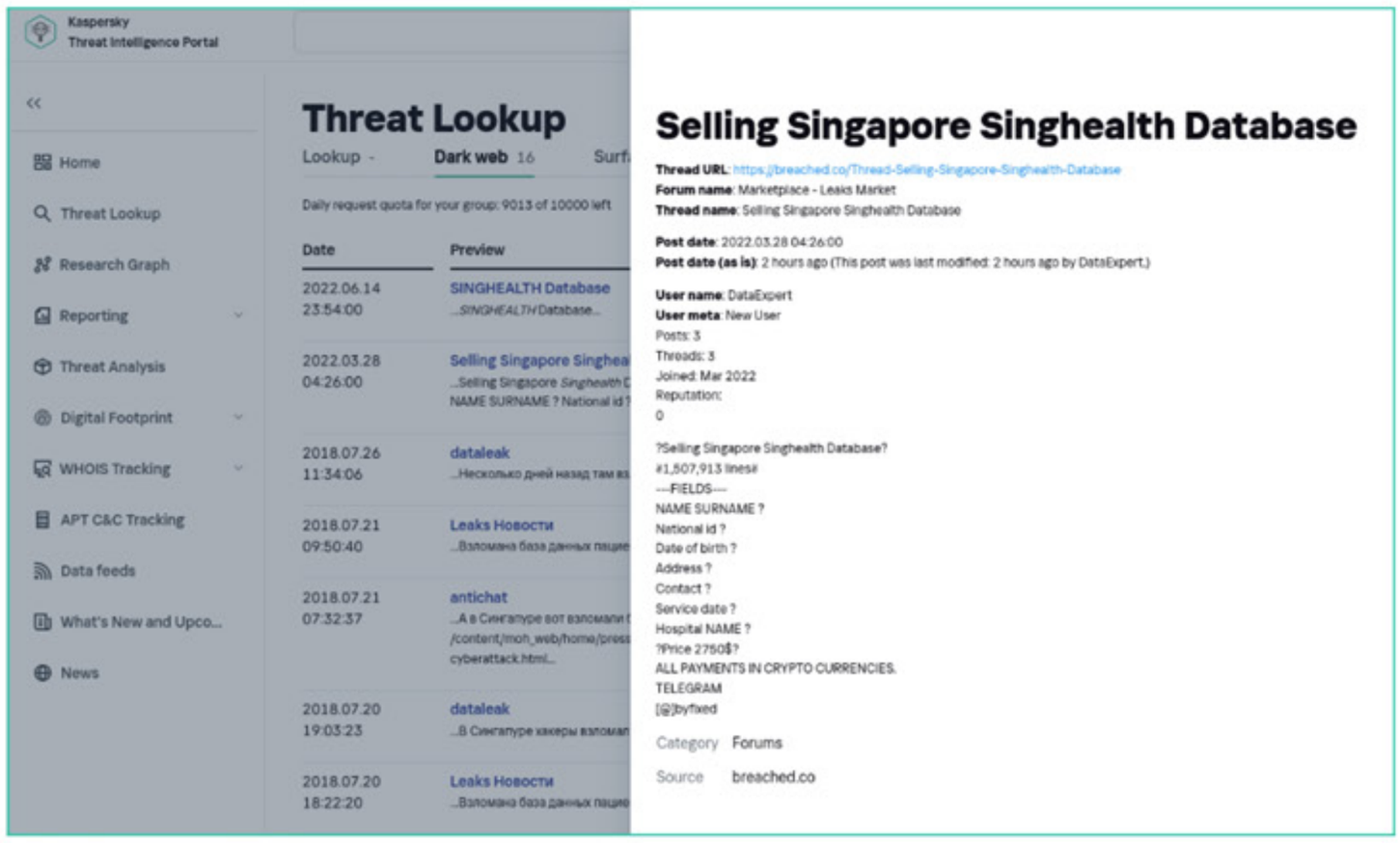

Organizations from Australia, mainland China, India and Singapore take 84% of all data leaks sell orders placed on the Darknet.

Singapore's and Australia's data leaks market are by far the largest when looking at the weighted with GDP amounts of orders.

It should be noted, that Philippines, Pakistan, and Thailand organizations were among the adversaries interest to begin an attack or appeared as already compromised, but the amount of data leaks is on par with other countries from the middle of the group.

### Selling Singapore Singhealth Database

Database selling order example (Source: Kaspersky Threat Intelligence portal)




15. The weighted value is the ratio of adverts number to GDP

kaspersky

# Digital Footprint Intelligence

2022