BRANDEFENSE

RANSOMWARE GROUPS ACTIVITY REPORT

01.08.2022 - 08.08.2022

Prepared by : Brandefense CTI Team

Contact: info@brandefense.io

Key Insights

Brandefense Analysts analyzed the following items this week

- 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?

Numbers of The WEEK

BRANDEFENSE

Company

27

Targeted by
Ransomware groups

Country

15

Affected by
cyber attacks

IoC

4

Shared with
TI service

Numbers of The Attacks in July

BRANDEFENSE

Company

147

Targeted by
Ransomware groups

Country

65

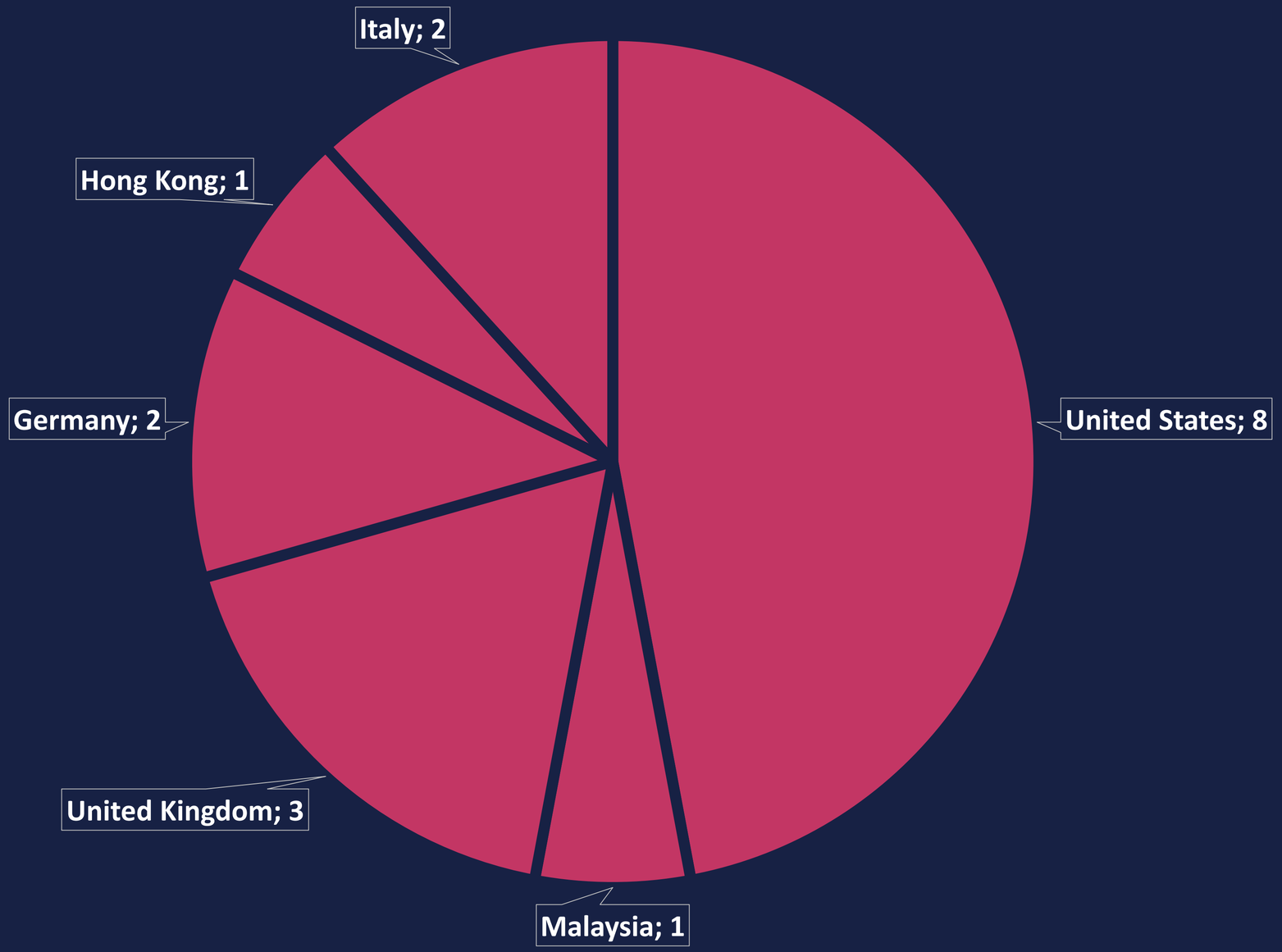
Affected by
cyber attacks

IoC

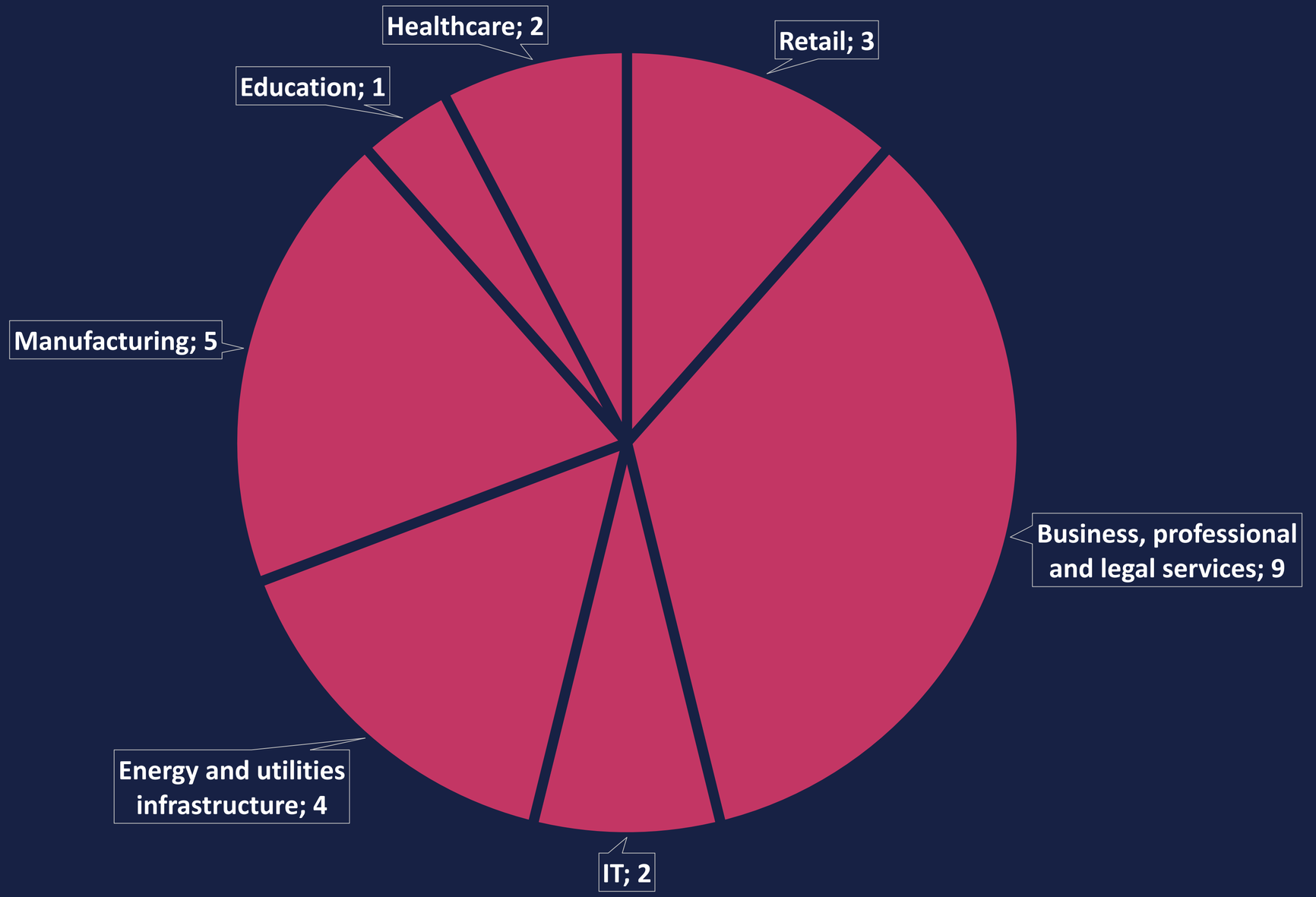
48

Shared with
TI service

Top Targeted Countries

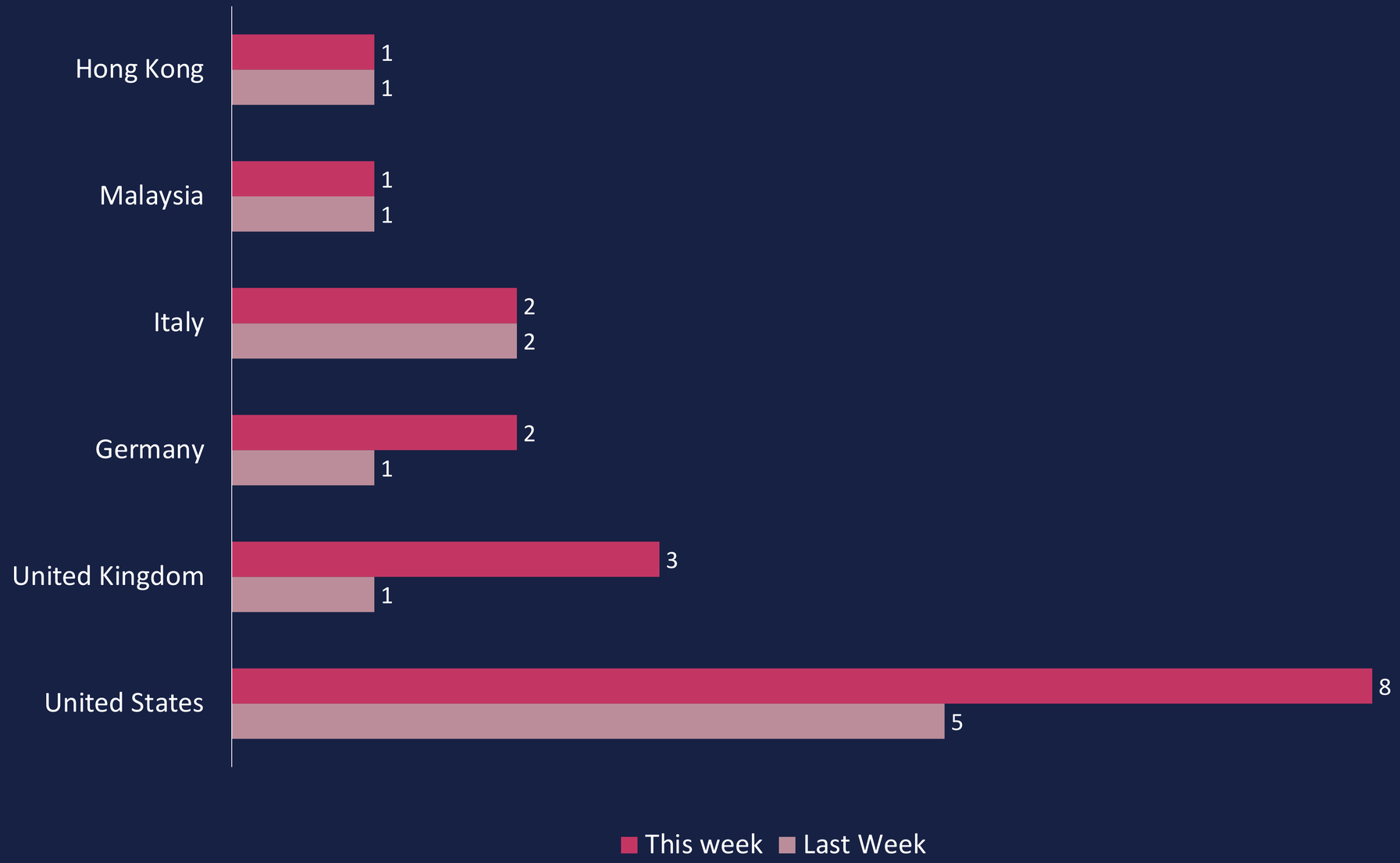


Top Targeted Sectors



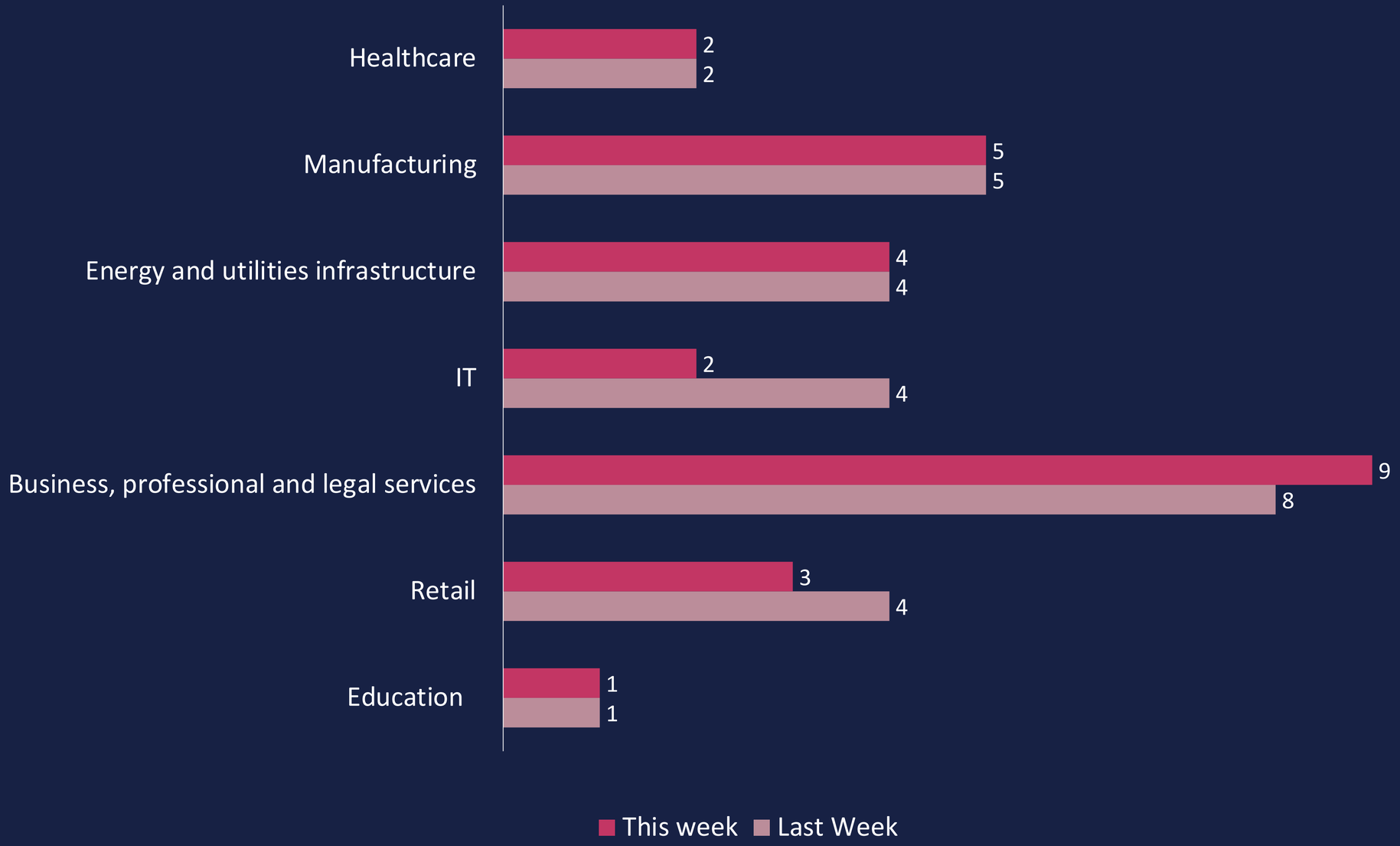
Top Attacked Countries

Comparison With The Previous Week



Top Attacked Sectors

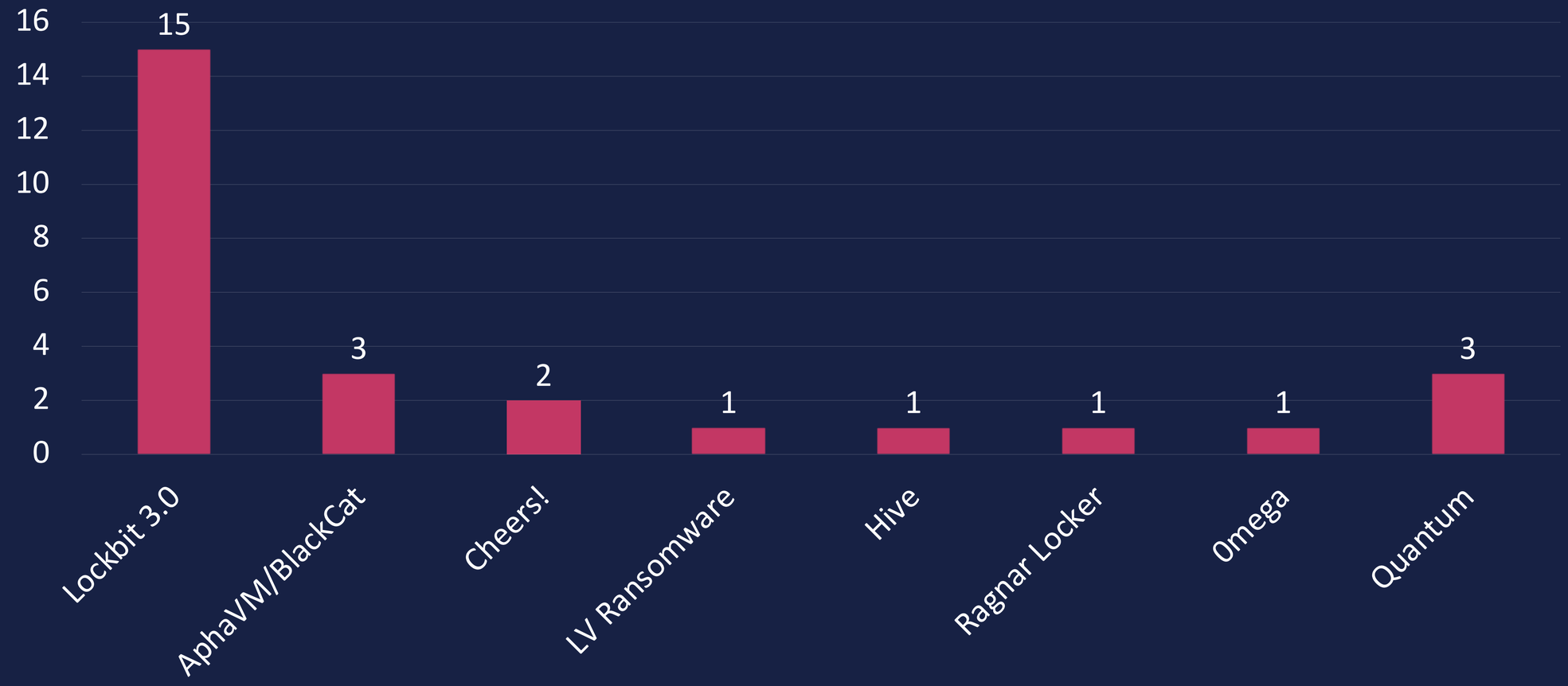
Comparison With The Previous Week



BRANDEFENSE

Number of Ransomware Attacks by Groups

1 - 8 August



List of Targeted Companies

Company	Website	Industries	Country
Kangaroo	kangaroo.vn	Healthcare	Vietnam
Mario Sinacola	mariosinacola.com	Energy and utilities infrastructure	United States
Freyr Solutions	freyrsolutions.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 Managment 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

BRANDEFENSE

Groups and Attacks

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 Managment 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.COM

200+ GB DATA!!!

===

22 BILLIONS REVENUE!

The conglomerate's greatest disgrace
We logged into this network with password 123456
The requested amount is wholly deserved for such negligence

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
转寄_ Peak Re - Monthly Investment ...	2019/4/16 7:20	Outlook 项目	7,171 KB

Victim’s Sensitive Directories

Other Victims

Shopper 360 Attack

Precision Flooring Products Attack

Kangaroo Attack

Scohil Construction Attack

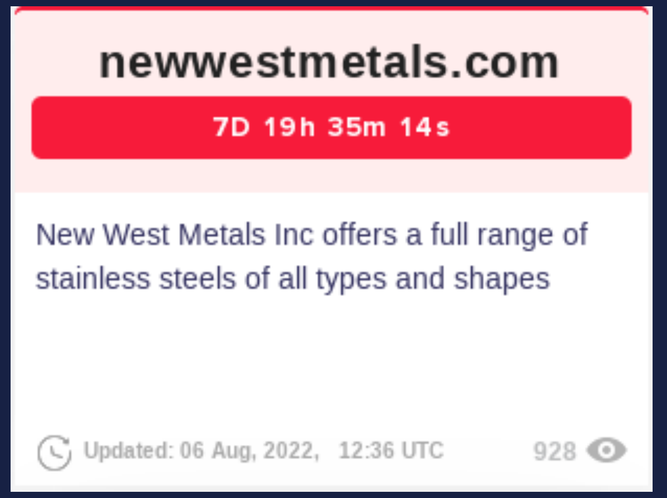
Casa Pellas Attack

Tekinox Attack

Other Victims

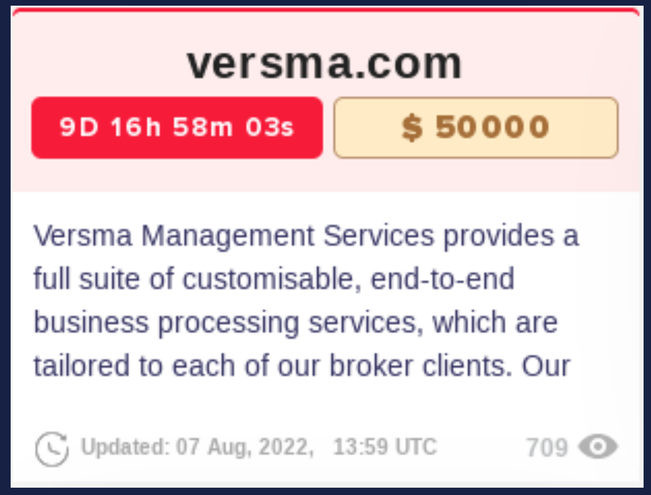
Hatcher Attack

Trial Pro Attack



New West Metals Attack

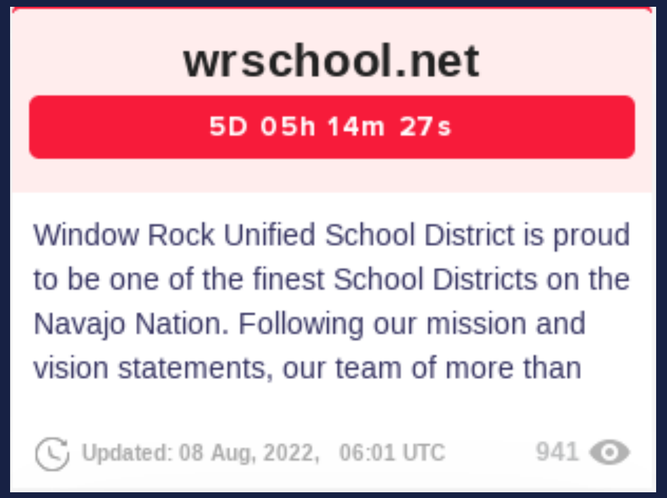
Unimasters Logistics Plc Attack



Versma Managment Services Attack

Ring Plastik Attack

Other Victims



Window Rock Unified School District Attack

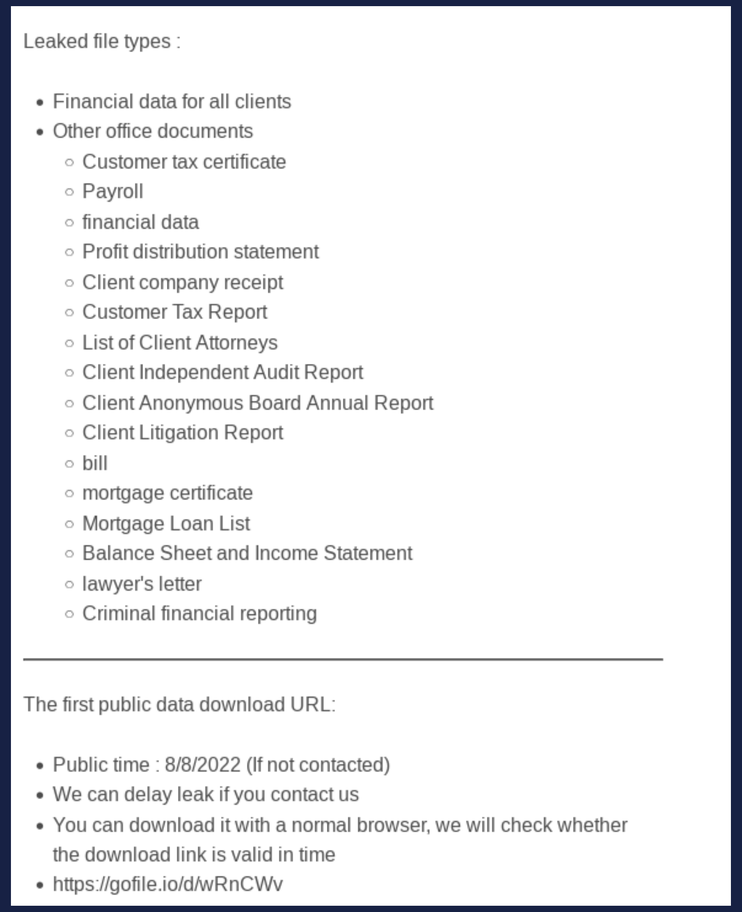
Axel Höer Architekten Attack

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

Güreli Yeminli Mali Müşavirlik Attack



Victim’s Document Tree

Other Victims

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

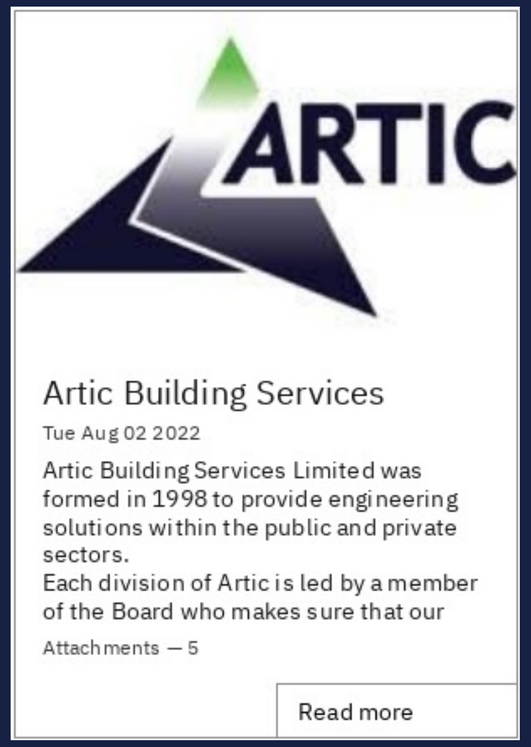
WEEKLY VICTIM CASES

AD Consulting Group Attack

Victim's Sensitive Document

Victim's Identity Card

Other Victims



Artic Building Services Attack

Mario Sinacola Attack

Hive

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

WEEKLY VICTIM CASES

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

publication at 09.08.22 06:00 GMT

https://www.valverdehotel.com

HACKED AND MORE THEN 10GB DATA LEAKED

Victim's Identity Card

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

adad

O Responsável, ESTORIL 8023 - INVESTIMENTOS TURÍSTICOS, S.A. A Administração

(Na qualidade de Administradores)

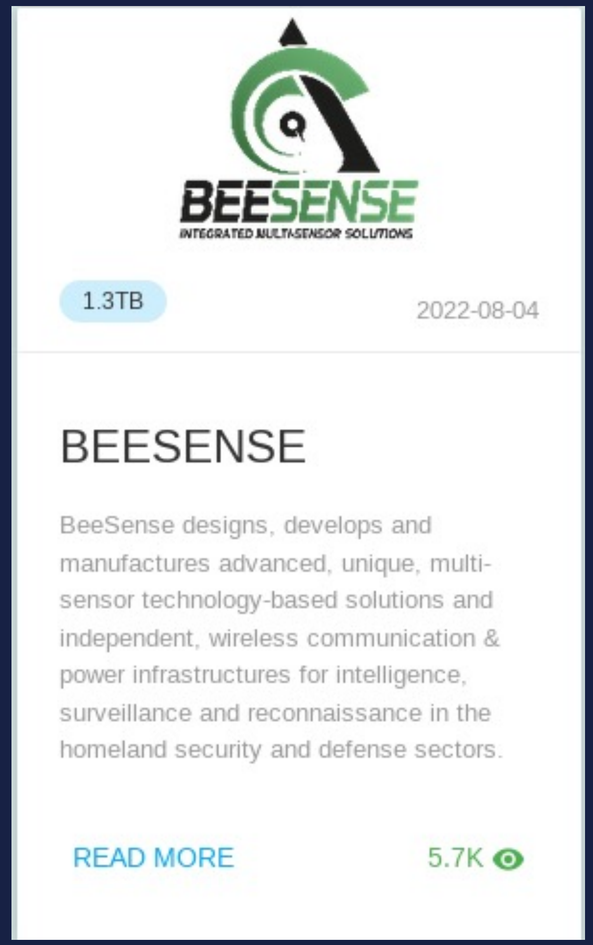
Victim's Sensitive Document

Quantum

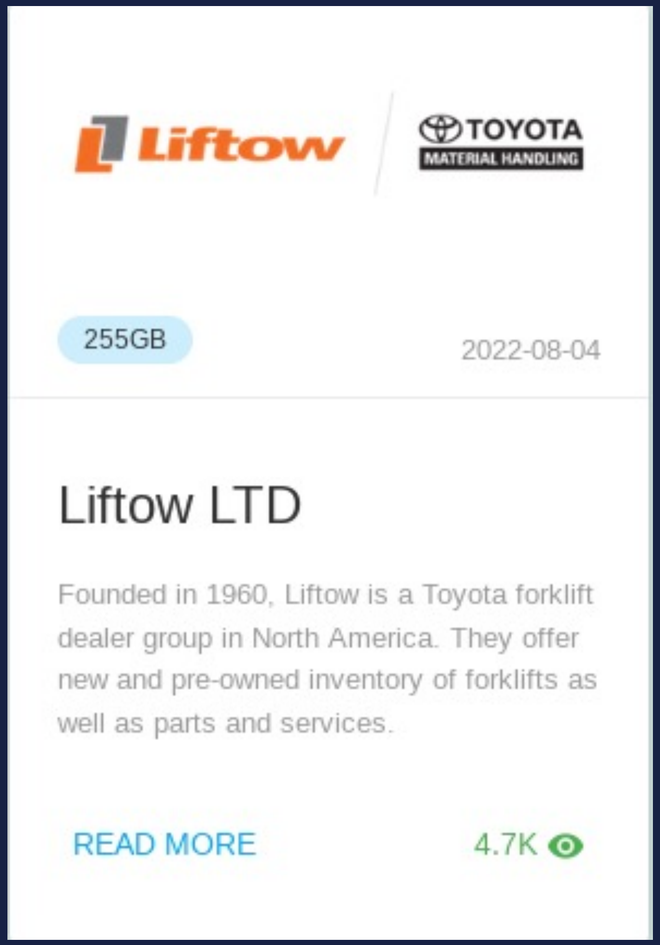
Victims	Industries	Stolen Data	Ransom Price
Freyr Solutions	Business, professional and legal services	400 GB	UNKNOWN
BEESENSE	IT	1.3 TB	UNKNOWN
Liftow LTD	Business, professional and legal services	255 GB	UNKNOWN

WEEKLY VICTIM CASES

Freyr Solutions Attack



Beesense Document



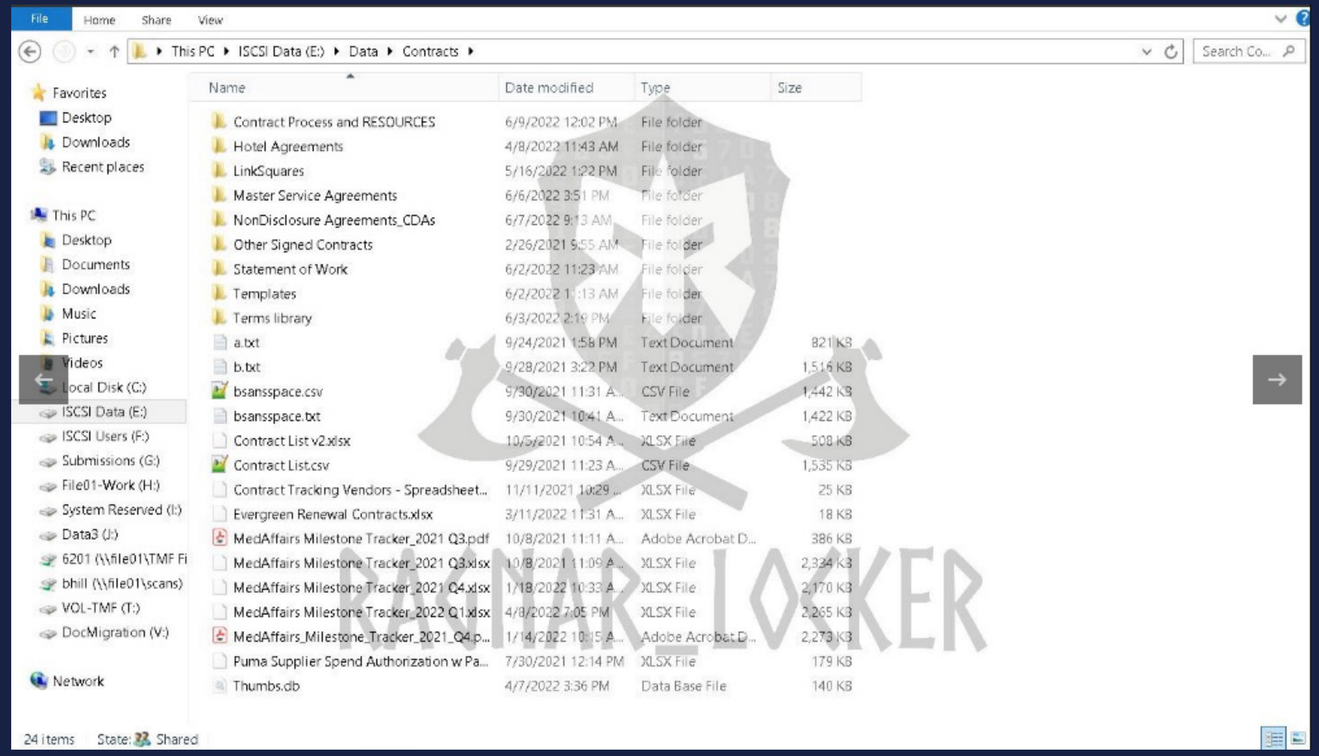
Liftow TLD Card

Ragnar Locker

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

WEEKLY VICTIM CASES

Puma Biotechnology Attack

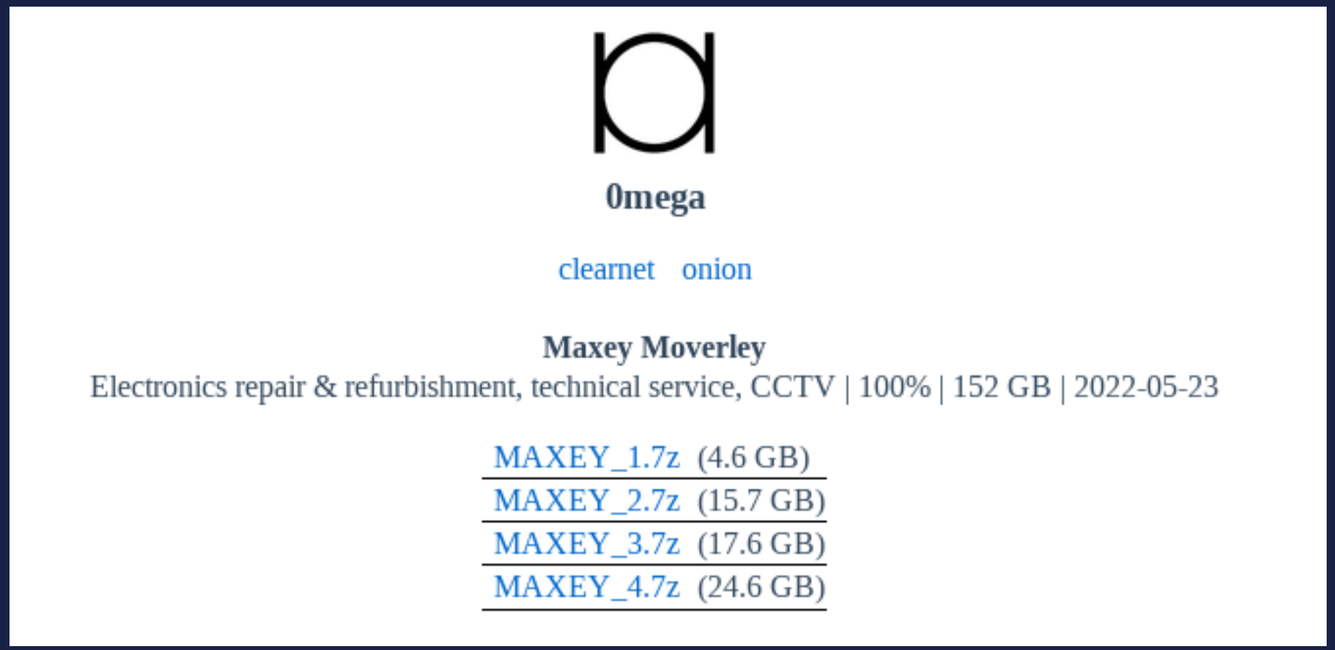


Victim's Computer

Omega

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

WEEKLY VICTIM CASES

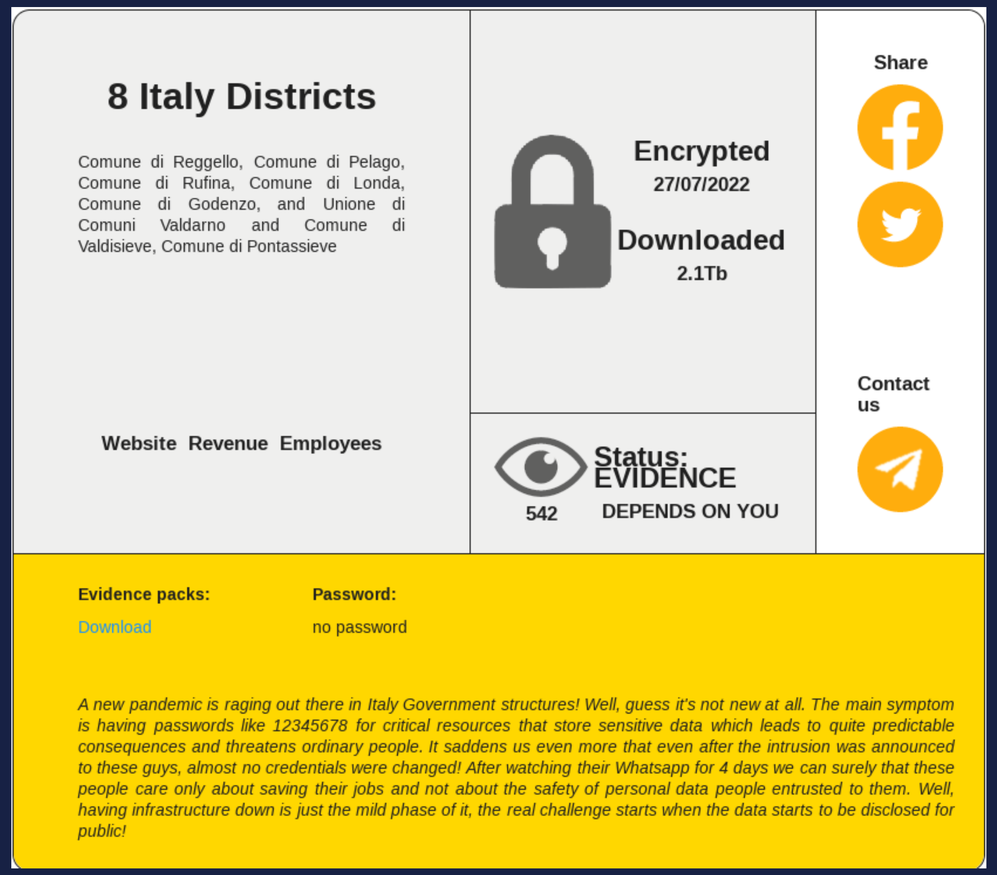


Maxey Moverley Attack

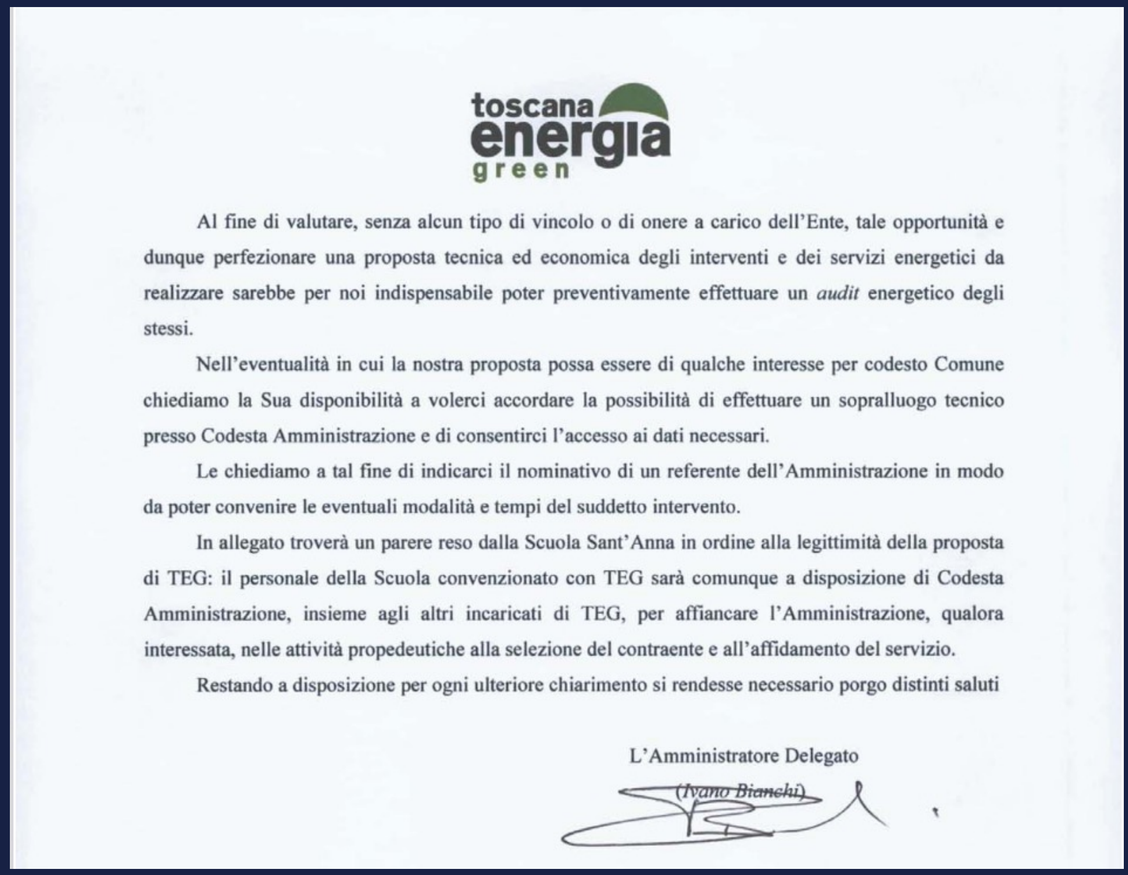
RansomHouse

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

WEEKLY VICTIM CASES



8 Italy Districts Attack



Victim's Sensitive Document

BRANDEFENSE

Mitigation Suggestions

BRANDEFENSE

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,

BRANDEFENSE

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.

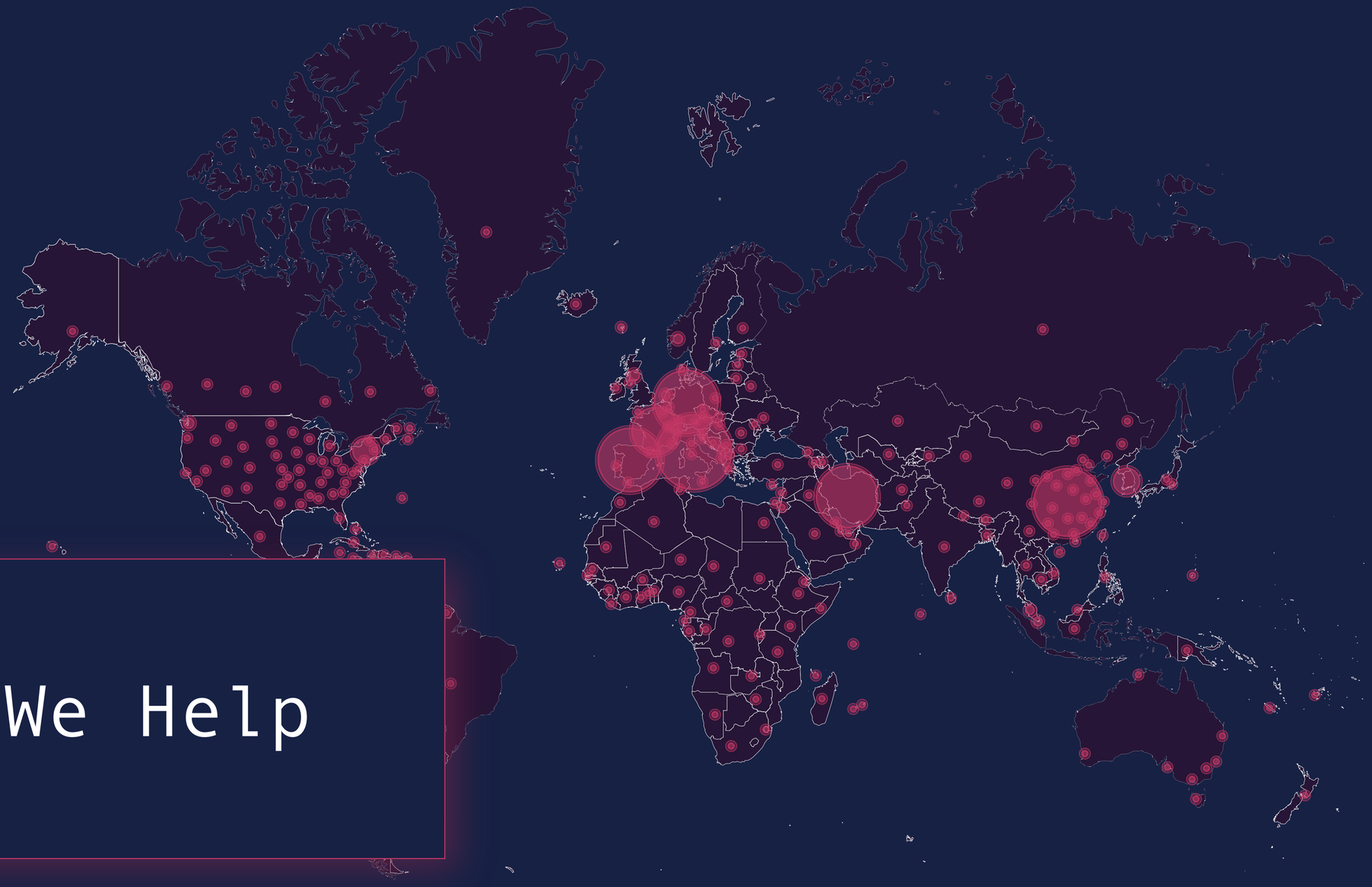
BRANDEFENSE

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

BRANDEFENSE

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 »