

Threats Landscape

2021



Guidelines

- 01 Introduction
- 02 Global Attack Trends
- 03 KSA Statistics
- 04 sirar Battles

Glossary

Cybersecurity

Gives protection against the criminal or unauthorized use of electronic data or the measures taken to achieve this.

Cybersecurity System Integration

Gives you powerful tools to implement automation and digitalization of business processes. Optimize, exchange data across any apps and It systems.

SOCaaS

security operations centre (soc) as service provides an industry leading 24/7 proactive monitoring and detection services which helps organizations to detect cyber threats proactively. It combines a team of skilled experts, cutting edge technologies, best practice processes, tools and services offered to provide monitoring, detection, prevention, protection, and response to cybersecurity incidents.

Dwell

The time between an attacker's initial penetration of an organization's environment and the point at which the organization finds out the attacker is there

Ransomware Attack

Is where a malware designed to deny a user or organization Access to files on their computer. By encrypting these files and Demanding a ransom payment for the decryption key.

NPM Repository

It serves as a package manager and online software repository for open-source node.js projects. User can interact with the repository through a command-line tool to assist with package installation, version management, and dependency management.

Mandiant

Provides public and private organizations and critical infrastructure worldwide with early threat insights through unmatched intelligence and response expertise for the highest-profile incidents.

Fin12

Is a russian based ransomware

Trickbot

Is malware designed to steal banking information.

DDoS

A distributed denial-of-service (ddos) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of internet traffic.

MITRE ATT&CK

MITRE ATT&CK (Adversarial tactics, techniques and common knowledge) is a framework, set of data matrices, and assessment tool developed by mitre corporation to help organizations understand their security readiness and uncover vulnerabilities in their defences. Supply-chain.

Supply-Chain

Also called a malicious actor or backdoor breach, is when threat actors hack an organization's supplier or third-party vendor that has access to a company's data to eventually infiltrate the targeted organization's network.

Malware

Is software that's specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

Njrat

The "njrat" remote access trojan is a popular password stealing Remote control applet used mostly by threat actors in the middle East.

Ai security

Are the tools and techniques that leverage artificial intelligence (ai) To autonomously identify and/or respond to potential cyber threats based on similar or previous activity.

Phishing Attacks

Are when attackers try to trick users into doing 'the wrong thing', such As clicking a bad link that will download malware, or direct them to a Suspect website.

Cyber architecture

Also known as network security architecture, is the practice of designing computer systems to assure the security of your underlying data. Cybersecurity architecture is at the foundation of your organization's defence against cyber threats.

Zero trust security

Sometimes known as perimeter less security zero trust is a security Framework requiring all users, whether in or outside the Organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data.

Dark web

Is the part of the world wide web that's only accessible by means of Special software, allowing users and website operators to remain Anonymous or untraceable.

NTP

Network time protocol network time protocol is an internet Protocol used to synchronize with computer clock time sources in a network.

UDP

User datagram protocol refers to a protocol used for communication Throughout the internet. It is specifically chosen for time-sensitive Applications like gaming, playing videos, or domain name system (dns) lookups.

DNS Servers

It is domain name server it is a system that work as the phonebook of the internet, by matching external server ips with website domains

VMDR

Vulnerability management, detection & response services gives the organization a continuous, always on, assessment of the infrastructure cybersecurity vulnerabilities and compliance posture.

BEC

Business email compromise is a form of phishing attack where a criminal attempts to trick a senior executive into transferring funds or revealing sensitive information.

01

Introduction

■ Introduction



Established by stc, the region's top ICT and digital services provider, sirar by stc is a cutting-edge cybersecurity provider that empowers organizations to take control of their cyber and digital capabilities.

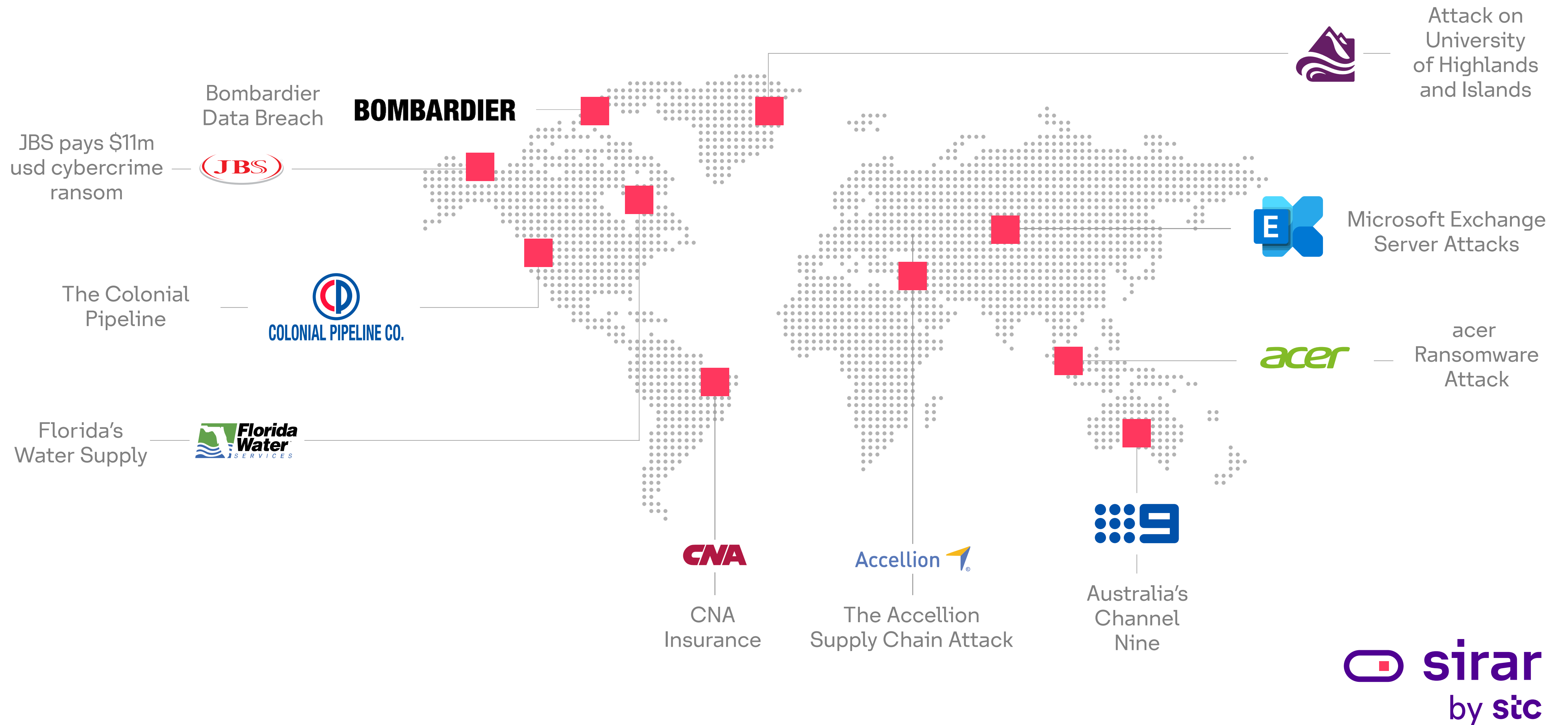
This report will illustrate the cyber threats in the year 2021 that were attacked globally, and locally, and they were prevented by sirar by stc.

The report will show threats statistics and trends, cyber security predictions, and sirar by stc solutions to prevent these threats. Also, sirar by stc suggestions to save organization from the threats and attacks.

02

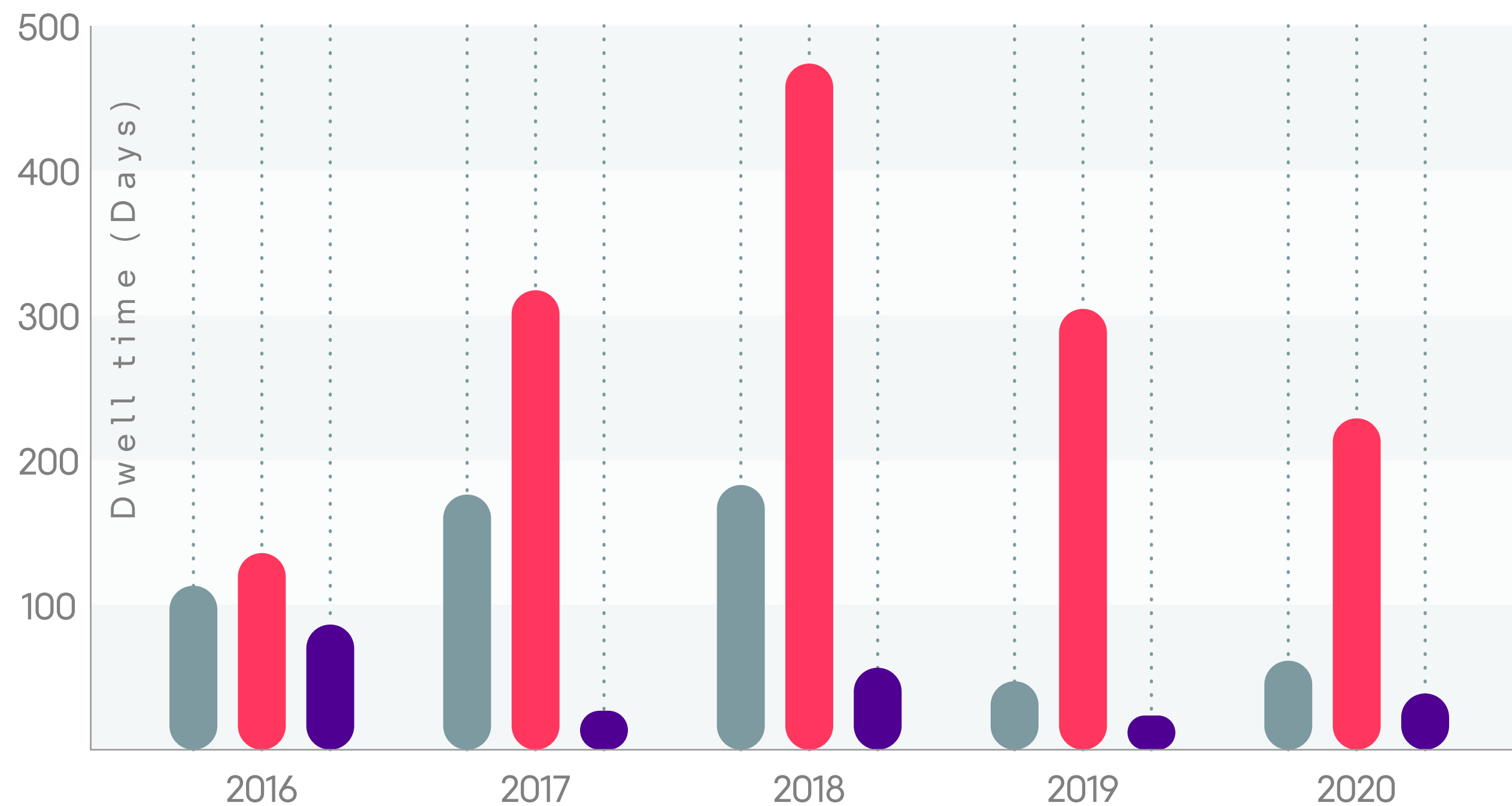
Global Attack Trends

10 Biggest Attacks in 2021



Global Threat Landscape

EMEA MEDIAN DWELL TIME, 2016-2020



Notifications

ALL External Internal

Source: Mandiant and Dell reports

11s
Every 11 secs there is
a successful cyber or
ransomware attack

60%
of companies have
experienced a data
breach

2021

Threat Landscape

Ransomware

- Acer was hit by a REvil ransomware attack demanding US\$50 million
- Washington DC Police Department hit by babuk, ransom US\$4 million
- CNA Financial Corp targeted by Phoenix CryptoLocker ransomware, US\$40 million to regain control of its data and system

Vulnerabilities Exploitation

- PrintNightmare (Affecting Windows printer services)
- Proxylogon (MS Exchange server)
- Apache Server RCE (CVE-2021- 42013)
- VMware RCE (CVE-2021-22005)
- RCE in all Windows OS versions (CVE-2021-40444)

Supply Chain Attack

- More SolarWinds breaches are heard of in this year
- Compromised NPM repository (UA Parser.js) for JavaScript libraries delivered by remote access trojans
- Acellion (File Transfer Appliance) product updates led to clop ransomware campaigns

Data Leakage

- Gigabyte suffered ransomware attacks with major breaches
- Facebook is fined US\$56 million by South Korea over data breach
- Twitch data breach leaked source code of entire platform

Ransomware

Global Attack Trends

Global

Spotlight Notable Ransomware Threat Actor



FIN12 Threat Actor

Attacks

Prolific ransomware attacks typically deploy the Ryuk ransomware variant and have been associated with Cobalt Strike, Beacon, Trikoot and Bazarloader actors

Attackers' Victim's Statistics

Almost 20% of ransomware intrusions, according to Mandiant, were attributed to FIN 12

Other targeted sectors include: business service, education, technology government, manufacturing, retail and finance

Techniques / Technology TRICKBOT

FIN12 exclusively leverage TRICKBOT accesses as a launching point for their ransomware attacks

Sponsor

Unknown

Motivation

Financial crime & gain

Targets

Regional targets: Europe/Asia Pacific/North America
Targeted industry: Healthcare

Russian based threat actor

Global Ransomware Technique Growth

Extortion 1989

PC Cyborg virus
asked for US\$189 as a ransom.

Monetization 2010

The Emergence Of Cryptocurrencies
10,000 ransomware samples, Birth of Bitcoin,
Screen-locking ransomware appears

Double Extortion 2019

Maze Ransomware
Demanded ransom.
Encrypted data and disclosure of the
breached data.

Quadruple Extortion 2021

Darkside Group
Demanded ransom.
Encrypted data and disclosure of the breached data. Started a
new trend by launching DoS attack together with ransomware.
Contacted customers informing them that the
organization had been hacked.

Triple Extortion 2020

REvilGroup
Demanded ransom.
Encrypted data and disclosure of the breached data.
Started a new trend by launching DoS attack together
with ransomware.

Source: Crowd strike, History of Ransomware, June 2021

Global Ransomware incidence



REvil

Ransomware Family

GandCrab is a ransomware as-a-service variant.

Attackers' Victim's Statistics

Reaches 18 million households with ADSL

Almost 26 million with optical fiber

MasMovil 4G mobile network covers 98.5% of the Spanish population and they were ALL at risk

Techniques / Technology

Ransomware gang claimed to have downloaded databases and other important data belonging to the MasMovil Group.

Source

Russia based

Apprehension & Arrest

A total of seven affiliates, behind the REvil, were arrested in different countries with a US\$6m seizure and a US\$10m reward.

Targets

MasMovil is a major telecom provider and has a very big imprint in Spain.

Affiliate has been arrested.

Global Ransomware technique to MITRE

Mapping the top 4 attacks in 2021 with MITRE ATT&CK Framework

Impact Darkside Conti Avaddon Sodinokibi

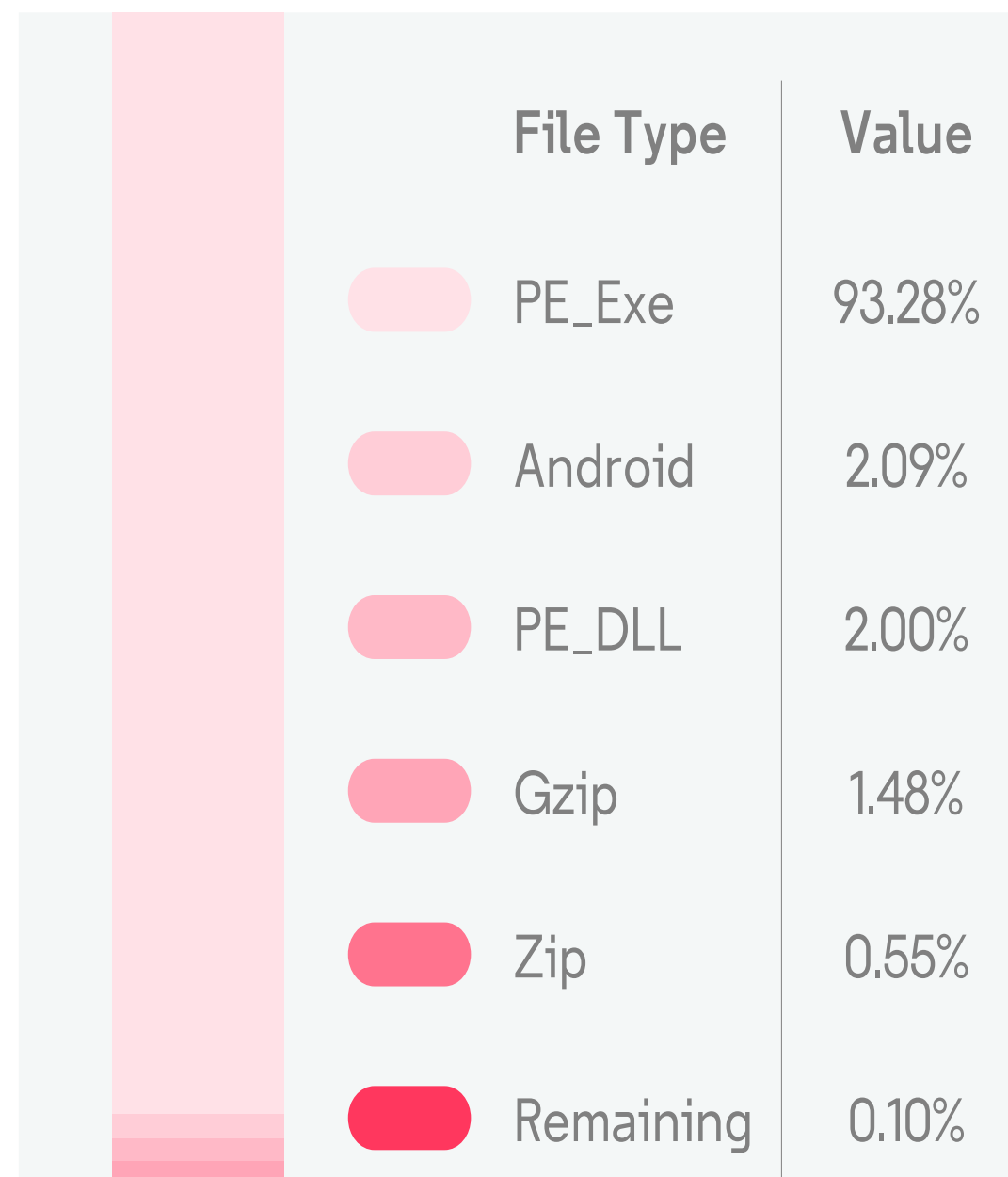


Techniques All used techniques listed under each tactics.

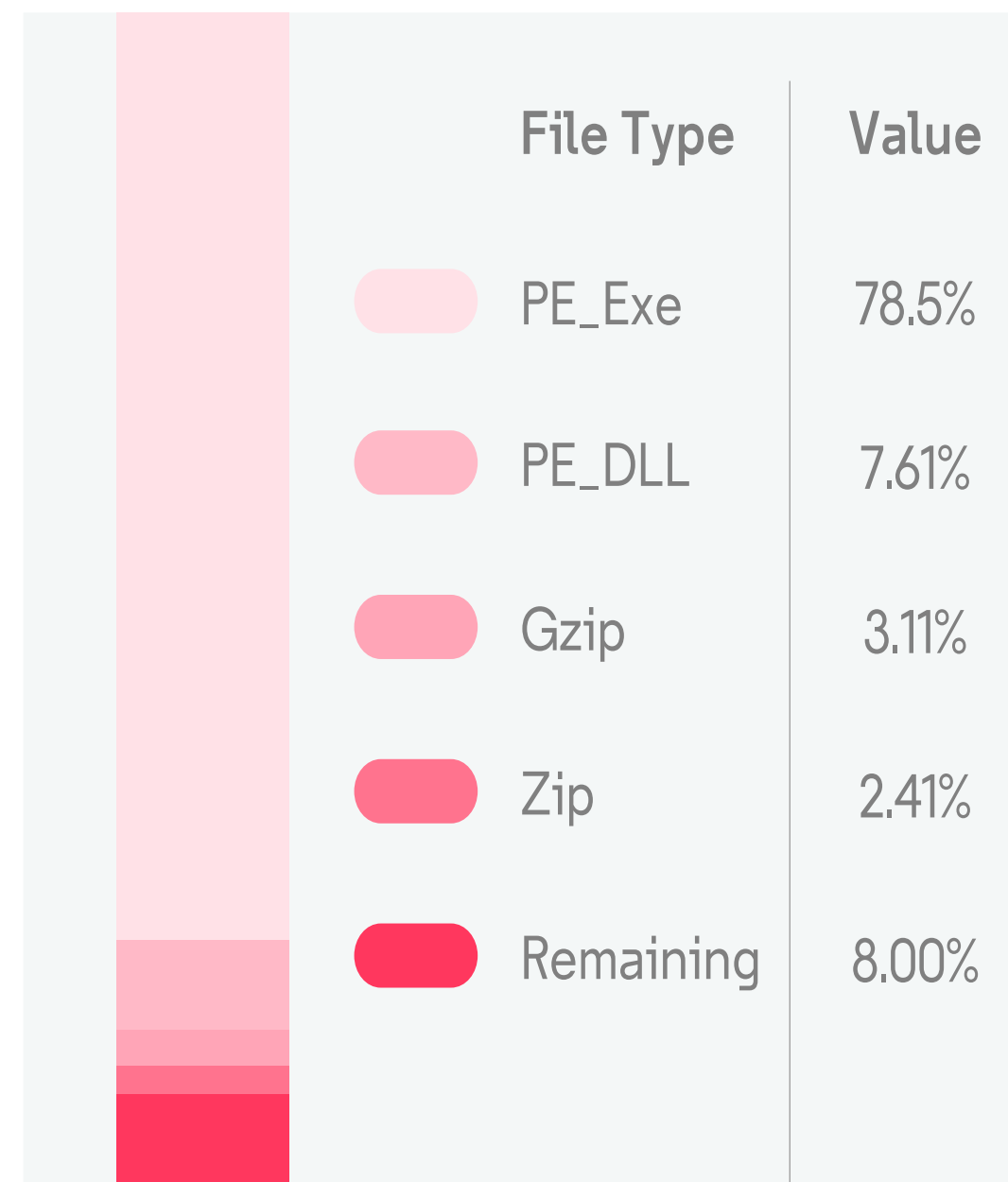
Confidential

Global Ransomware Statics

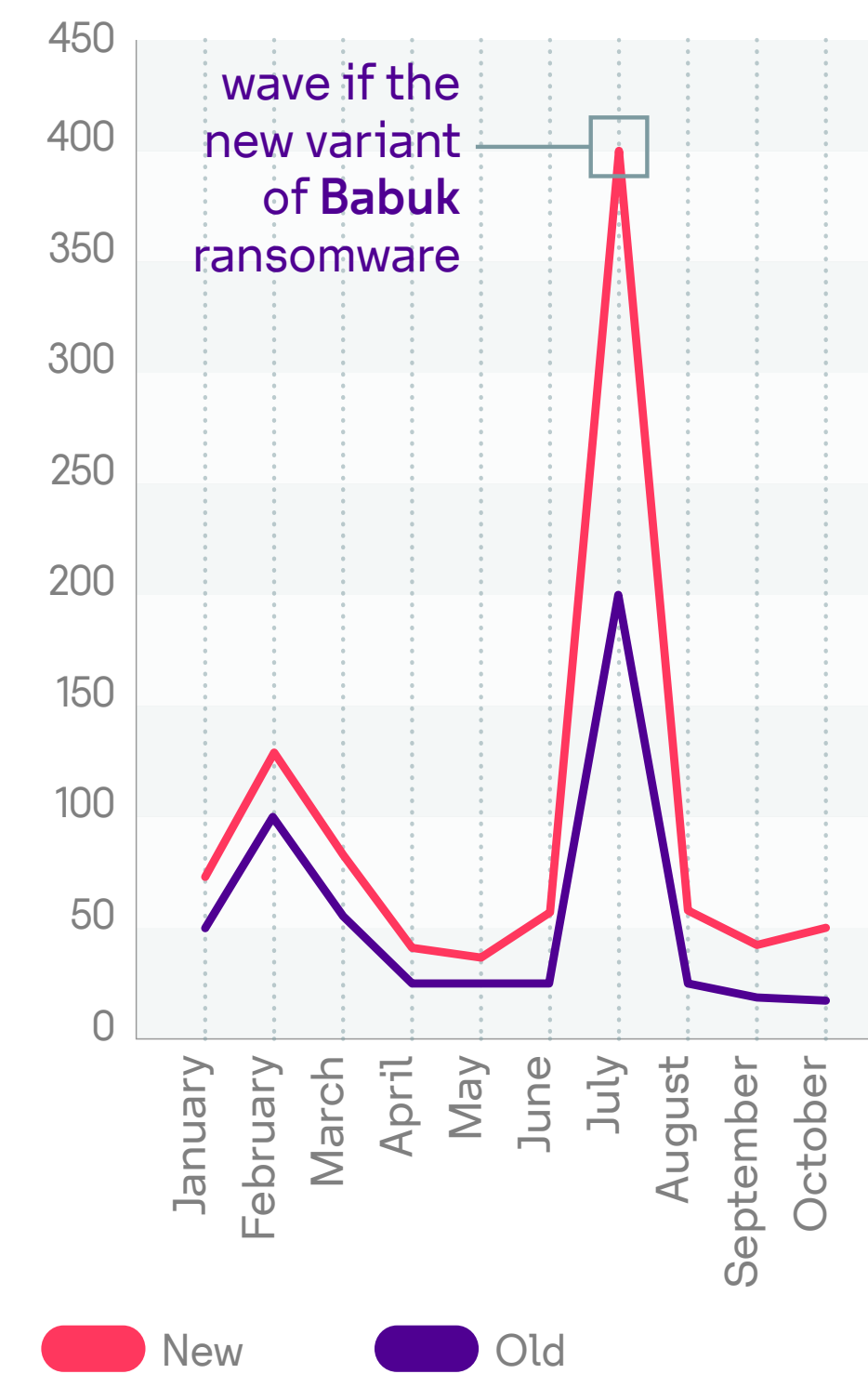
Types of Ransomware File Types



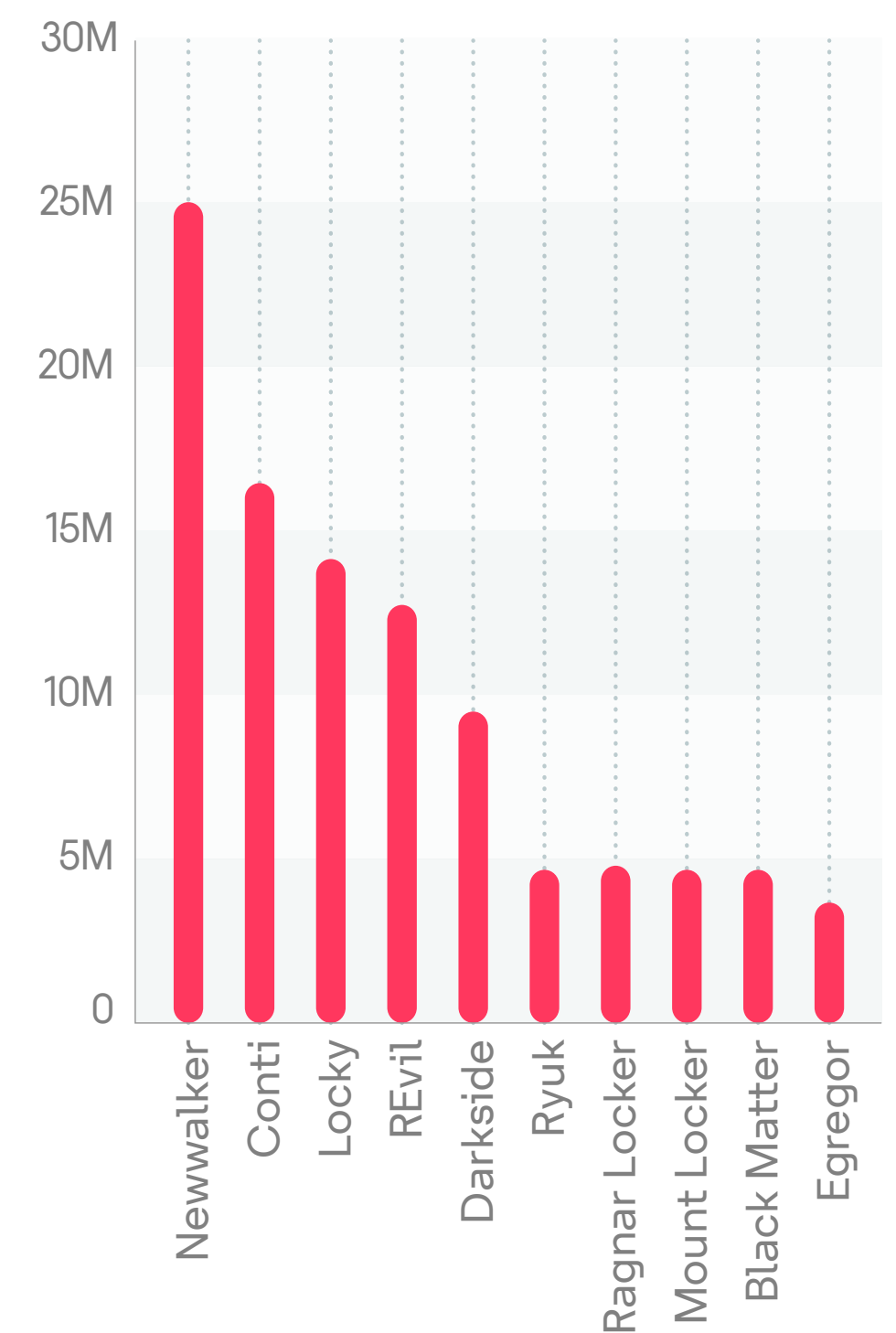
The Most Active Ransomware Families



Ransomware Sample Submitted to Virus Total in 2021



Total Payments in US\$- 2021



Supply Chain Attack

Global Attack Trends

Global

Spotlight Notable Supply-Chain Threat Actor



Fancy Bear Threat Actor *

Supply-Chain Attacks

Nobelium is part of a Russian group who were behind the SolarWinds attack in 2020.

Attackers' Victim's Statistics

140 organizations targeted in a new round of supply chain attacks

Microsoft identify 23,000 attempted attacks between July and October.

609 attempts against Microsoft's clients, with a low success rate

Techniques / Technology

A sophisticated malware to remotely exfiltrate the database configuration of compromised Active Directory Federation Services servers.

Sponsor

State-sponsored.

Motivation

Information theft

Espionage.

Targets

Targets observed: United States / Europe

Russian based threat actor

Global Supply-Chain Attacks

50%

of the attacks are attributed to well known threat actor groups including APT's.

62%

of the attacks used malware as the attack technique deployed.

42%

of threat actors behind these campaigns have not been attributed to any known threat actor group.

66%

of the attackers focused on the supplier's code for further compromise of the targeted customers.

62%

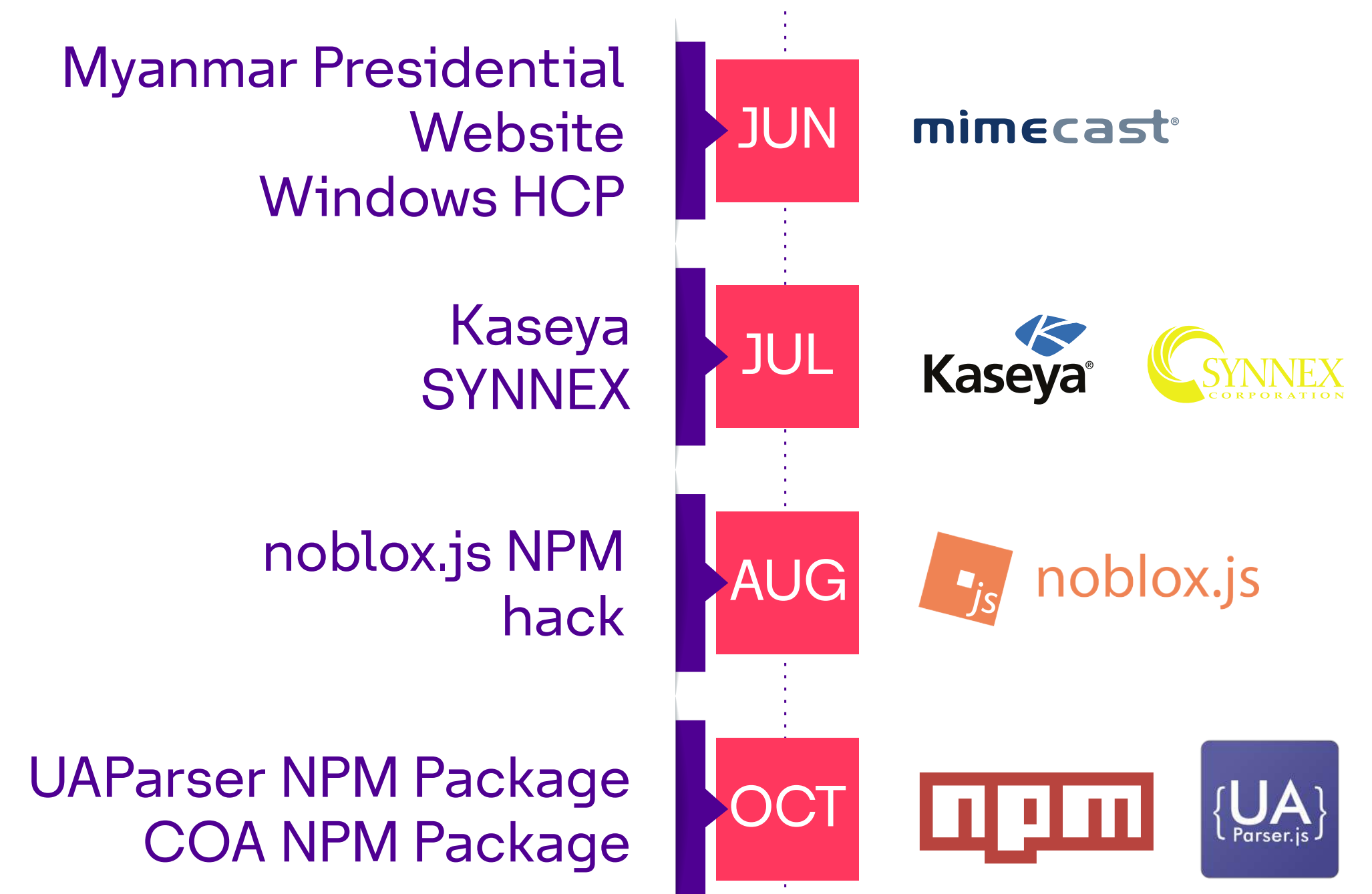
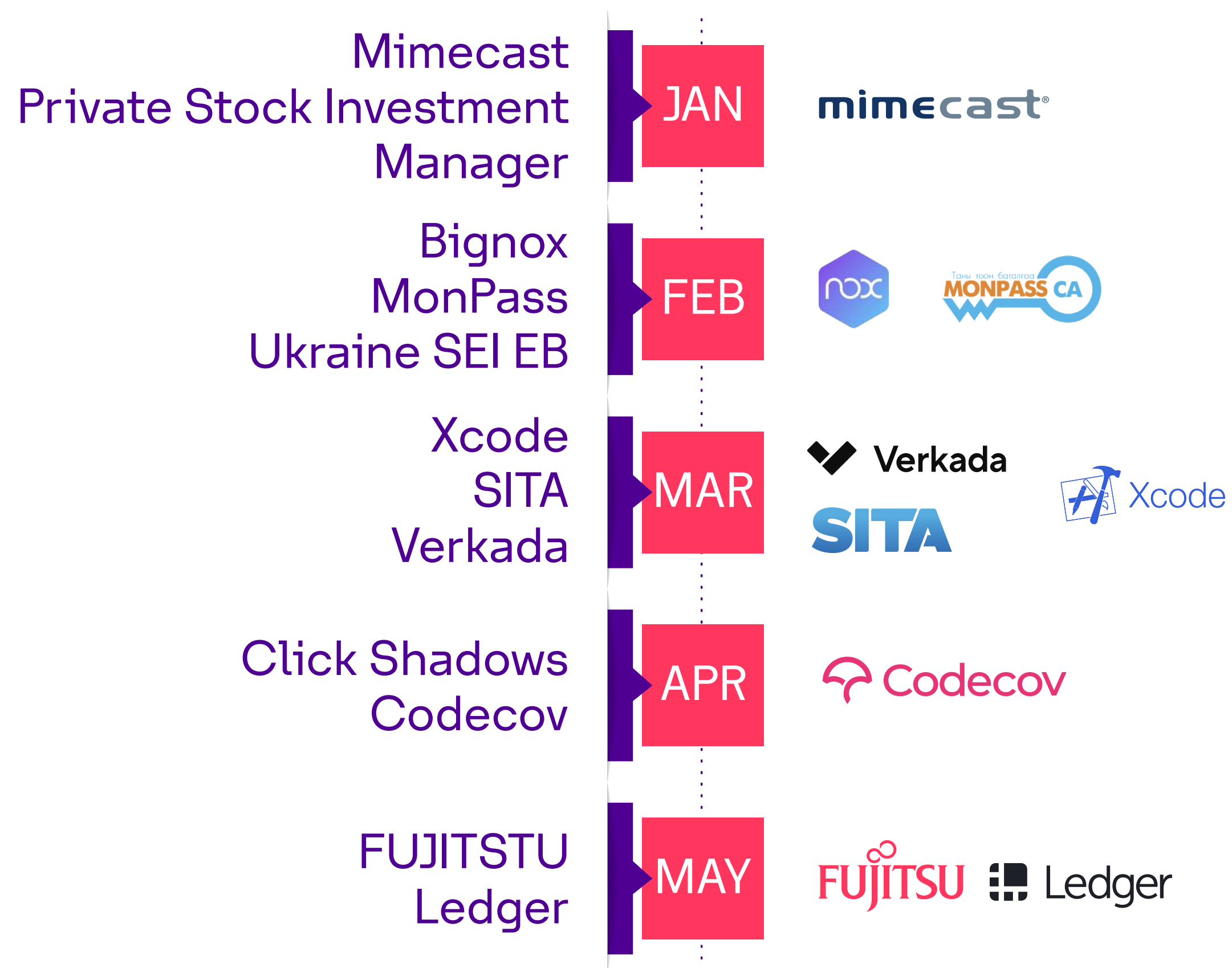
of these attacks misused customer's trust in their supplier.

58%

of all the attacks were supply chain attacks, aimed at gaining access to the customer data.

Global

Supply - Chain Attacks



Global Supply-Chain Attack

SITA

The Most Affected Airlines by SITA Supply-Chain Attack

AIR NEW ZEALAND 

CATHAY PACIFIC 

UNITED
AIRLINES 

malaysia 
airlines

SINGAPORE
AIRLINES 

 Lufthansa

American Airlines 

FINNAIR

 JAPAN AIRLINES



The attack has been traced to
Chinese State Actor APT41

90%

of the world's airline
industry were at risk.

580,000

membership information
of Club loyalty were
compromised.

\$ 3,000

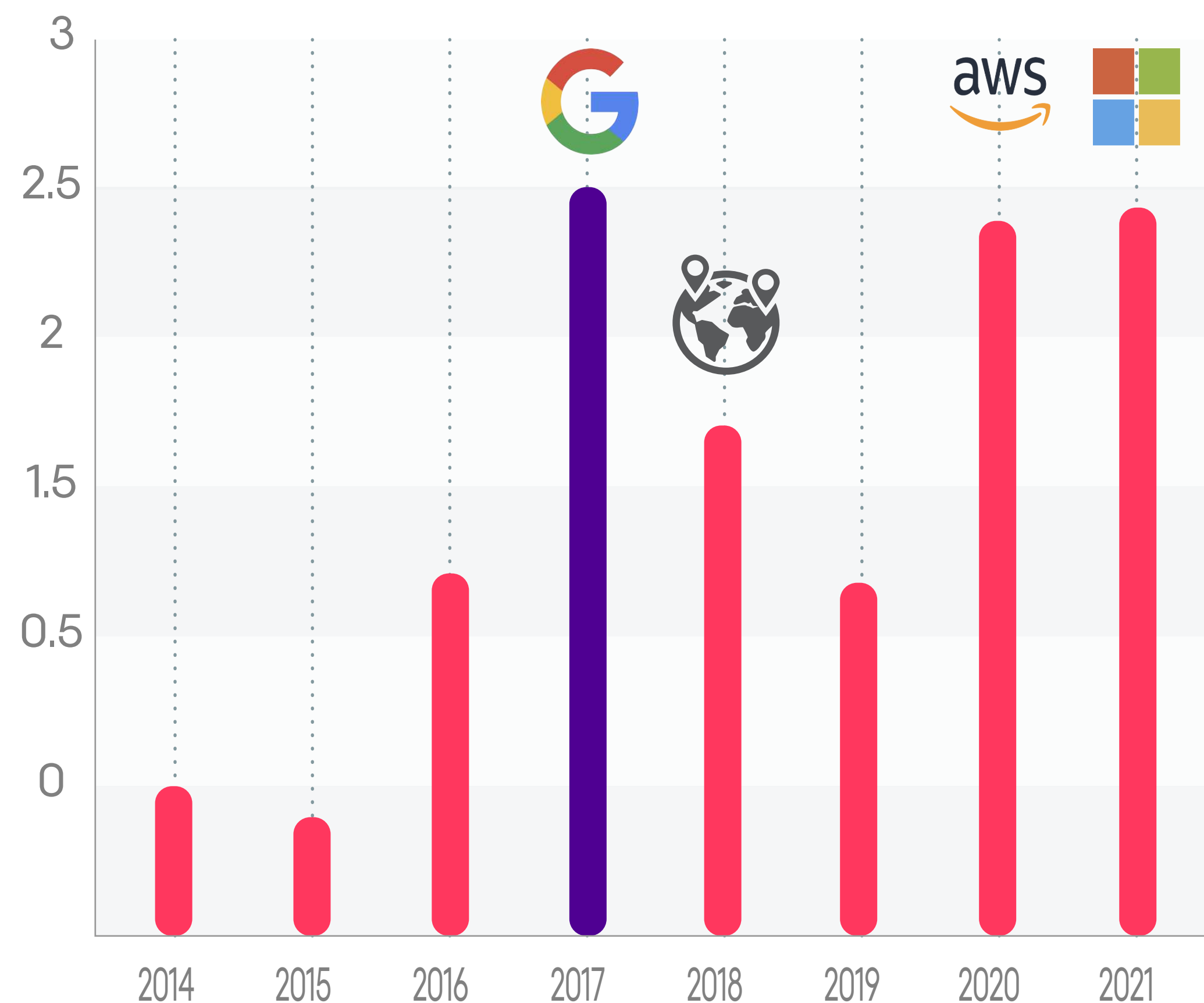
is the price of
breached database on
leak site.





400+

potential airlines were
affected by the breach.

Global Supply-Chain Attack

Largest DDoS attacks over years (in Tbps)



-  DDoS the top attacks in history In 2021 , Microsoft suffered a 2.4Tbps UDP reflection DDoS attack . Which ranged for 10 minutes and fluctuated from 0.55 Tbps to 2.4 Tbps.
-  G Google has announced recently that they had intercepted an attack of size 2.5Tbps in 2017
-  aws suffered a 2.3Tbps attack hit and broke the record.
-  the global record for the largest DDoS attacks was known to be 1.7Tbps, which happened in 2018.

Global Log4shell Threat Landscape

Facts

90%

of fortune 500 uses
java

1m

attacks attempted
after 72 hours

30%

of infected instances
remain vulnerable

2.8k

web application
infected

Exposure

3m

vulnerable instances
detected

22m

vulnerable
applications flagged

150m

assets scanned
globally

Trends

80%

linux vulnerable
assets

22k

weekly potential
attack

17 days

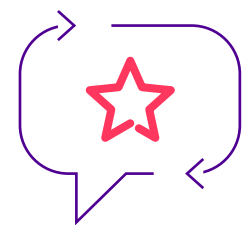
average remediation
after detection

Source : Qualys

IoT

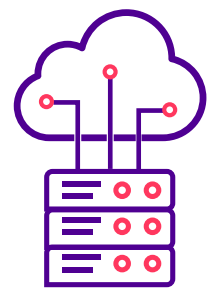
Concerns & Stats

Concerns

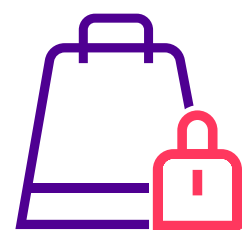


**Lack of
patches and
updates**

**Insecure
interfaces**



**Insufficient data
protection**



**Weak
protection**

Stats

639

Million increase

872

Million leveraged
telnet

1.51

Billion breach



>_SSH Access to IoT networks via the telnet protocol

Vulnerabilities Exploitation

Global Attack Trends

Global

Spotlight Threat Actor Targeting Saudi Arabia



Charming Kitten

Popular Campaigns

In 2018, they built a website meant to mimic a legitimate cybersecurity company. The only difference was that the fake website had a slightly altered domain name. This helped them to get the login details of some of the company's clients.

Attackers' Victim's Statistics

They made 2,700 attempts to gain information regarding targeted email accounts resulting in 241 attacks and 4 compromised accounts.

Leaked over 1TB of data, which consisted of staff personal details and shows, which were yet to be aired officially.

Techniques / Technology

Charming Kitten was thought to be using a fake profile on Social media as a part of phishing campaigns targeting high risk users.

Sponsor

sponsored..

Targets

The usual targets in Saudi Arabia, UAE, Israel, and the rest of the Middle East region.

Targeted: Government, Defense Technology, Military, Healthcare and Diplomacy sectors

Motivation

Information theft.

Espionage

Iranian based threat actor

Global

Spotlight Threat Actor Targeting Telecommunications



Aquatic Panda

Motivation & Sponsor

China - based targeted intrusion adversary with a dual mission of intelligence collection and industrial espionage. Aquatic Panda are State - sponsored.

Sponsor

State-sponsored.

Attackers' Victim's Statistics

Their malware Ghost RAT targeted more than 1,000 computers in 103 countries

They were part of Bignox supply - chain attack .

Motivation

Information theft | Espionage.

Techniques / Technology

Relies heavily on Cobalt Strike, and its toolset includes the unique Cobalt Strike downloader tracked as FishMaste. it Also has been observed delivering njRAT payloads to targets.

Targets

Primarily focused on entities in the telecommunications , technology and government sectors across Asai.

China based threat actor

Data Leakage

Global Attack Trends

Global Cybersecurity Statistics

171% increase in the average ransom payment

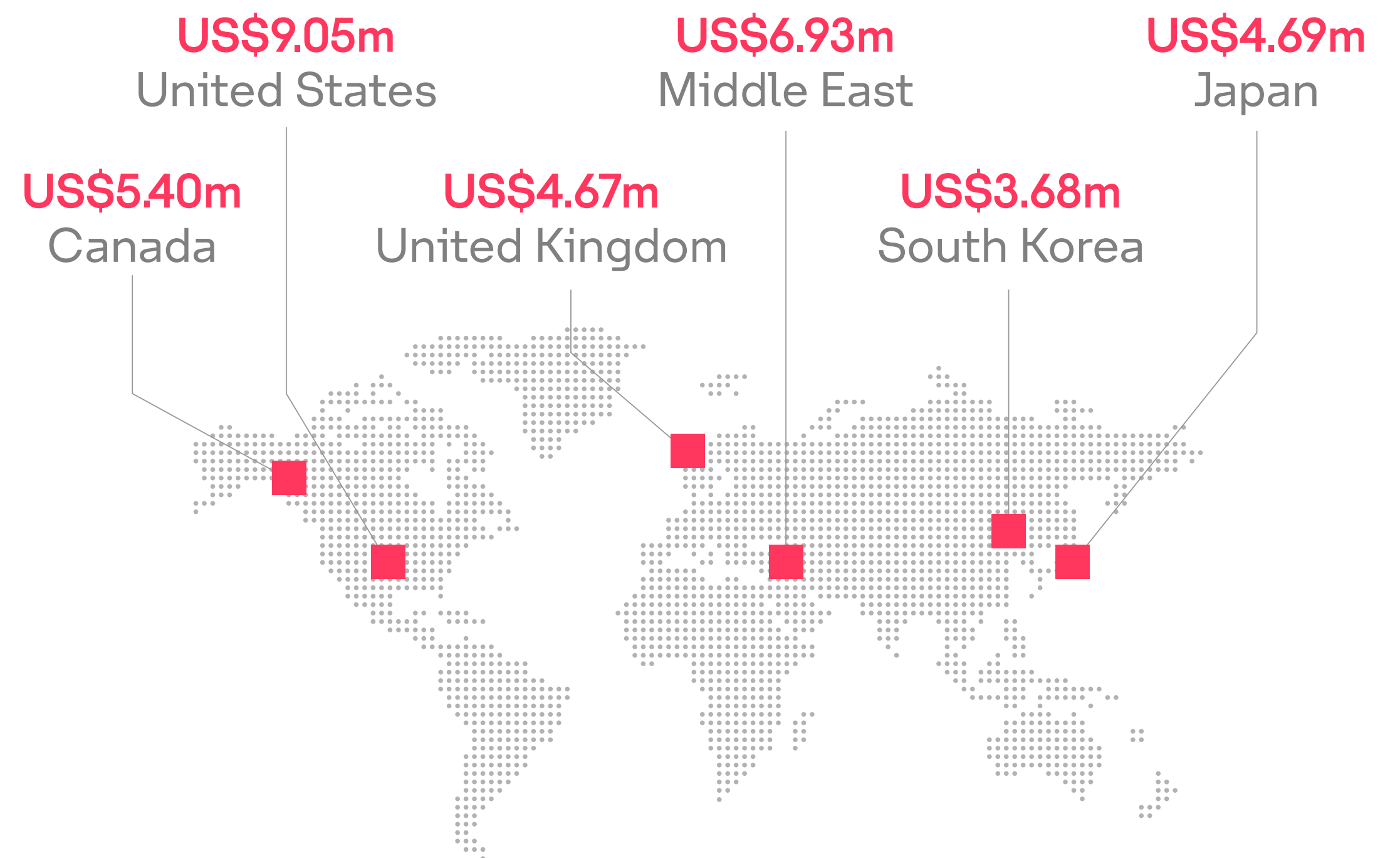
36% increase in weekly average of attacks per organization in the EMEA

20% of data breaches rely on compromised credentials

\$6T the expected peak in global average cost of cybercrime by end of 2021

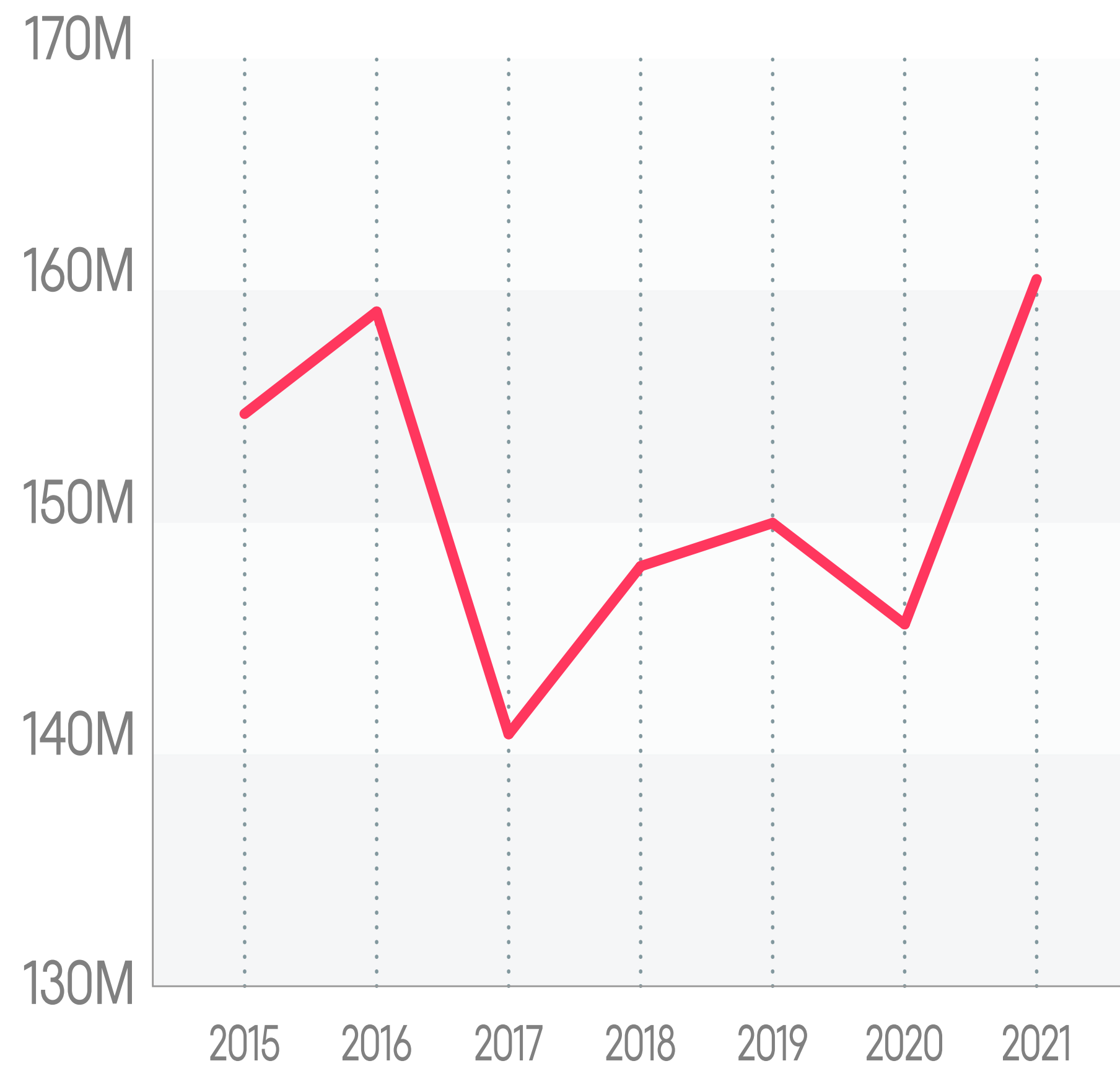
80% decrease in Data Breach Costs when implementing Security AI and Automation Controls

Average Data Breach Cost By Region (2021)

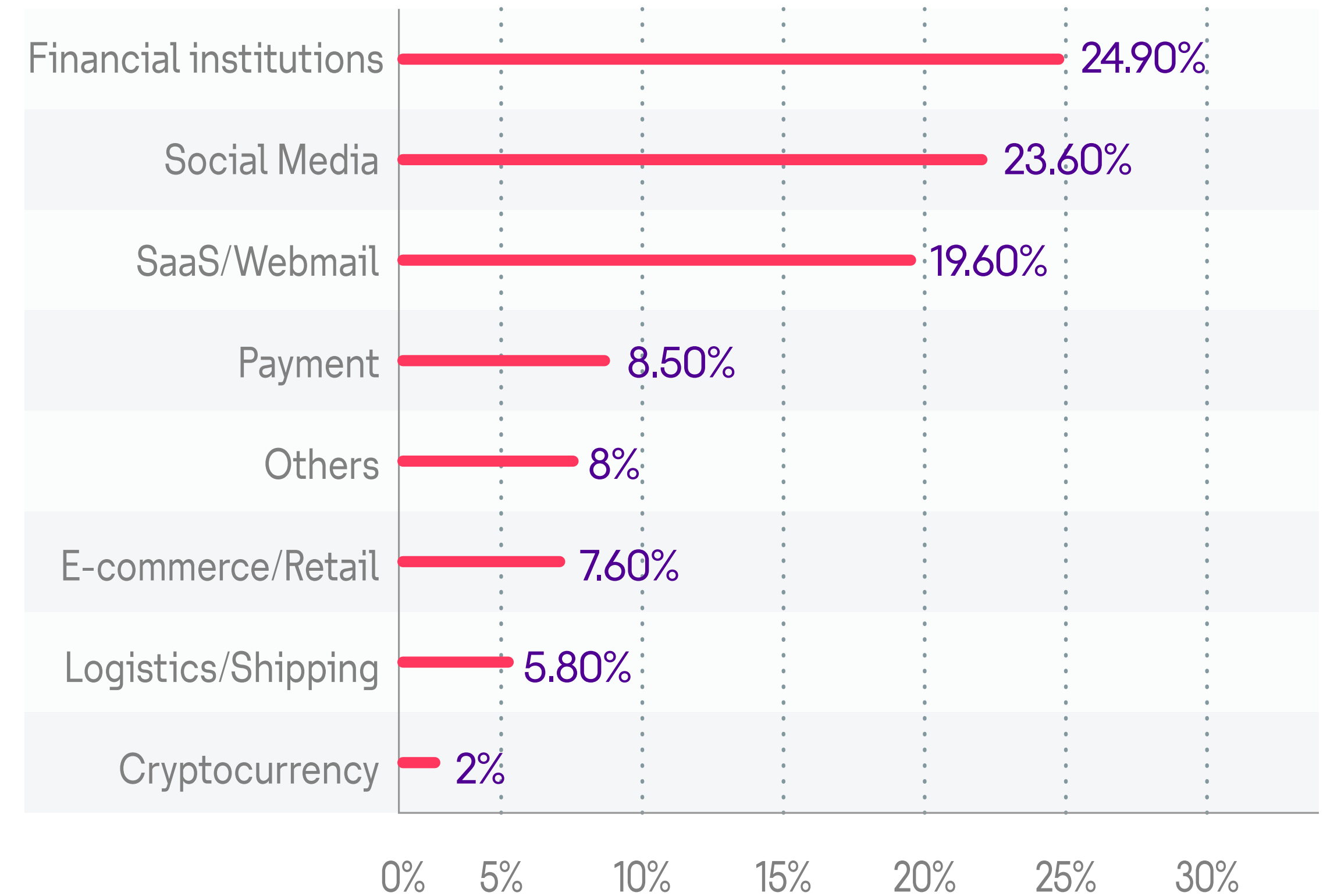


Global Cybersecurity Statistics

Average Total Cost of a Data Breach in Millions (2015-2021)



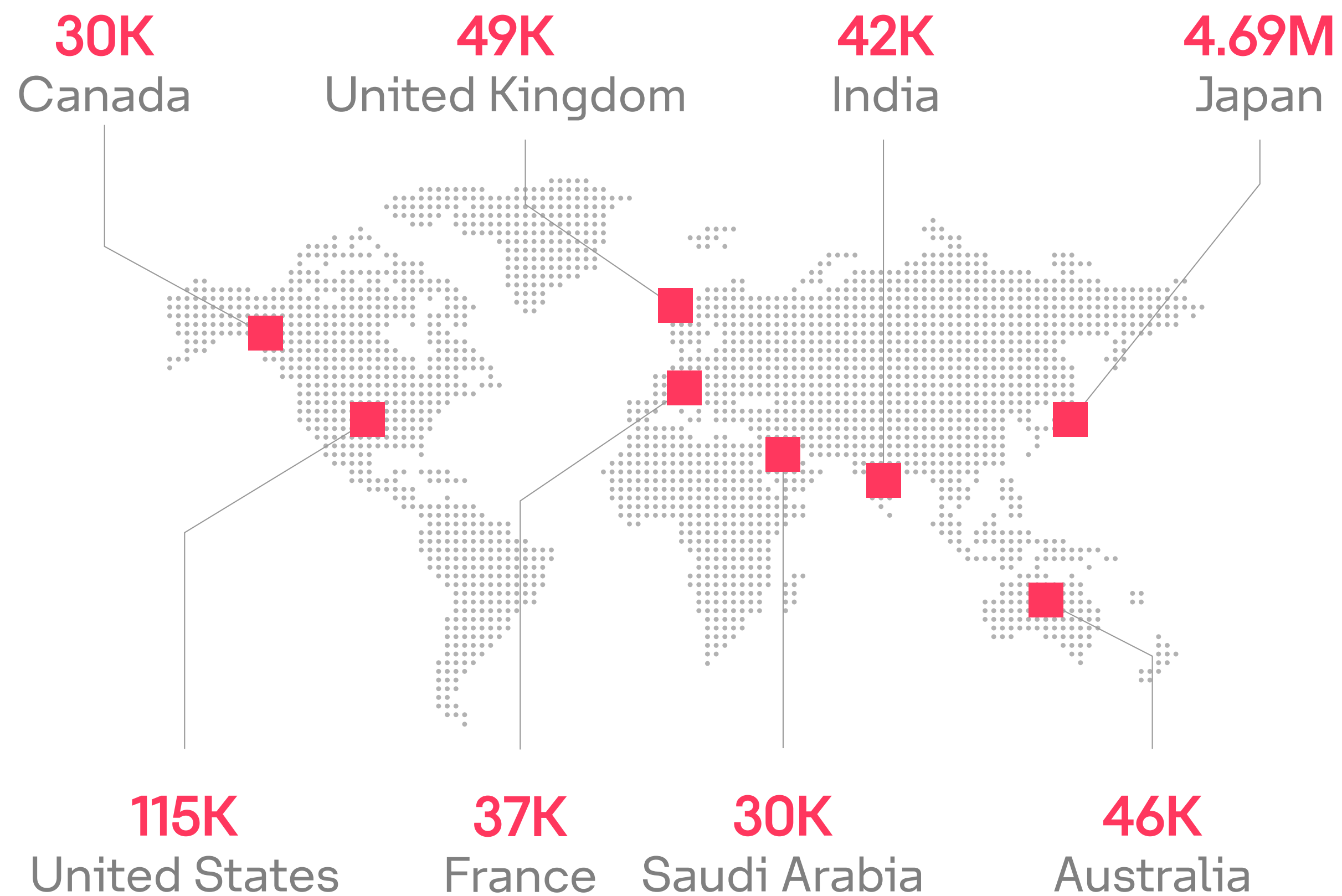
Industries Targeted by Phishing Attacks



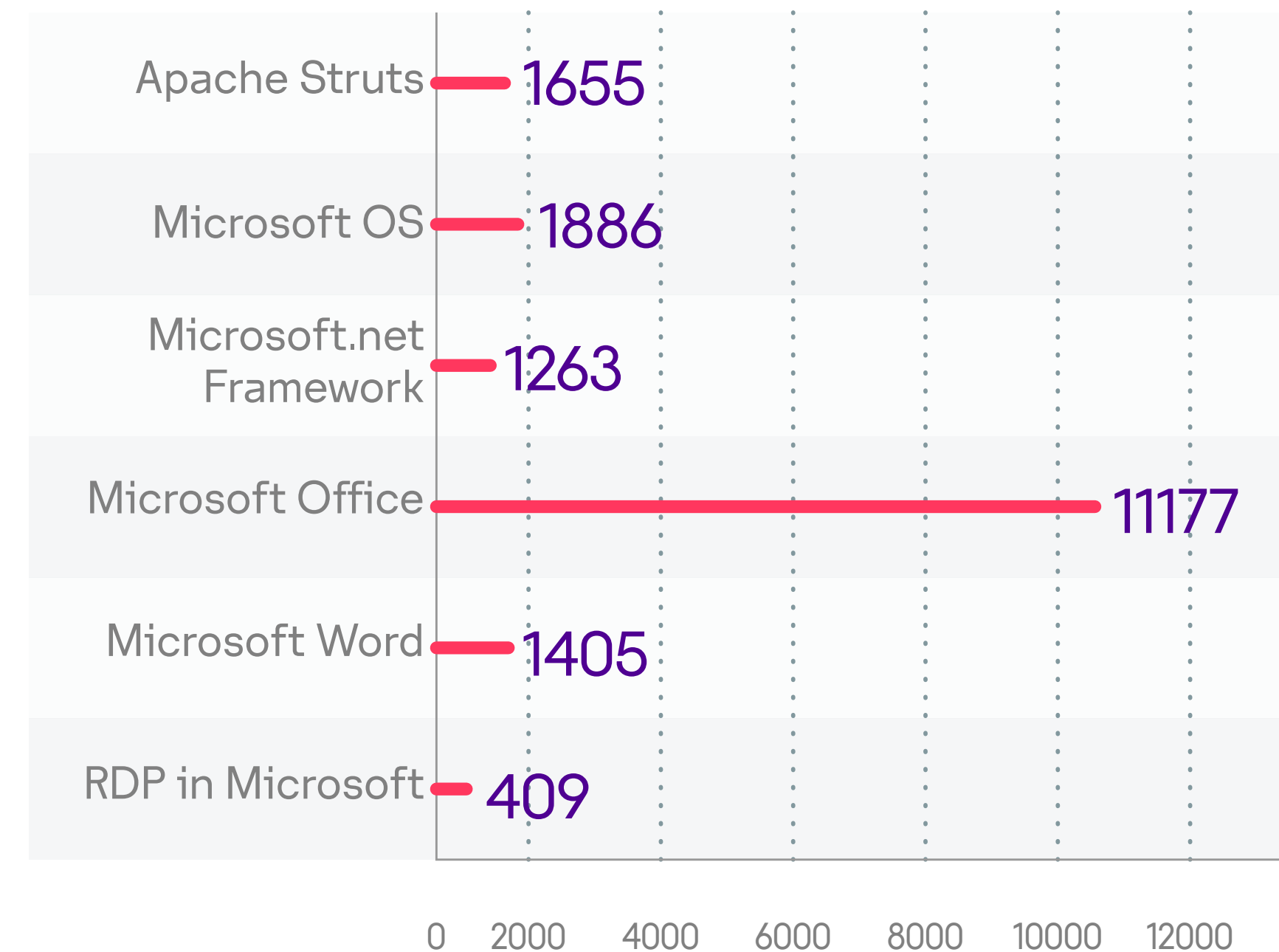
Global Cybersecurity statistics

Global Cybersecurity Statistics

Top Targeted Countries by Threat Actors

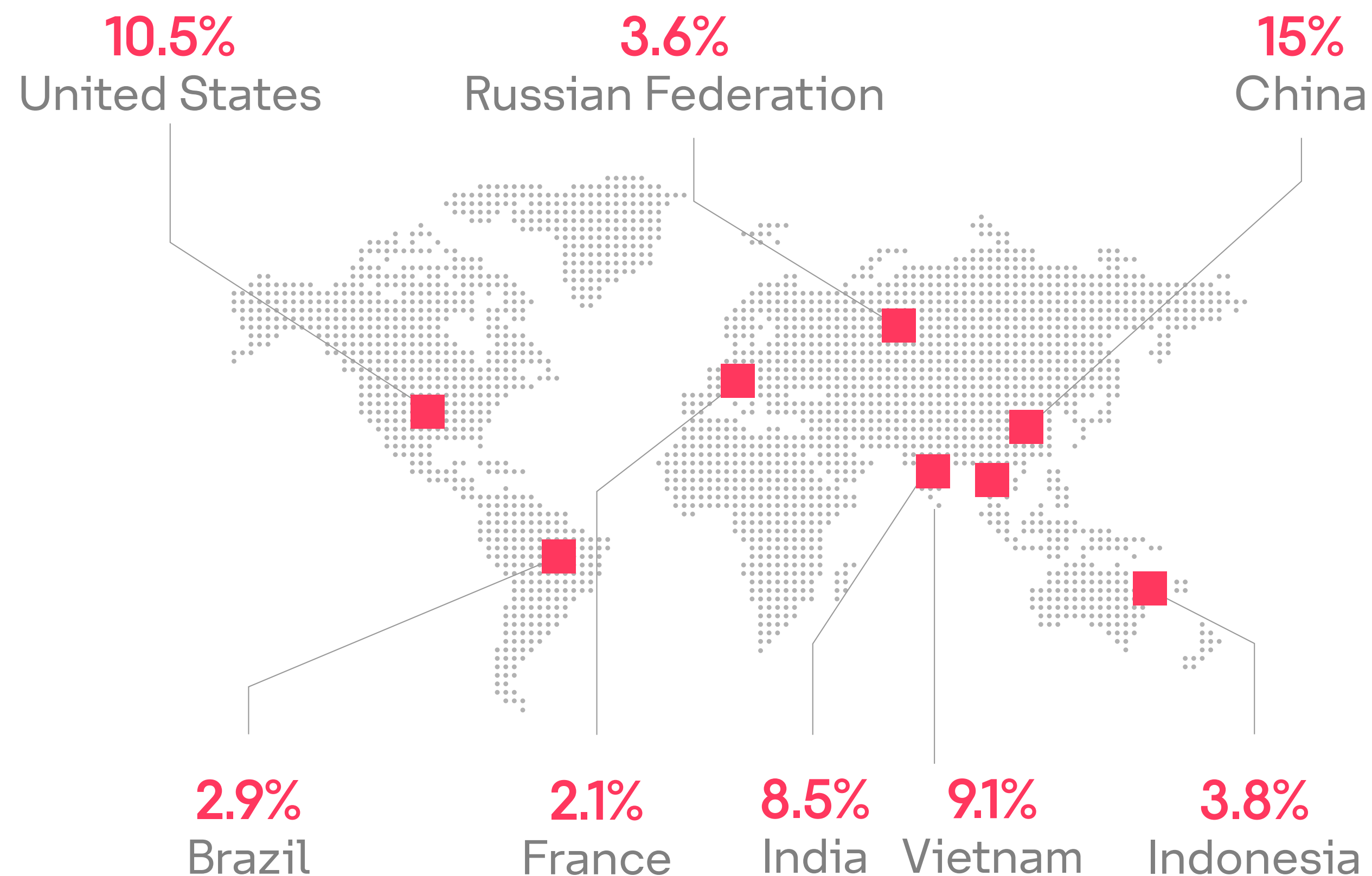


Top Target Products By Attacks

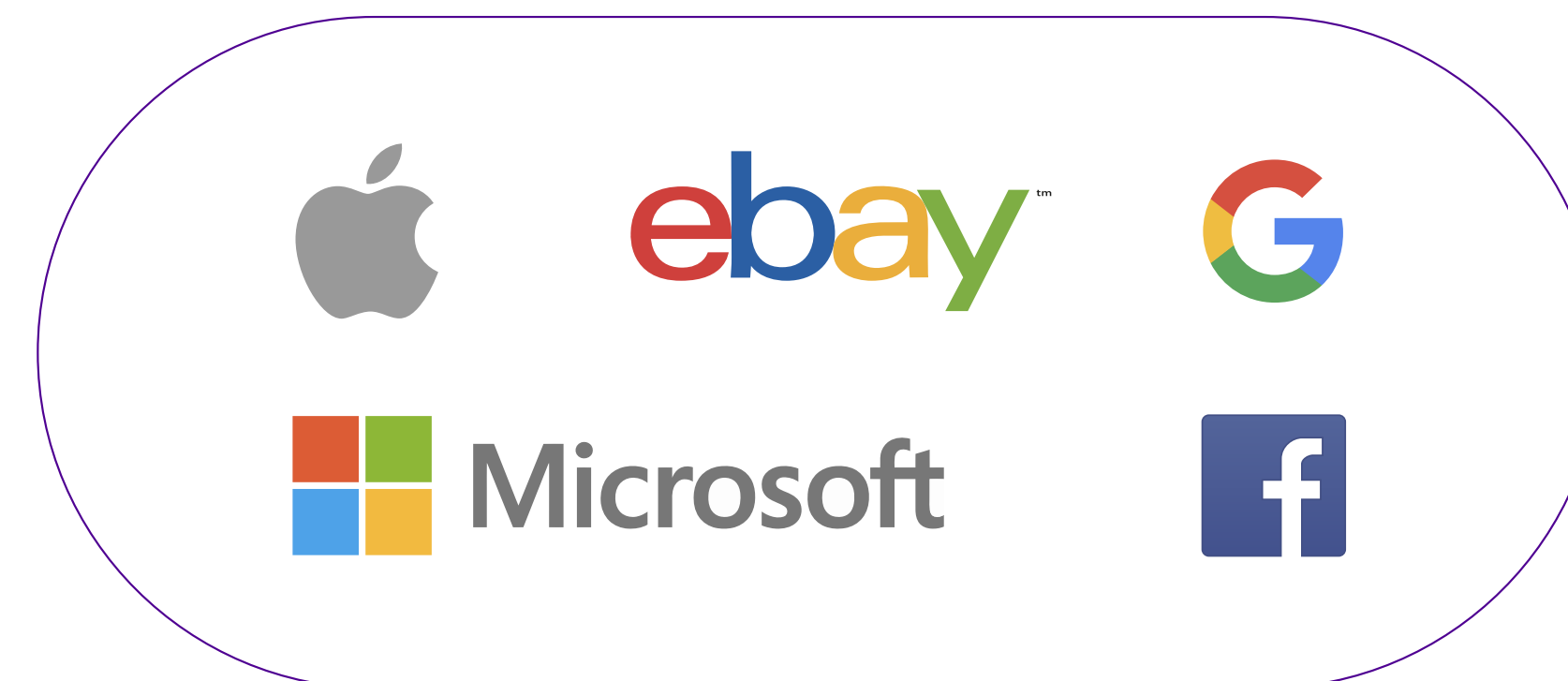


Global Cybersecurity Statistics

Countries Accounted for Half of the Top Malicious IP



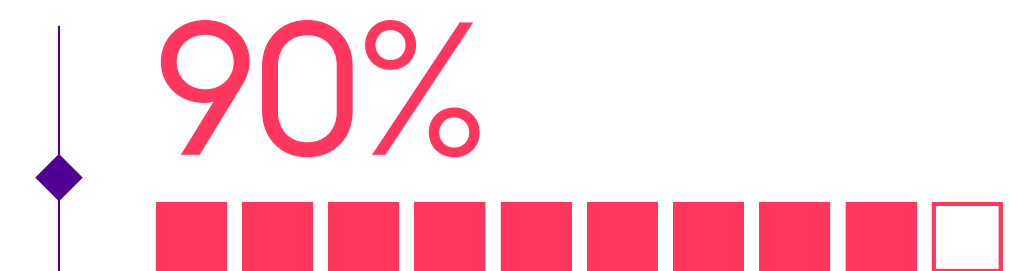
Top 5 Impersonated Brands



Global Cybersecurity Predictions

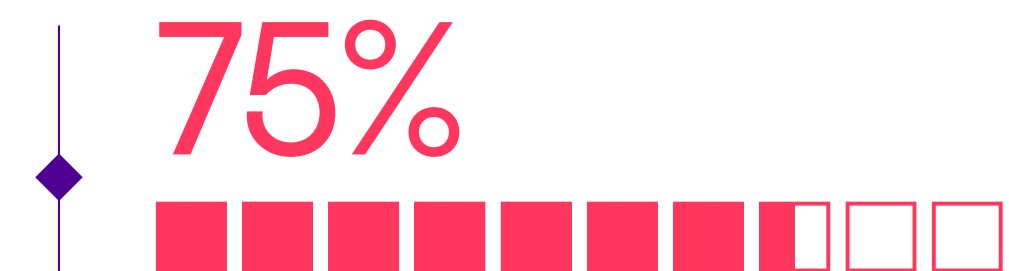
Reduce Financial Impact

By 2024, Matured Cyber Architecture will reduce financial impact by 90%.



Enhance Privacy Laws

By 2023, Global Privacy laws will be enhanced to cover 75% of PII for Global Individuals.



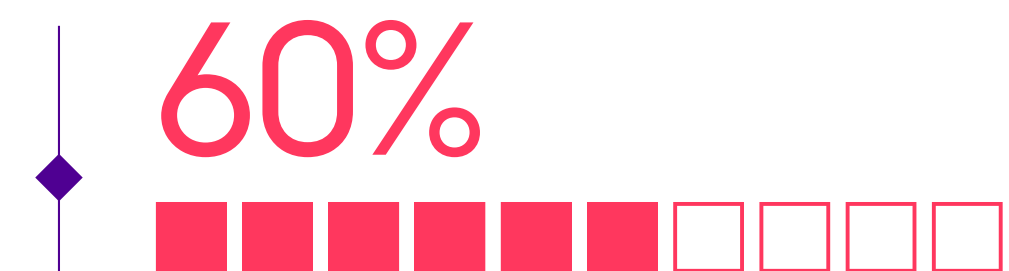
Operational Resilience

By 2025, 70% of organization's Resilience will be made mandatory to include Cyber Security.



Cyber Risk

By 2025, Cyber risk share in the overall Enterprise risk will increase to 60%.



Cloud IT Security

By 2024, 30% of global companies will adopt Cloud IT security.



03

KSA Statistics

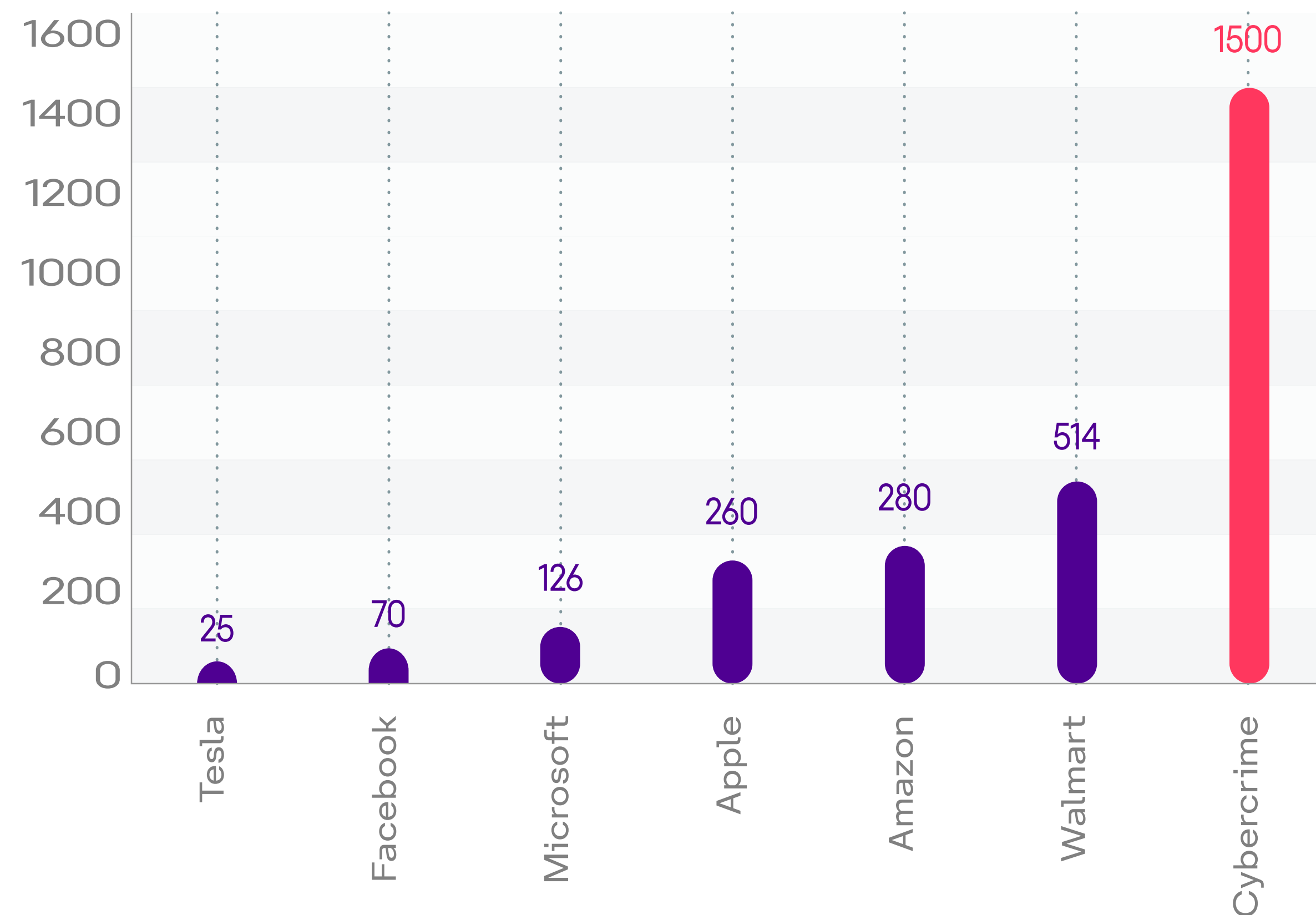
Threats in KSA

Saudi Attack Trends

Threat

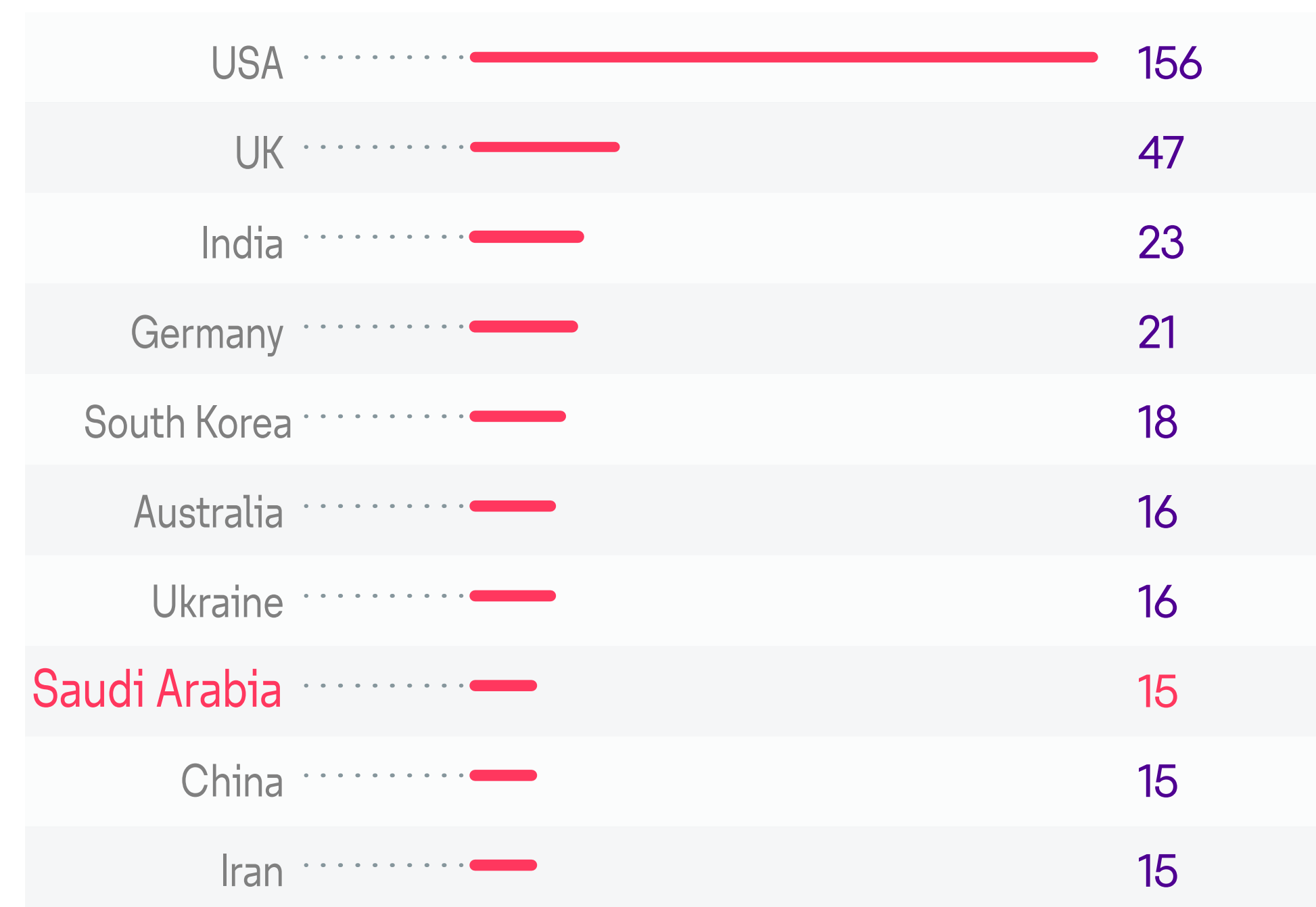
Landscape in Saudi

Cybercrime Revenue (Billions USD) | 2019



Source : Center for Strategic & International Studies (CSIS)

Top 10 Countries with Significant Attacks | 2006-2020



6th Botnets C & C

KSA Statistics And
Achievements

Saudi Attack Trends

KSA

Cybersecurity Statistics

13-38

is the average age of cyber criminal's victims in Saudi Arabia.

22.5m

brute force attacks targeted on remote desktop protocols (rdp) per year in Saudi Arabia.

95%

of saudi businesses have experienced at least one cyberattack.

3.5m

the average number of cyberattacks targeting Saudi Arabia per month.

KSA

Cybersecurity Incidents



أرامكو
aramco

\$ 50M 1 TB

is the ransom requested by attacker to delete the Aramco data placed on the darknet .

of Saudi Arabian Oil Co. data had been held by an extortionist , citing a web page it had accessed on the darknet .



غلوب ميد
GlobeMed

201 GB

of patient records were obtained and published during cyberattack targeting Saudi GlobeMed

KSA

Cybersecurity Achievements

Saudi Arabia has been ranked in cybersecurity as

1st among the Arab world countries, Middle East and Asia.

2nd among 193 countries around the world cybersecurity field.

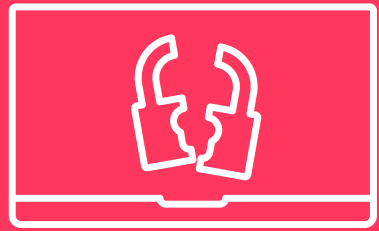
40 increased by 40 ranks since the Saudi Vision 2030 launch.

Breaches on the Dark web

Saudi Attack Trends

KSA

Saudi Breaches on the Dark Web



5

Underground forums selling or sharing the leaked data.



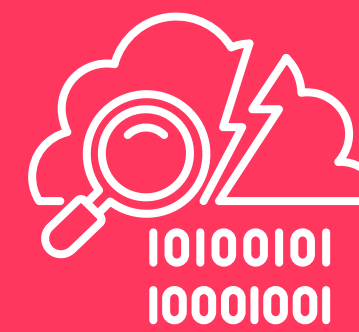
111

Corporation infected by the breaches.



256

The number of Actors behind the breaches.



1057

Total number of breaches on the dark web.

04



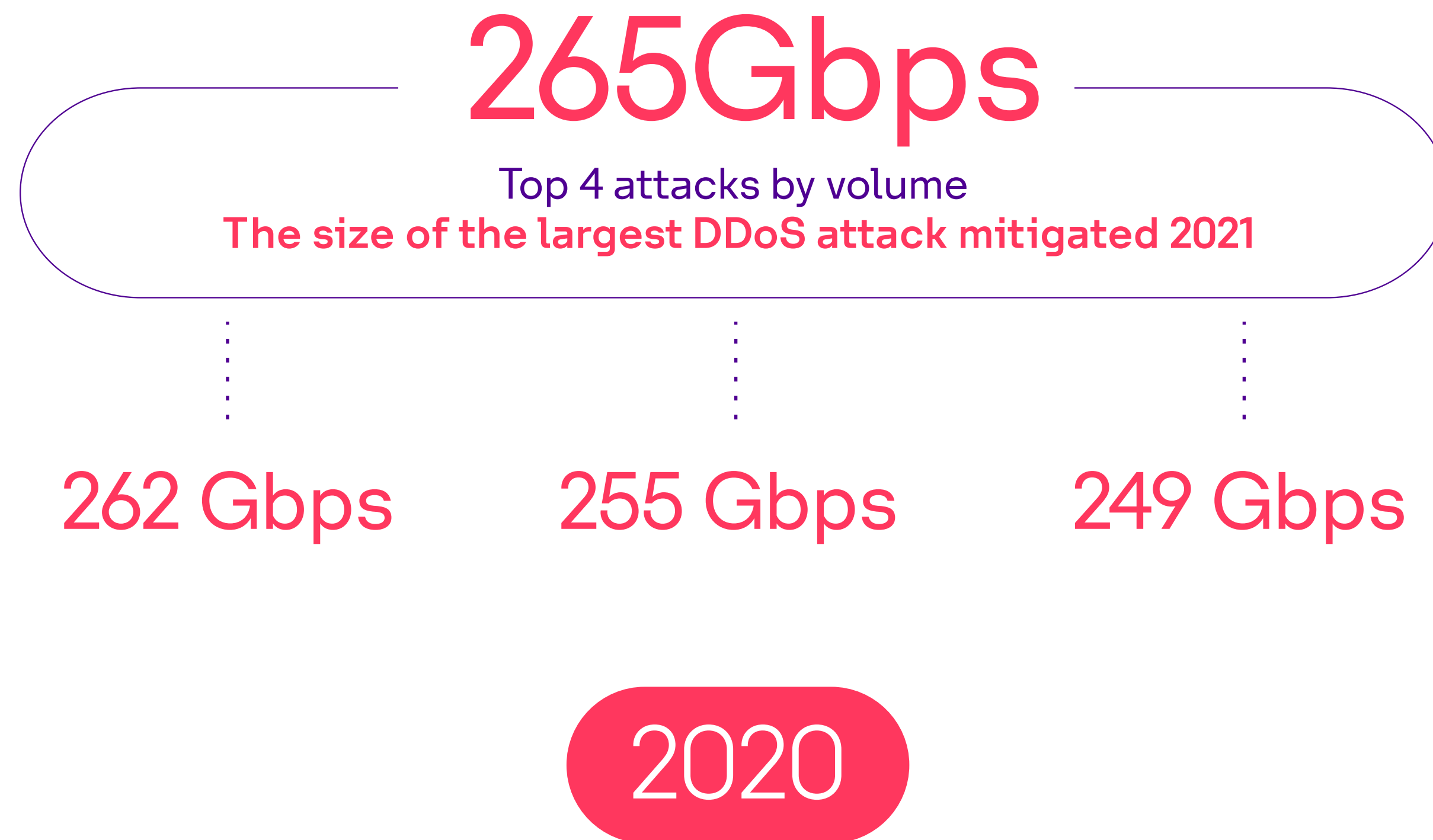
sirar Battles

DDoS

sirar Battles

Top DDoS

Attacks in stc at 2021



The largest DDoS in 2020: **166Gbps**
The increase on attack size **62.64 %**

Total Prevented Downtimes

7,366 Hours

The period of time a DDoS attack could have taken services / network / applications down if not mitigated properly .

4 TB

The local scrubbing can mitigate up to 8tps on cloud level

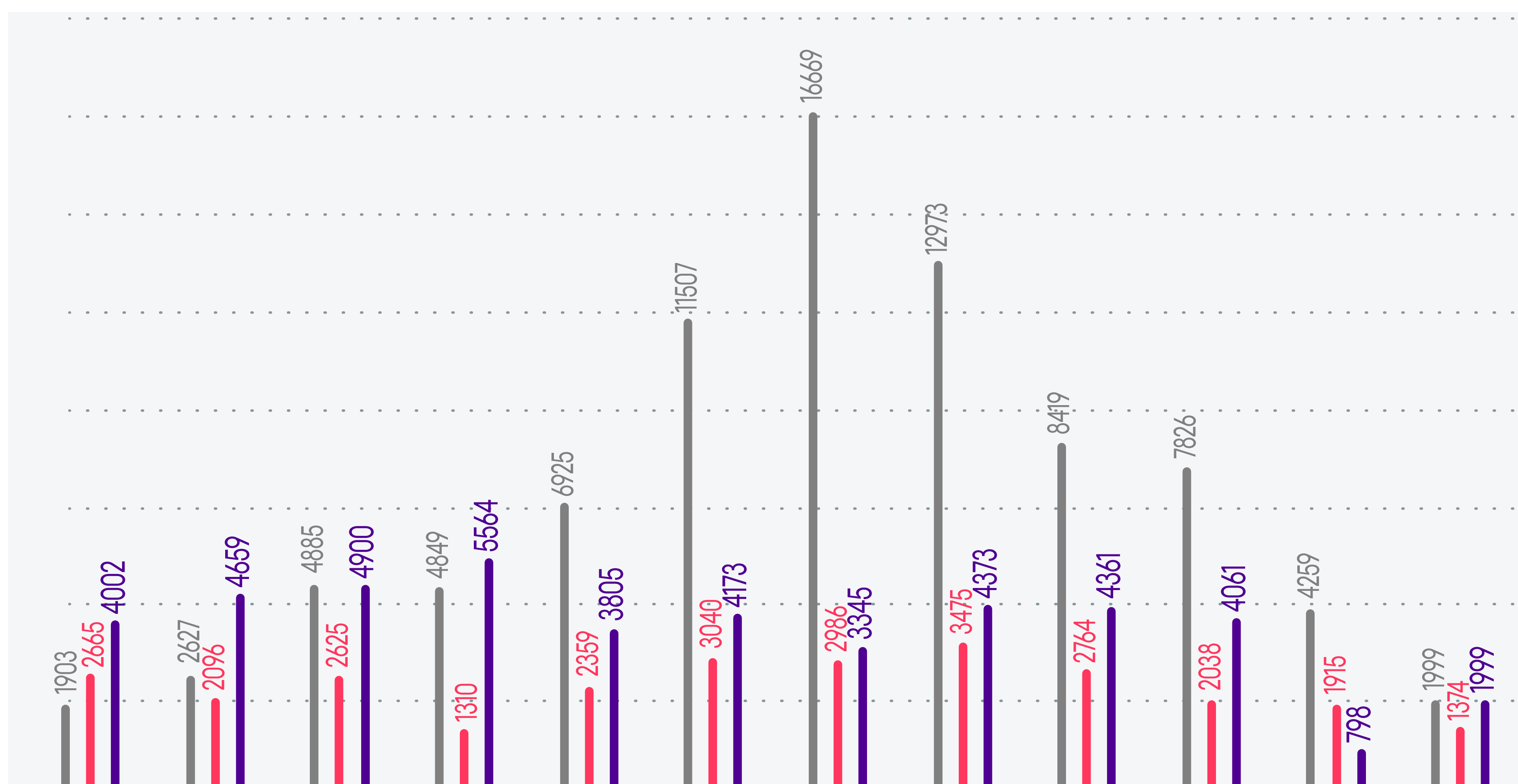
Top DDoS

Attacks in stc at 2021

DDoS attacks
in 2019

DDoS attacks
in 2020

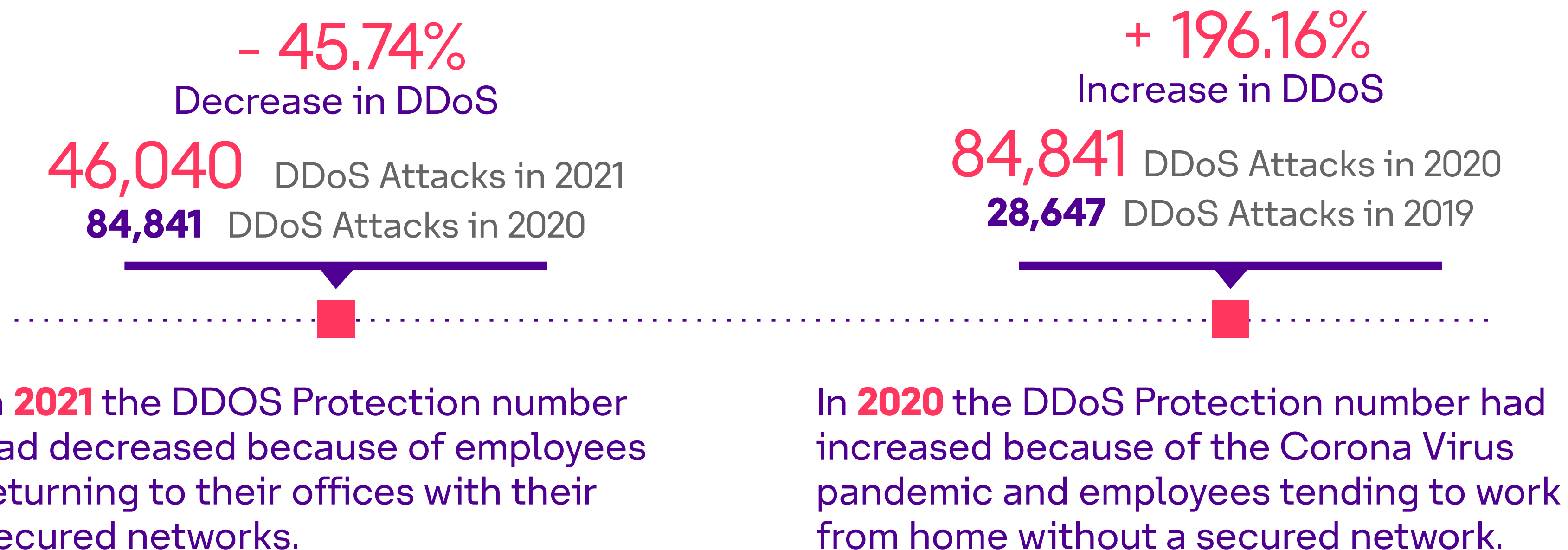
DDoS attacks
in 2021



Source : sirar Anti - DDoS service

DDoS

Attacks in Details



Source : sirar Anti - DDoS service

DDoS

Attacks in Details



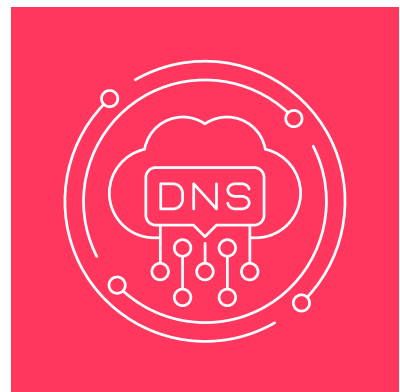
38% NTP Amplification

DDoS attacks that exploit publicly - accessible Network Time Protocol (NTP) servers to overwhelm the targeted with UDP traffic.



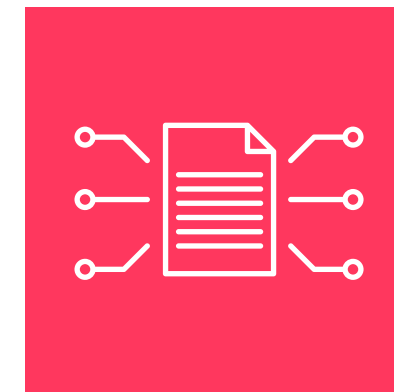
23% Others

Other vectors i.e. TCP SYN, CLDAP, Memcache.. etc.



30% DNS Amplification

DDoS attacks that massively exploit open recursive DNS servers mainly for performing bandwidth consumption DDoS attacks.



9% UDP

DDoS attacks that can be initiated when an attacker sends a large number of UDP packets to random ports on a remote host.

Vulnerability Management,
Detection and Response

sirar Battles

Vulnerability

Management, Detection and Response (VMDR)



70,016

CLOSED VULNERABILITIES

223,140

VULNERABILITIES DETECTED

Identify your Cybersecurity Vulnerabilities proactively.

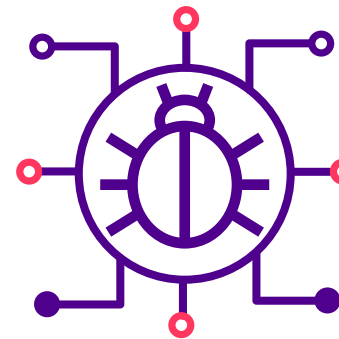
Cybersecurity is changing constantly, and new threats are emerging daily, sirar by stc vulnerability management detection and response services gives your organization a continuous, always - on, assessment of your infrastructure Cybersecurity vulnerabilities and compliance posture.

A comprehensive visibility across your entire IT assets, wherever they reside, with automated built - in threat prioritization, patching, and other response capabilities.

Email Security

sirar Battles

■ Email Security



Attackers' Victim's Statistics

sirar by stc, Cloud - based Email security service is a secure email gateway that delivers advanced multi - layered protection against the full spectrum of email borne threats. Helping customers to prevent, detect and respond to the latest email - borne threats including spam, phishing, malware, zero - day threats, impersonation, and Business Email Compromise (BEC) attacks.

83.71%

PERCENTAGE OF CLEAN EMAILS

16.30%

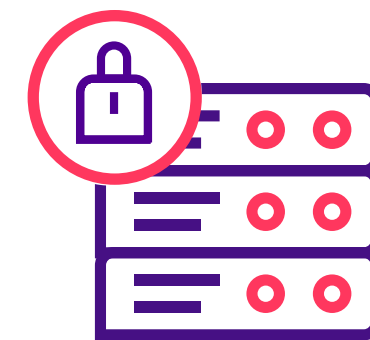
PERCENTAGE OF BLOCKED EMAILS

Web Security

sirar Battles

■ Web Security

Web Security service is a secure internet and web gateway solution, offered as a full security stack with all the in - depth protection that is ever needed. It is a security solution that prevents malicious traffic from entering an internal network of an organization. It is used by enterprises to protect their employees/ users from accessing and being infected by malicious. web content (virus, malware, ad - ware, backdoors, etc...).



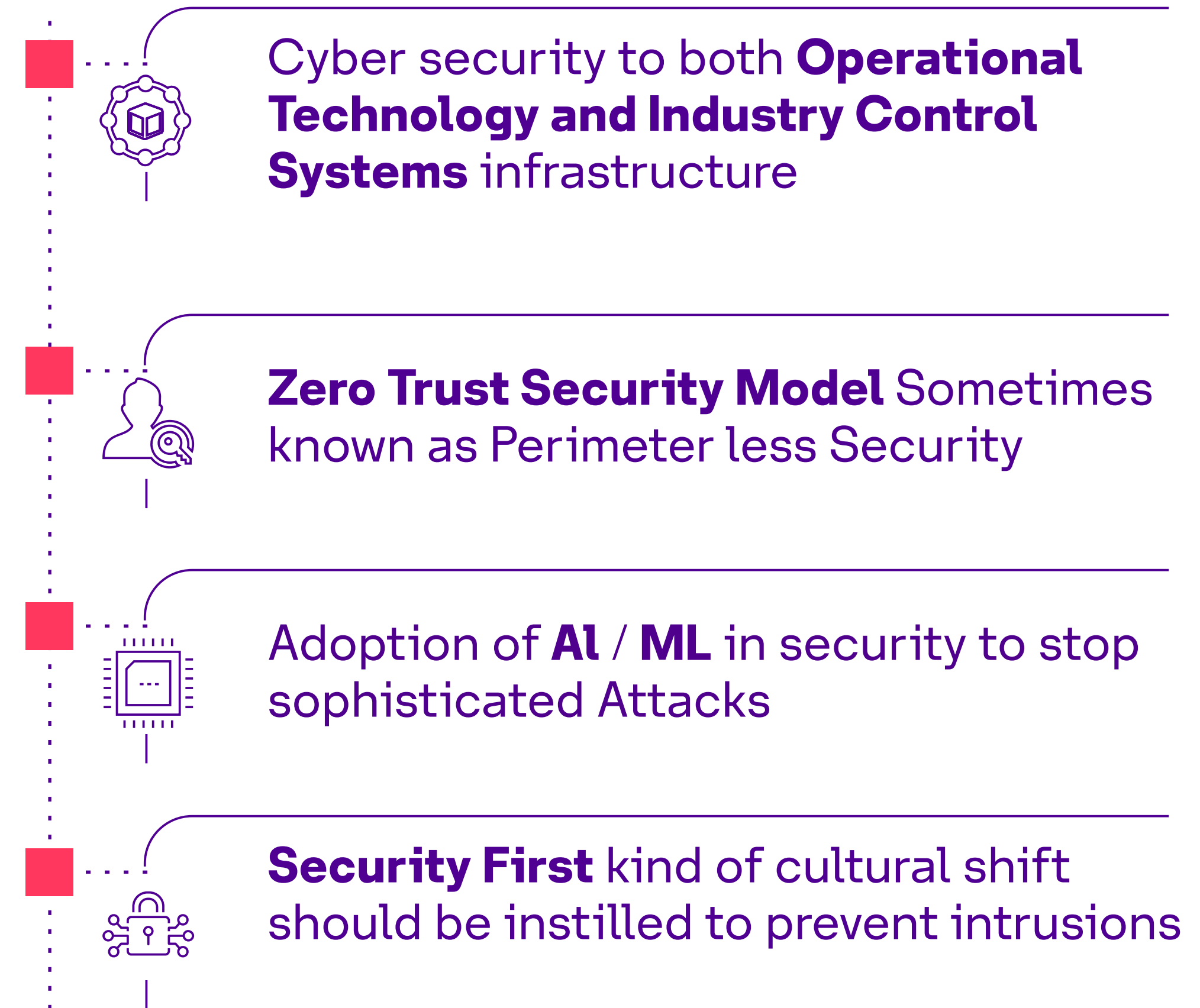
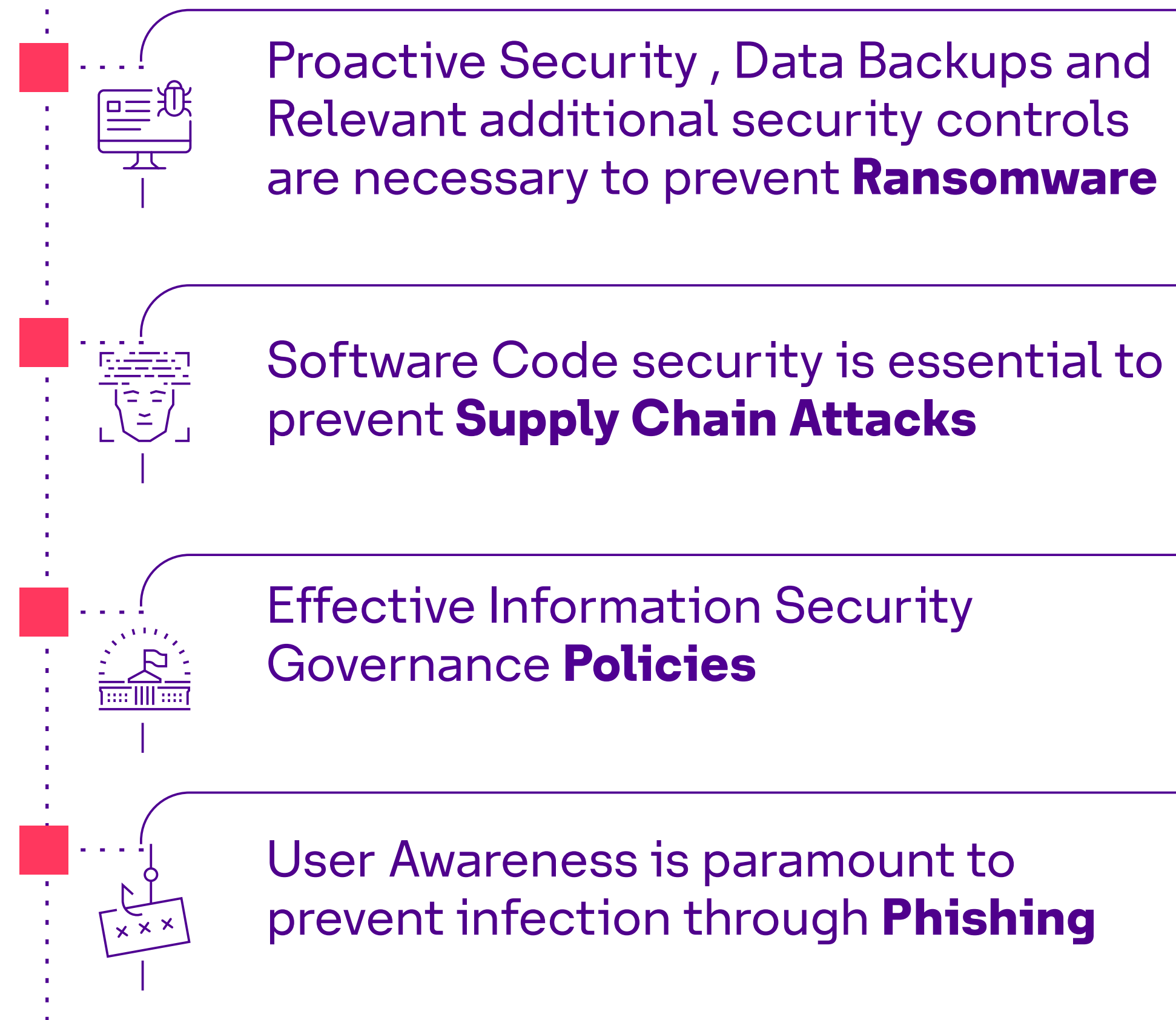
248, 630, 817 | THREATS BLOCKED

309, 064, 827 | TRANSACTIONS PROCESSED

sirar Recommendation

■ sirar

Recommendations



Confidential

SHUKRAN