

•  
•  
•  
**BRANDFENSE**



# RANSOMWARE GROUPS ACTIVITY REPORT

01.08.2022 - 08.08.2022

Prepared by : Brandfense CTI Team

Contact: [info@brandfense.io](mailto:info@brandfense.io)

•  
•

# Key Insights

Brandefense Analysts analyzed the following items this week

BRANDEFENSE

- 27 Organizations and 15 Country were targeted as a result of ransomware attack.
- More than 11.169 Gigabyte of data was stolen by threat actors.
- More than \$735.000 in ransom demanded.

# WHO HAS BEEN TARGETED?



Weekly Ransomware Group Activity Report

•  
•

# Numbers of The WEEK

---

Company

27

Targeted by  
Ransomware groups

Country

15

Affected by  
cyber attacks

IoC

4

Shared with  
TI service

•  
•

BRANDDEFENSE

# Numbers of The Attacks in July

---

Company

147

Targeted by  
Ransomware groups

Country

65

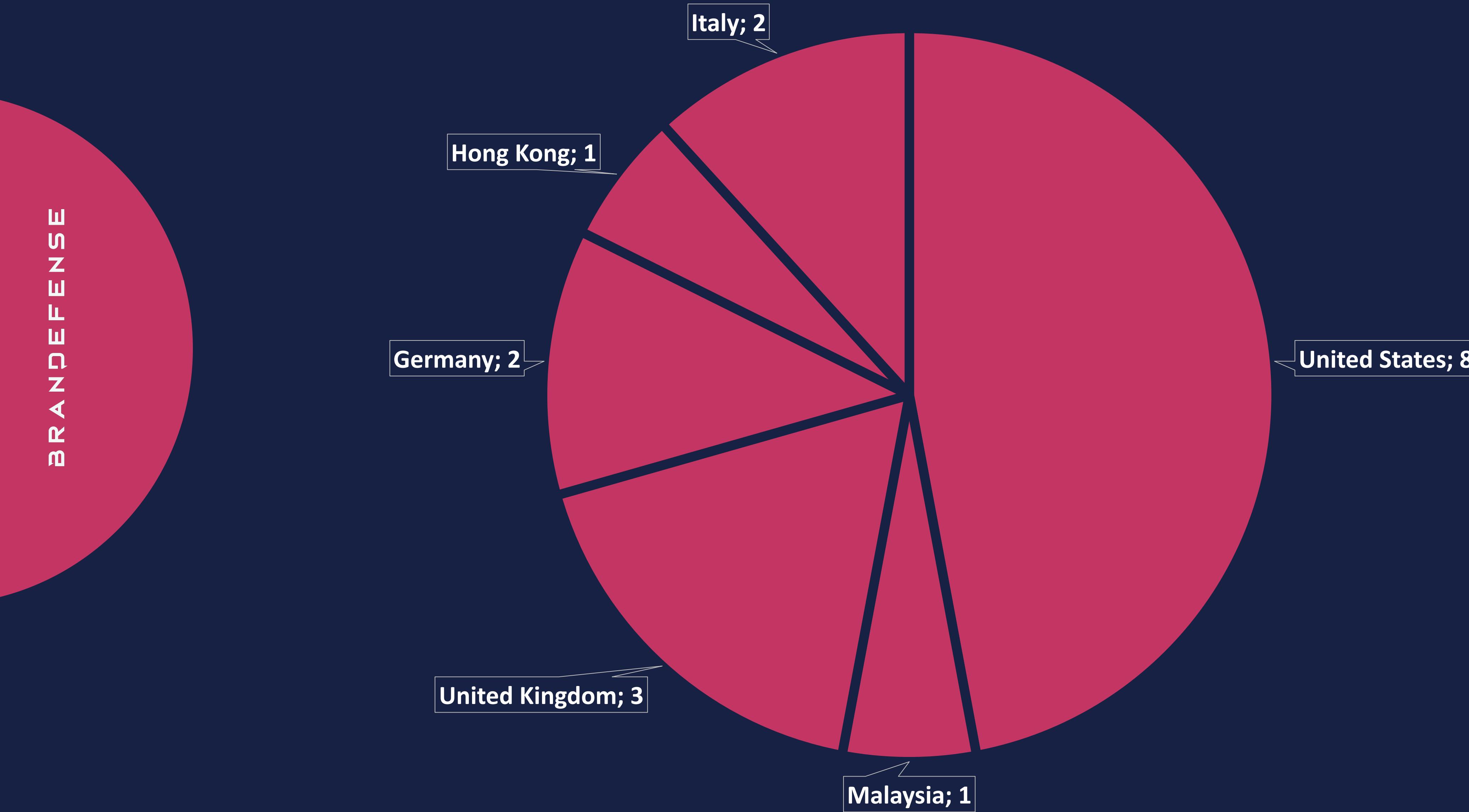
Affected by  
cyber attacks

IoC

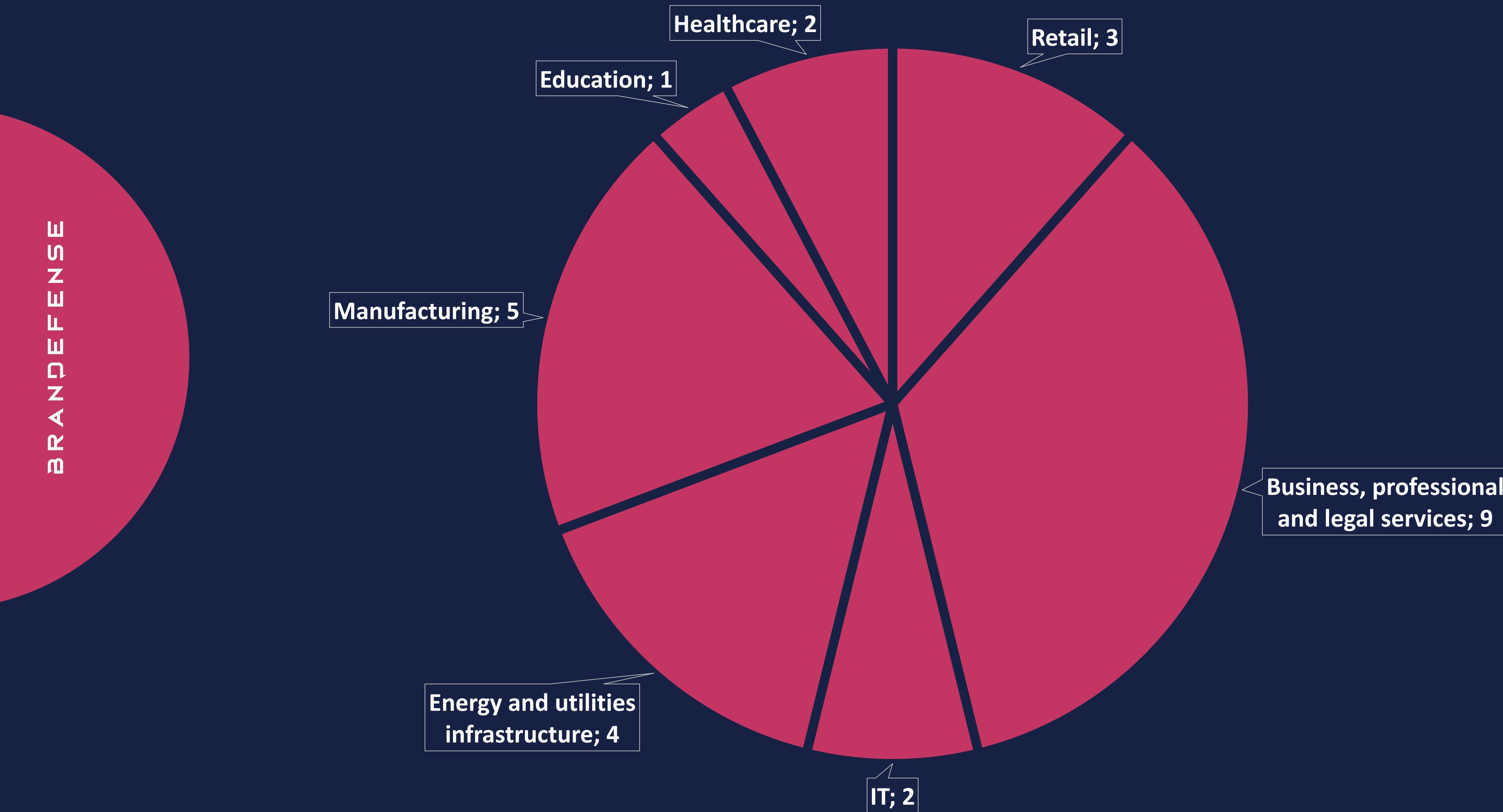
48

Shared with  
TI service

## Top Targeted Countries

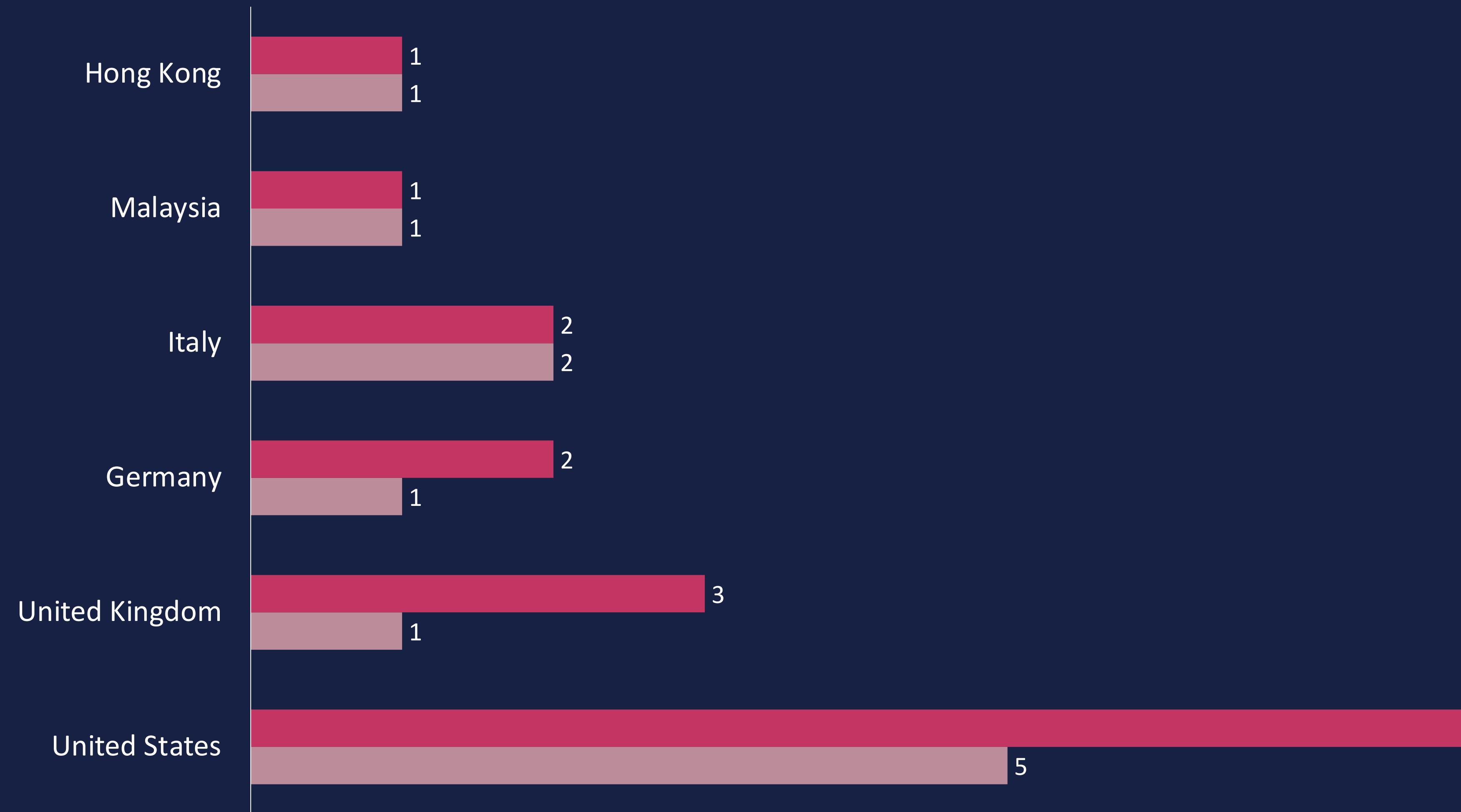


# Top Targeted Sectors



# Top Attacked Countries

Comparison With The Previous Week

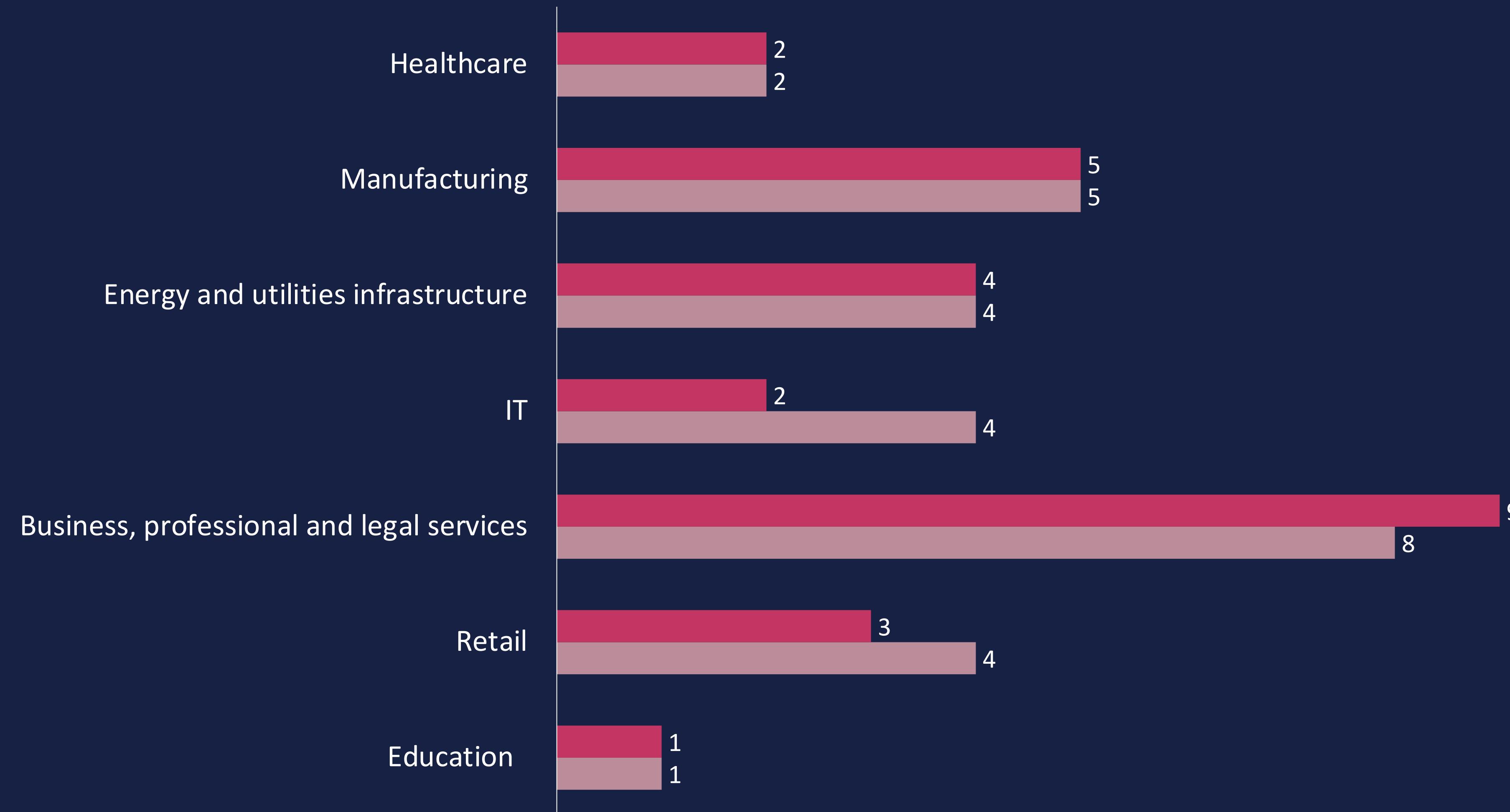


■ This week ■ Last Week



# Top Attacked Sectors

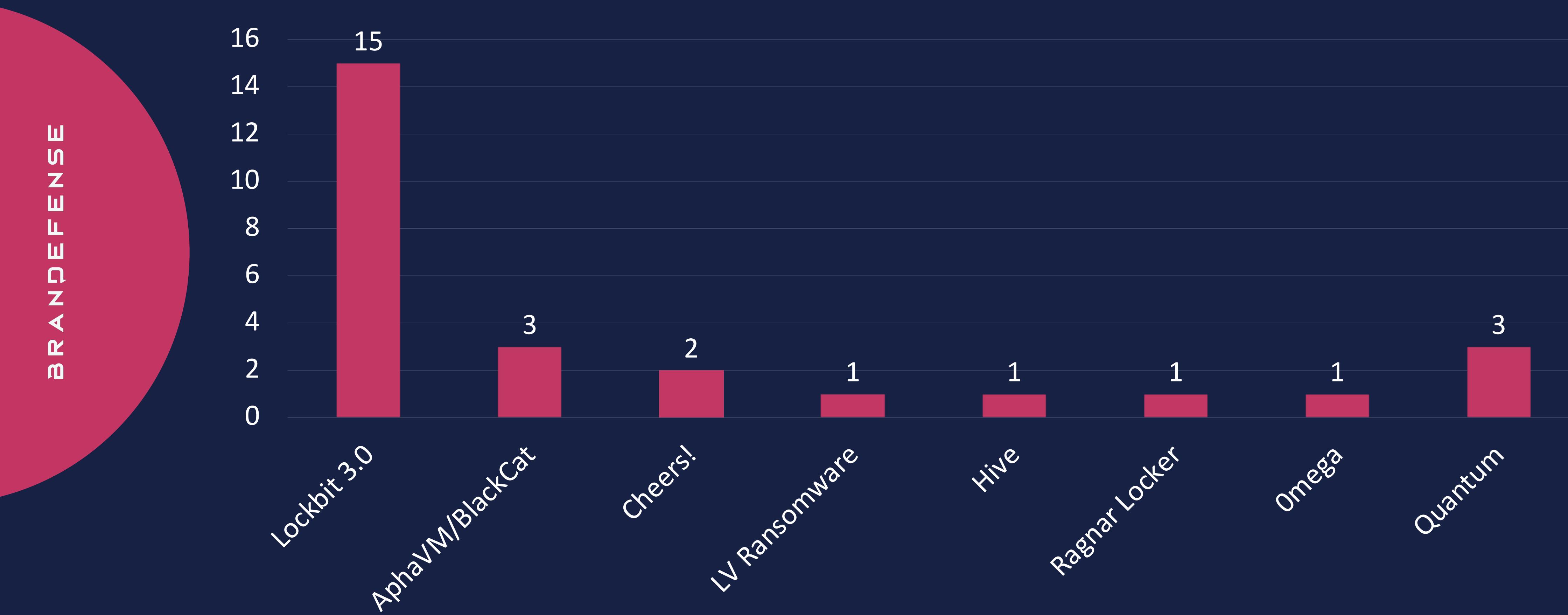
Comparison With The Previous Week



■ This week ■ Last Week

# Number of Ransomware Attacks by Groups

1 - 8 August



# List of Targeted Companies

BRAND DEFENSE

Company	Website	Industries	Country
Kangaroo	kangaroo.vn	Healthcare	Vietnam
Mario Sinacola	mariosinacola.com	Energy and utilities infrastructure	United States
Freyr Solutions	freysolutions.com	Business, professional and legal services	United States
Puma Biotechnology Inc	pumabiotechnology.com	Healthcare	United States
Scohil Construction	scohil.com	Energy and utilities infrastructure	United States
Precision Flooring Products	preflooring.com	Retail	United States
Window Rock Unified School District	wrschool.net	Education	United States
Hatcher	hatcherins.com	Business, professional and legal services	United States
Trial Pro	trialpro.com	Business, professional and legal services	United States
Hudson Contract	hudsoncontract.co.uk	Financial services	United Kingdom
Artic Building Services	articbuildingservices.com	Energy and utilities infrastructure	United Kingdom
Maxey Moverley	maxeymoverley.com	IT	United Kingdom
Güreli Yeminli Mali Müşavirlik	gureli.com.tr	Business, professional and legal services	Turkey
Versma Management Services	versma.com	Business, professional and legal services	South Africa

# List of Targeted Companies

Company	Website	Industries	Country
Valverde Hotel	valverdehotel.com	Business, professional and legal services	Portugal
Casa Pellas	casapellas.com	Retail	Nicaragua
Shopper 360	shopper360.com.my	Retail	Malaysia
AD Consulting Group	adcgroup.com	Business, professional and legal services	Italy
Tekinox	tekinox.it	Manufacturing	Italy
BEESENSE	beesense-sys.com	IT	Israel
Fosun	fosun.com	Manufacturing	Hong Kong
Axel Höer Architekten	ah-a.de	Manufactruing	Germany
Ring Plastik	ring-plastik.de	Manufacturing	Germany
ENN Group	enn.cn	Energy and utilities infrastructure	China
Liftow LTD	liftow.com	Business, professional and legal services	Canada
New West Metals	newwestmetals.com	Manufacturing	Canada
Unimasters Logistics Plc	unimasters.com	Business, professional and legal services	Bulgaria

# Groups and Attacks



Weekly Ransomware Group Activity Report

# LockBit 3.0

Victims	Industries	Stolen Data	Ransom Price
Shopper 360	Retail	178 GB	UNKNOWN
Scohil Construction	Energy and utilities infrastructure	UNKNOWN	\$70.000
Precision Flooring Products	Retail	UNKNOWN	\$100.000
Casa Pellas	Retail	165 GB	UNKNOWN
Kangaroo	Healthcare	86 GB	UNKNOWN
Tekinox	Manufacturing	4.2 GB	UNKNOWN
Window Rock Unified School District	Education	UNKNOWN	UNKNOWN
Hatcher	Business, professional and legal services	12 GB+	UNKNOWN
Trial Pro	Business, professional and legal services	UNKNOWN	UNKNOWN
New West Metals	Manufacturing	UNKNOWN	UNKNOWN
Unimasters Logistics Plc	Business, professional and legal services	UNKNOWN	UNKNOWN

•  
•  
•

# LockBit 3.0

Victims	Industries	Stolen Data	Ransom Price
Versma Management Services	Business, professional and legal services	UNKNOWN	\$50.000
Ring Plastik	Manufacturing	UNKNOWN	\$15.000
Fosun	Manufacturing	200GB+	\$500.000
Axel Höer Architekten	Manufactruing	UNKNOWN	UNKNOWN

# WHO is LockBit 3.0

LockBit ransomware is malicious software designed to block user access to computer systems in exchange for a ransom payment. LockBit will automatically vet for valuable targets, spread the infection, and encrypt all accessible computer systems on a network.

This ransomware is used for highly targeted attacks against enterprises and other organizations.

## LockBit 3.0 in the press

 Stuff.co.nz

### Ransomware group claims to have hit Eden Park caterer

A posting by the gang indicated that Melbourne-based O'Brien Group had been targeted by Lockbit 3.0 ransomware and that its computer files...



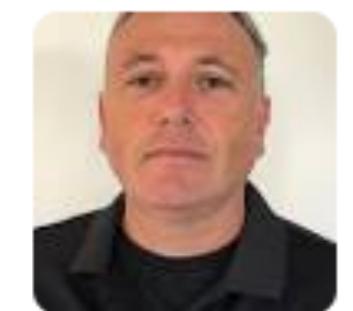
1 gün önce

[See Details](#)

 datensicherheit.de

### Ransomware-as-a-Service missbraucht Windows Defender

Es handelt sich demnach bei der Ransomware „LockBit 3.0“ um eine neuere Version einer weit verbreiteten RaaS-Familie (Ransomware-as-a-Service),...



1 saat önce

[See Details](#)

 CPO Magazine

### Suspected Lockbit Ransomware Attack on Italian Tax Agency Potentially Leaked About 100 GB of Data

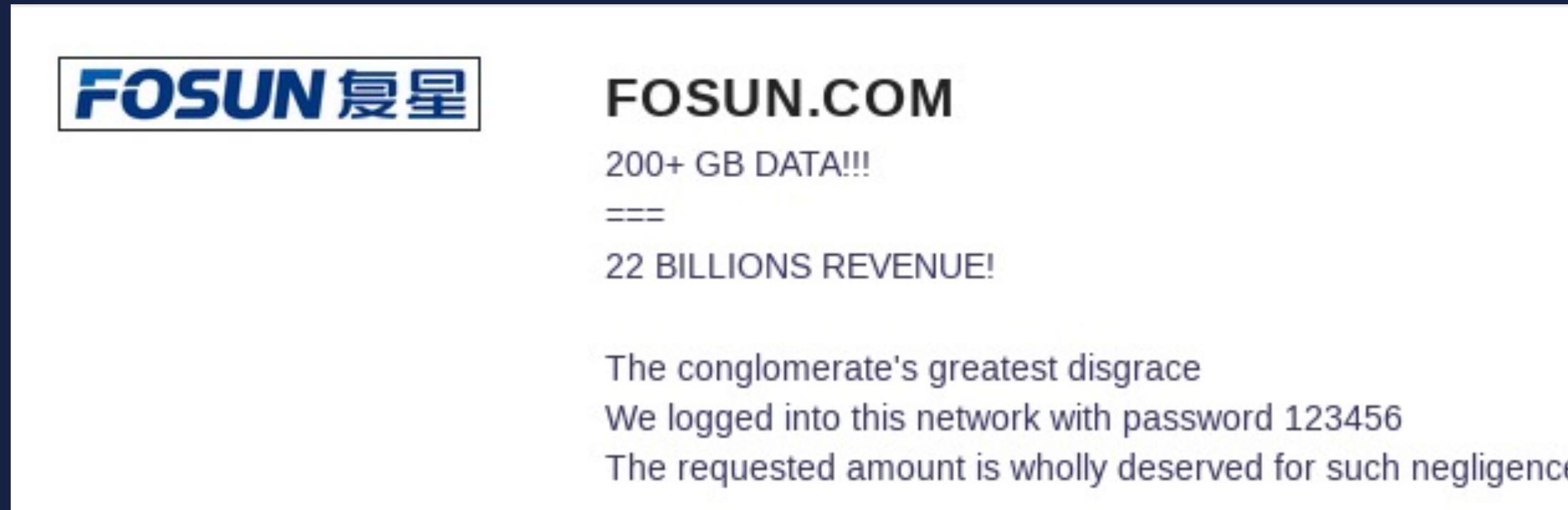
The group also developed a variant exploiting the vulnerabilities of the VMWare ESXi virtual machines. In June 2022, the extortion group released LockBit 3.0...



5 gün önce

[See Details](#)

# VICTIM CASES FOR LAST WEEK



Fosun Attack



Victim's Sensitive Document

13年审计报告	2021/8/4 15:48	文件夹
14年审计报告	2016/6/2 15:17	文件夹
15年审计报告	2017/1/12 7:37	文件夹
16年审计报告	2017/8/25 17:29	文件夹
17年审计报告	2018/9/26 12:15	文件夹
18年审计报告	2020/6/29 10:58	文件夹
1231数据收集	2017/7/14 17:54	文件夹
2012年审计报告	2016/11/4 16:33	文件夹
2015年1-4月报表	2016/1/7 9:16	文件夹
2016年1月份数据收集	2016/3/14 19:05	文件夹
2016年审计报告	2017/2/9 8:39	文件夹
2017年预算	2016/8/11 13:11	文件夹
2017业务经营分析会	2017/2/7 8:18	文件夹
2018年审计报告	2018/8/27 15:22	文件夹
Fidelidade	2019/10/9 8:17	文件夹
G Project	2015/7/10 10:58	文件夹
Ironshore	2015/7/29 7:35	文件夹
MIG	2019/10/9 8:16	文件夹
NS	2015/7/28 17:08	文件夹
Peakre	2015/10/27 14:32	文件夹
PI	2015/10/20 17:14	文件夹
保险集团Package	2015/11/27 1:58	文件夹
备用	2021/6/8 16:48	文件夹
德国runoff	2017/5/17 19:20	文件夹
复保	2017/9/19 17:00	文件夹
管会保险模板-2015年12月	2016/5/10 16:52	文件夹
管会保险模板-2016年3月 - 副本	2016/5/10 16:53	文件夹
行业数据	2016/4/6 13:32	文件夹
永安	2015/11/9 9:13	文件夹
Management accounting system dat...	2019/4/16 7:25	Outlook 项目 1,119 KB
复星保险2018Q2业务经营分析会-【葡...	2019/4/16 7:18	Outlook 项目 8,088 KB
复星保险板块2018Q2业务经营分析会-...	2019/4/16 7:22	Outlook 项目 6,968 KB
轉寄_Peak Re - Monthly Investment ...	2019/4/16 7:20	Outlook 项目 7,171 KB

Victim's Sensitive Directories

## Other Victims

**shopper360.com.my**

**PUBLISHED**

Stolen 178GB: passports, scans, financial statements, contracts, documents and more  
Shopper360 Limited is a Malaysia-based provider of shopper marketing services to

⌚ Updated: 09 Aug, 2022, 17:49 UTC 1879 ⏹

Shopper 360 Attack

**preflooring.com**

**PUBLISHED**

Since 1994, Precision Flooring Products, Inc. has been a leading manufacturer and distributor of customized prefinished mouldings to the wood flooring industry

⌚ Updated: 01 Aug, 2022, 16:37 UTC 1767 ⏹

Precision Flooring Products Attack

**kangaroo.vn**

**PUBLISHED**

Stolen: 86 GB, folder with passports, there are several confidential files, accounting, marketing, and more The Kangaroo Group was proudly established in 2003 by two

⌚ Updated: 09 Aug, 2022, 16:59 UTC 1814 ⏹

Kangaroo Attack

**scohil.com**

**PUBLISHED**

Scohil Construction Services has experience in, and the capability to perform, the following construction related activities:  
Storm Water Detention Ponds Lime /

⌚ Updated: 01 Aug, 2022, 16:24 UTC 1734 ⏹

Scohil Construction Attack

**casapellas.com**

**PUBLISHED**

Stolen: 165 gigs: CREDITCAP folders, insurance documents, credit documents, employee folders, proceedings, disputes and more Sale of new cars, liquor, industrial

⌚ Updated: 05 Aug, 2022, 06:03 UTC 1692 ⏹

Casa Pellas Attack

**tekinox.it**

**PUBLISHED**

Workshop for the production of turned parts, Tekinox Srl is specialized in the processing of all families of stainless steels

⌚ Updated: 10 Aug, 2022, 06:59 UTC 1868 ⏹

Tekinox Attack

## Other Victims

### [hatcherins.com](#)

8D 15h 30m 33s

With deep-roots in the insurance community dating back to 1942, Hatcher has been serving Florida for over half-a-century.

🕒 Updated: 08 Aug, 2022, 00:01 UTC

892

Hatcher Attack

### [trialpro.com](#)

8D 15h 32m 48s

The seasoned injury law specialists at Trial Pro, have well over a combined 100 years of experience practicing all types of injury law, including but not limited to personal injury,

🕒 Updated: 08 Aug, 2022, 00:02 UTC

893

Trial Pro Attack

### [newwestmetals.com](#)

7D 19h 35m 14s

New West Metals Inc offers a full range of stainless steels of all types and shapes

🕒 Updated: 06 Aug, 2022, 12:36 UTC

928

New West Metals Attack

### [unimasters.com](#)

1D 05h 01m 02s

Unimasters Logistics Plc is a dynamic, advanced supply chain management company, headquartered in Bulgaria with fully owned subsidiaries in Romania and

🕒 Updated: 09 Aug, 2022, 14:02 UTC

901

Unimasters Logistics Plc Attack

### [versma.com](#)

9D 16h 58m 03s

\$ 50 000

Versma Management Services provides a full suite of customisable, end-to-end business processing services, which are tailored to each of our broker clients. Our

🕒 Updated: 07 Aug, 2022, 13:59 UTC

709

Versma Management Services Attack

### [ring-plastik.de](#)

7D 14h 56m 23s

\$ 150 000

Experience since 1969 Centrally located between Augsburg and Munich, Ring-Plastik has been manufacturing high-quality plastic parts since 1969. From the development

🕒 Updated: 07 Aug, 2022, 13:58 UTC

760

Ring Plastik Attack

- 
- 
- Other Victims

wrschool.net

5D 05h 14m 27s

Window Rock Unified School District is proud to be one of the finest School Districts on the Navajo Nation. Following our mission and vision statements, our team of more than

 Updated: 08 Aug, 2022, 06:01 UTC    941 

Window Rock Unified School District Attack

ah-a.de

9D 17h 09m 13s

Axel Höer Architekten is a construction firm. They offer architectural and civil engineering

 Updated: 10 Aug, 2022, 06:12 UTC    208 

Axel Höer Architekten Attack

# Cheers!

Victims	Industries	Stolen Data	Ransom Price
Güreli Yeminli Mali Müşavirlik	Business, professional and legal services	4.8 TB	UNKNOWN
Hudson Contract	Financial services	120 GB	UNKNOWN

# WEEKLY VICTIM CASES

## AN TURKEY CERTIFIED PUBLIC ACCOUNTANCY FIRMS -UNPAY

Target : Güreli Yeminli Mali Müşavirlik  
Domain URL : <http://www.gureli.com.tr/>  
Affected by GDPR : No  
Number of clients : 1300+

Attack time : 8/7/2022  
Volume of leaked data : 4.8 TB  
First public date : 8/8/2022 (If not contacted)  
Full public date : 8/15/2022 (If negotiations fail)

Güreli Yeminli Mali Müşavirlik Attack

Leaked file types :

- Financial data for all clients
- Other office documents
  - Customer tax certificate
  - Payroll
  - financial data
  - Profit distribution statement
  - Client company receipt
  - Customer Tax Report
  - List of Client Attorneys
  - Client Independent Audit Report
  - Client Anonymous Board Annual Report
  - Client Litigation Report
  - bill
  - mortgage certificate
  - Mortgage Loan List
  - Balance Sheet and Income Statement
  - lawyer's letter
  - Criminal financial reporting

The first public data download URL:

- Public time : 8/8/2022 (If not contacted)
- We can delay leak if you contact us
- You can download it with a normal browser, we will check whether the download link is valid in time
- <https://gofile.io/d/wRnCWv>

Victim's Document Tree

•  
•  
Other Victims

· 08-05-2022 · /

# AN BRITISH FINANCIAL COMPANY -UNPAY

---

Target : Hudson Contract  
Domain URL : <https://www.hudsoncontract.co.uk/>  
Affected by GDPR : Yes

---

Attack time : 7/18/2022  
Volume of leaked data : 120GB  
Full public date : 8/15/2022 (If negotiations fail)

---

Leaked file types :

- All financial data
- All project files
- The latest backup of all business system databases
- All employee personal information
- Customer contracts and receipts

Hudson Contract Attack

# ALPHV/Blackcat

Victims	Industries	Stolen Data	Ransom Price
AD Consulting Group	Business, professional and legal services	UNKNOWN	UNKNOWN
Artic Building Services	Energy and utilities infrastructure	237 GB	UNKNOWN
Mario Sinacola	Energy and utilities infrastructure	200 GB	UNKNOWN



AD Consulting Group Attack



Victim's Sensitive Document



Victim's Identity Card

## Other Victims



**Artic Building Services**

Tue Aug 02 2022

Artic Building Services Limited was formed in 1998 to provide engineering solutions within the public and private sectors.

Each division of Artic is led by a member of the Board who makes sure that our

Attachments — 5

[Read more](#)

Artic Building Services Attack



**MarioSinacola**

Tue Aug 02 2022

Mario Sinacola & Sons, Excavating, Inc. is a dynamic, family-owned firm that has built a reputation for excellence, creative problem solving and superior performance. We have the state-of-the-art equipment, talented people,

[Read more](#)

Mario Sinacola Attack

# Hive

Victims	Industries	Stolen Data	Ransom Price
ENN Group	Energy and utilities infrastructure	UNKNOWN	UNKNOWN

# WEEKLY VICTIM CASES

## ENN Group

ENN Group is an energy and natural gas production company headquartered in the Hebei province of China.

Stock Symbol: 600803

\*\*\*\*\* SENSITIVE DATA WILL BE PUBLISHED SOON \*\*\*\*\*

Website	Revenue
<a href="http://www.enn.cn">www.enn.cn</a>	\$100 000M
Employees	
39 474	



Encrypted at  
**6 July 2022**  
**19:29:00**



Disclosed at  
**4 August 2022 · 12:10:30**

Share



ENN Group Attack

- 
- 

# LV Ransomware

Victims	Industries	Stolen Data	Ransom Price
Valverde Hotel	Business, professional and legal services	10 GB+	UNKNOWN

# WEEKLY VICTIM CASES

## VALVERDEHOTEL.COM

<https://www.valverdehotel.com>

HACKED AND MORE THEN 10GB DATA LEAKED



Victim's Identity Card

publication at 09.08.22 06:00 GMT

## DECLARAÇÃO SOB COMPROMISSO DE HONRA - REGULARIZAÇÃO TRIBUTÁRIA E CONTRIBUTIVA -

Para efeitos da alínea a) do n.º 1 do artigo 177.º-A do Código de Procedimento e de Processo Tributário e n.º 1 do artigo 208.º do Código dos Regimes Contributivos do Sistema Previdencial de Segurança Social, declaro, sob compromisso de honra e na qualidade de representante da empresa

ESTORIL 8023 – Investimentos Turísticos, S.A. , NIPC nº 508 276 659 , com sede em Av. Marginal n.º 8023, 2765-249 Estoril , nos termos e para os efeitos de acesso à linha de crédito Linha APOIO À ECONOMIA19 , que a empresa tem as suas situações tributária e contributiva regularizadas, junto da Autoridade Tributária e Aduaneira e a Segurança Social.

Cascais , 04 de Agosto de 2020

O Responsável,  
  
(Na qualidade de \_\_\_\_\_ Administradores \_\_\_\_\_)

Victim's Sensitive Document

# Quantum

Victims	Industries	Stolen Data	Ransom Price
Freyr Solutions	Business, professional and legal services	400 GB	UNKNOWN
BEESENSE	IT	1.3 TB	UNKNOWN
Liftow LTD	Business, professional and legal services	255 GB	UNKNOWN

# WEEKLY VICTIM CASES



400GB      2022-08-08

## Freyr Solutions

Freyr is one of the largest, global, Regulatory-focused solutions and services companies for the Life Sciences industry supporting, Large, Medium, and Small size global Life sciences companies (Pharmaceutical | Generics | Medical Device | Biotechnology | Biosimilar | Consumer Healthcare | Cosmetics | Food and Food Supplements | Chemicals) in their entire Regulatory value-chain; ranging from Regulatory Strategy, Intelligence, Dossiers, Submissions, etc. to Post-approval/Legacy Product Maintenance, Labeling, Artwork Change Management, and other related functions

[READ MORE](#)      1.2K

Freyr Solutions Attack



1.3TB      2022-08-04

## BEESENSE

BeeSense designs, develops and manufactures advanced, unique, multi-sensor technology-based solutions and independent, wireless communication & power infrastructures for intelligence, surveillance and reconnaissance in the homeland security and defense sectors.

[READ MORE](#)      5.7K

Beesense Document



TOYOTA  
MATERIAL HANDLING

255GB      2022-08-04

## Liftow LTD

Founded in 1960, Liftow is a Toyota forklift dealer group in North America. They offer new and pre-owned inventory of forklifts as well as parts and services.

[READ MORE](#)      4.7K

Liftow TLD Card

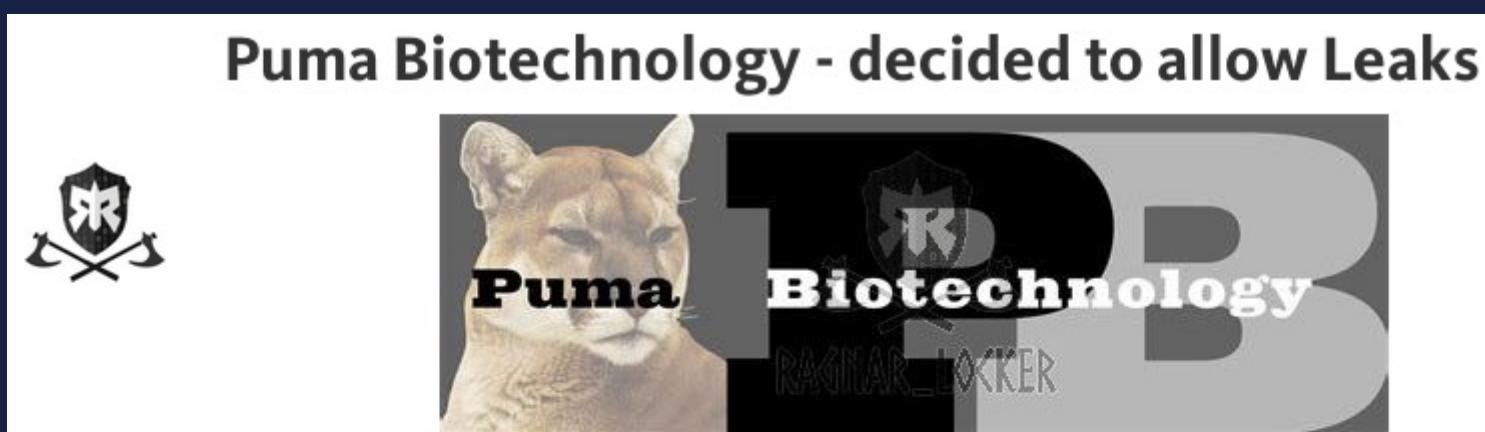
- 
- 

# Ragnar Locker

Victims	Industries	Stolen Data	Ransom Price
Puma Biotechnology Inc	pumabiotechnology.com	1.15 TB	UNKNOWN

# WEEKLY VICTIM CASES

**Puma Biotechnology - decided to allow Leaks**



Puma Biotechnology, Inc. is a bio pharmaceutical company with a focus on the development of drug candidates in the clinical-testing phase.

Headquarters: 10880 Wilshire Blvd, Ste 2150, Los Angeles, California, 90024, United States

Phone Number: (424) 248-6500

Website: [www.pumabiotechnology.com](http://www.pumabiotechnology.com)

Stock Symbol: PBYI

**Puma Biotechnology Attack**

File Home Share View

This PC > ISCSI Data (E:) > Data > Contracts >

Search Co... P

24 items State: Shared

Name	Date modified	Type	Size
Contract Process and RESOURCES	6/9/2022 12:02 PM	File folder	
Hotel Agreements	4/8/2022 11:43 AM	File folder	
LinkSquares	5/16/2022 1:22 PM	File folder	
Master Service Agreements	6/6/2022 3:51 PM	File folder	
NonDisclosure Agreements_CDAs	6/7/2022 9:13 AM	File folder	
Other Signed Contracts	2/26/2021 9:55 AM	File folder	
Statement of Work	6/2/2022 11:23 AM	File folder	
Templates	6/2/2022 1:13 AM	File folder	
Terms library	6/3/2022 2:19 PM	File folder	
a.txt	9/24/2021 1:58 PM	Text Document	821 KB
b.txt	9/28/2021 3:22 PM	Text Document	1,516 KB
bsansspace.csv	9/30/2021 11:31 AM	CSV File	1,442 KB
bsansspace.txt	9/30/2021 10:41 AM	Text Document	1,422 KB
Contract List v2.xlsx	10/5/2021 10:54 AM	XLSX File	508 KB
Contract List.csv	9/29/2021 11:23 AM	CSV File	1,535 KB
Contract Tracking Vendors - Spreadsheet...	11/11/2021 10:29 AM	XLSX File	25 KB
Evergreen Renewal Contracts.xlsx	3/11/2022 11:31 AM	XLSX File	18 KB
MedAffairs Milestone Tracker_2021 Q3.pdf	10/8/2021 11:11 AM	Adobe Acrobat D...	386 KB
MedAffairs Milestone Tracker_2021 Q3.xlsx	10/8/2021 11:09 AM	XLSX File	2,324 KB
MedAffairs Milestone Tracker_2021 Q4.xlsx	1/18/2022 10:33 AM	XLSX File	2,170 KB
MedAffairs Milestone Tracker_2022 Q1.xlsx	4/8/2022 7:05 PM	XLSX File	2,265 KB
MedAffairs_Milestone_Tracker_2021_Q4.p...	1/14/2022 10:15 AM	Adobe Acrobat D...	2,273 KB
Puma Supplier Spend Authorization w Pa...	7/30/2021 12:14 PM	XLSX File	179 KB
Thumbs.db	4/7/2022 3:36 PM	Data Base File	140 KB

Victim's Computer

# Omega

Victims	Industries	Stolen Data	Ransom Price
Maxey Moverley	IT	152 GB	UNKNOWN

# WEEKLY VICTIM CASES



**0mega**

[clearnet onion](#)

**Maxey Moverley**  
Electronics repair & refurbishment, technical service, CCTV | 100% | 152 GB | 2022-05-23

[MAXEY\\_1.7z \(4.6 GB\)](#)  
[MAXEY\\_2.7z \(15.7 GB\)](#)  
[MAXEY\\_3.7z \(17.6 GB\)](#)  
[MAXEY\\_4.7z \(24.6 GB\)](#)

Maxey Moverley Attack

- 
- 

# RansomHouse

Victims	Industries	Stolen Data	Ransom Price
Puma Biotechnology	Healthcare	2.1 TB	UNKNOWN



# WEEKLY VICTIM CASES

**8 Italy Districts**

Comune di Reggello, Comune di Pelago, Comune di Rufina, Comune di Londa, Comune di Godenzo, and Unione di Comuni Valdarno and Comune di Valdisieve, Comune di Pontassieve

**Website Revenue Employees**

**Evidence packs:** [Download](#)    **Password:** no password

**8 Italy Districts Attack**

A new pandemic is raging out there in Italy Government structures! Well, guess it's not new at all. The main symptom is having passwords like 12345678 for critical resources that store sensitive data which leads to quite predictable consequences and threatens ordinary people. It saddens us even more that even after the intrusion was announced to these guys, almost no credentials were changed! After watching their Whatsapp for 4 days we can surely that these people care only about saving their jobs and not about the safety of personal data people entrusted to them. Well, having infrastructure down is just the mild phase of it, the real challenge starts when the data starts to be disclosed for public!

**toscana energia green**

Al fine di valutare, senza alcun tipo di vincolo o di onere a carico dell'Ente, tale opportunità e dunque perfezionare una proposta tecnica ed economica degli interventi e dei servizi energetici da realizzare sarebbe per noi indispensabile poter preventivamente effettuare un *audit* energetico degli stessi.

Nell'eventualità in cui la nostra proposta possa essere di qualche interesse per codesto Comune chiediamo la Sua disponibilità a volerci accordare la possibilità di effettuare un sopralluogo tecnico presso Codesta Amministrazione e di consentirci l'accesso ai dati necessari.

Le chiediamo a tal fine di indicarci il nominativo di un referente dell'Amministrazione in modo da poter convenire le eventuali modalità e tempi del suddetto intervento.

In allegato troverà un parere reso dalla Scuola Sant'Anna in ordine alla legittimità della proposta di TEG: il personale della Scuola convenzionato con TEG sarà comunque a disposizione di Codesta Amministrazione, insieme agli altri incaricati di TEG, per affiancare l'Amministrazione, qualora interessata, nelle attività propedeutiche alla selezione del contraente e all'affidamento del servizio.

Restando a disposizione per ogni ulteriore chiarimento si rendesse necessario porgo distinti saluti

L'Amministratore Delegato  
*(Ivano Bianchi)*

**Victim's Sensitive Document**

# Mitigation Suggestions

- 
- 
- 



Weekly Ransomware Group Activity Report

1

Provide regular training in order to raise awareness of cyber security among your employees,

---

2

Identify, prioritize and back up the asset that you need to protect at regular intervals and keep 3 different copies of the created backups in two different media types and one outside the institution,

---

3

Behave suspiciously against e-mails of unknown origin and the file attachments they contain, if possible, do not open them,

---

4

Use licensed and up-to-date operating systems,

---

5

Use reliable anti-virus solutions,

---

6

Block all IoC (Indicator of Compromise) findings in this report by security devices.

---

# Indicator of Compromise



Weekly Ransomware Group Activity Report



# Indicator of Compromises

## FileHash-SHA256

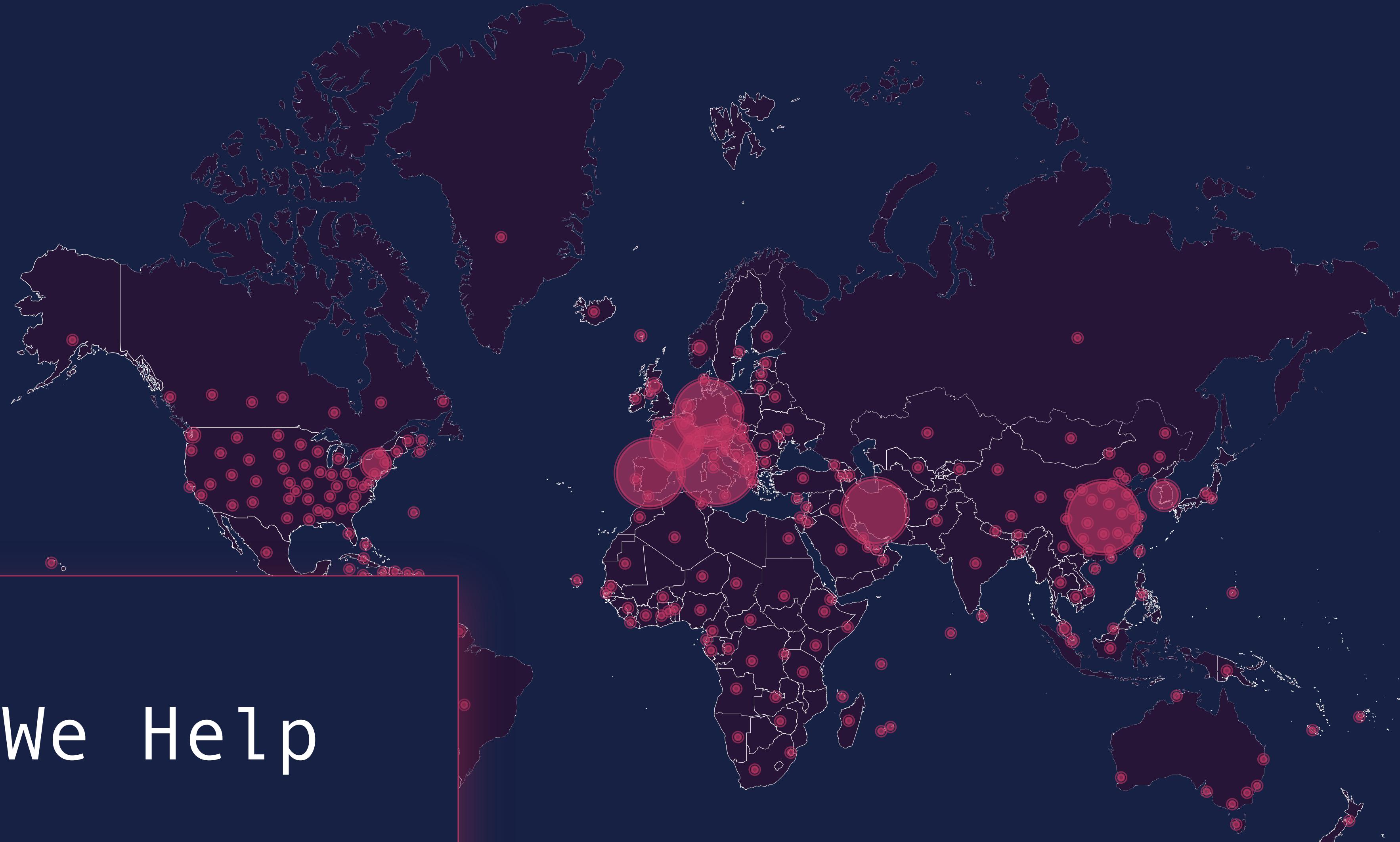
24d49f947f968c4f654ebfa2d4c0bdd3a8ddf45cfa909dc8b36b557724b14361

90ed51fea616dedcb23c6dbd131f6f216ec507c0399c8aae4ee55c4501f77270

8f62d06bbcc5c2ef2db32f0079903759ed296b80ed6d2795abdf730346f05fde

0a82b37e1a7cb6d8e8379796e929774b30fd93a7438782df2bd6b66cad0626a2

How  
Can We Help  
You?



# What We Are Doing?

Brandefense is the proactive digital risk protection solution for organizations.

Our AI-driven technology constantly scans the online world, including the dark, deep and surface web, to discover unknown events, automatically prioritize risks and deliver actionable intelligence you can use instantly to improve security.



## Account Takeover Detection

Identify the account takeover incidents with botnet and email breach monitoring service.



## Phishing Takedown Service

Identify the possible phishing domains with advanced rules and monitor them all.



## Deepweb Monitoring

Cybercriminals are talking, sharing, and exploiting inside the dark web. Then monitor this place deeply.



## Takedown the Threats

When Brandefense sends you an incident, know what you should do and takedown the threat quickly.

•  
•  
•

# Find the Perfect Packages For You



## Cyber Intelligence

You can get access to the high confidence threat intelligence feed, so you know what threats are coming your way before they happen.

[Learn More](#) >>>



## Brand & Reputation Protection

With our early action alerts, you'll have time to respond to incidents before they become significant problems and damage your company's reputation.

[Learn More](#) >>>



## Exposure Management

Enterprises increase technology investments day by day. We provide visibility about the attack surface and digital risks.

[Learn More](#) >>>

# BRANDFENSE

## Digital Risk Protection Services

### 360° Visibility



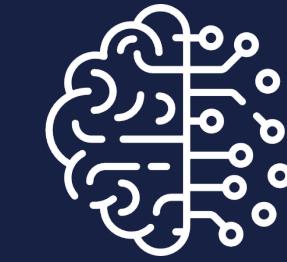
Get an accurate overview of how your company looks from an external perspective.



### Threat Hunting

Investigate and enrich the indicators that you found and optimized the response time

### AI Driven Detection



Identify the digital risks from our cyber crime database with AI-driven detection engines.



### Time Effective

Eliminates false positive incidents and focus on using your time more effectively

[Request Demo »»](#)