



BRANDEFENSE

RANSOMWARE GROUPS ACTIVITY REPORT

25.07.2022
Weekly Report

Prepared by : Brandefense CTI Team
Contact: info@brandefense.io



Weekly Ransomware Activities

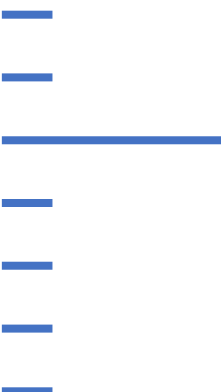
This report prepared by Brandefense Threat Intelligence Team, includes Ransomware attacks that took place between 18.07.2022 and 25.07.2022. Activities and published leaks of the Ransomware groups explained in details such as; which institutions targeted by threat actors, how much damage has been done, and when is the data captured by the attackers would be leaked to the internet if the ransom is not paid included.

The mentioned threat actors operate on Deepweb services and these services are constantly monitored by the Brandefense Digital Risk Protection Platform. Findings on this report are very important in order to raise security awareness against ransomware groups and their activities to be aware of current threats.

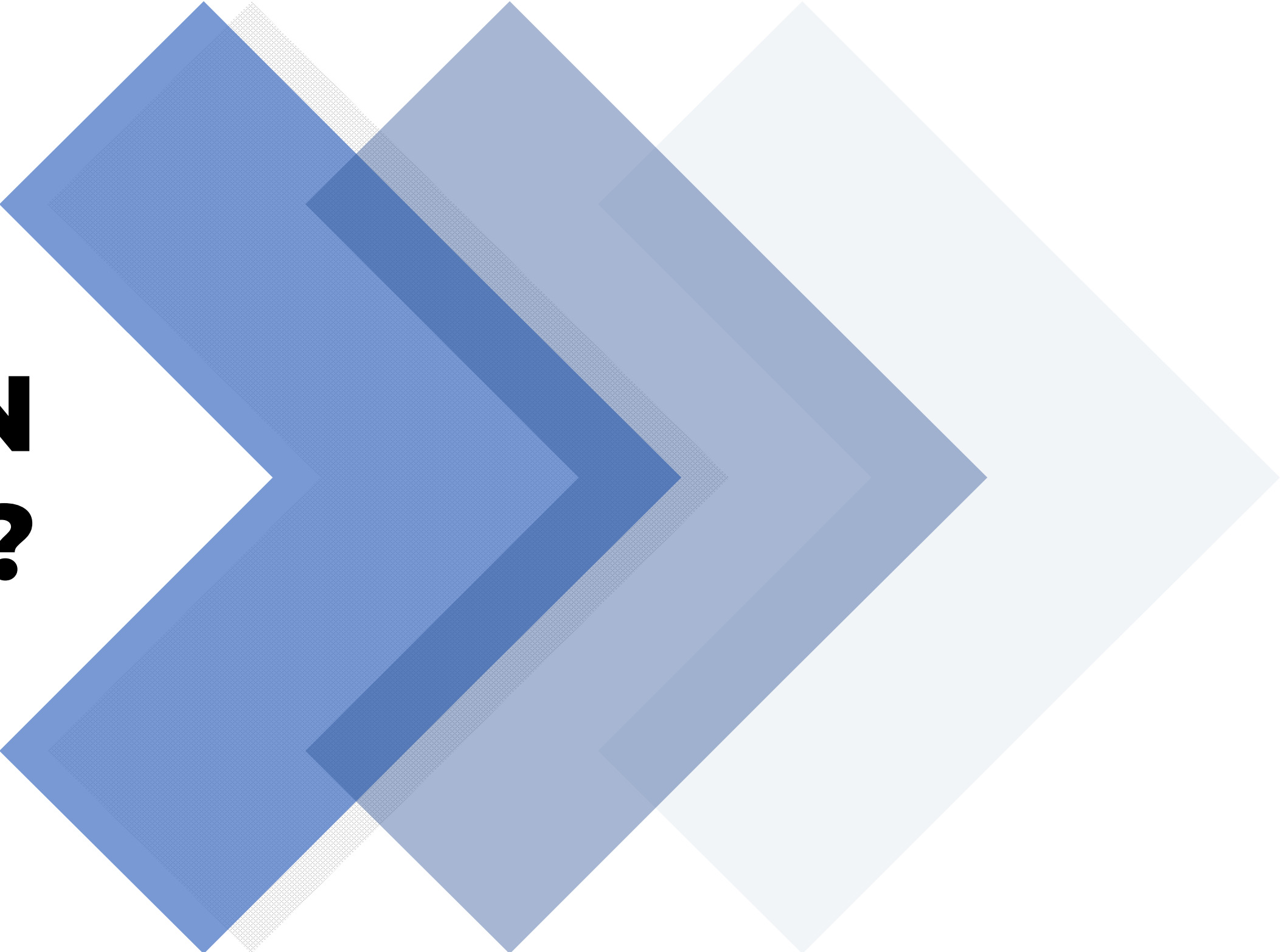
Ransomware is an online cyberattack by cybercriminals or nation-state-sponsored groups that demand monetary ransom to restore access to encrypted or compromised data. Ransomware attacks are mostly successful via the phishing techniques.

There are many different sectors targeted by the attacks, with 33% of the victims having an annual income of \$100M or less. The average payout for ransomware attacks that demanded hundreds of dollars has now risen to tens of thousands of dollars within 5 years.

In short, the Ransomware threats are growing and the ransom amounts are increasing significantly with the attacks that take place. Attackers target companies of different sizes, regardless of industry, and even amateur cyber threat actors cause disproportionate damage. Preventing ransomware threats requires a strong security architecture. Therefore, it is vital for organizations to invest in cybersecurity solutions against ransomware to protect themselves.²⁵



WHO HAS BEEN TARGETED?

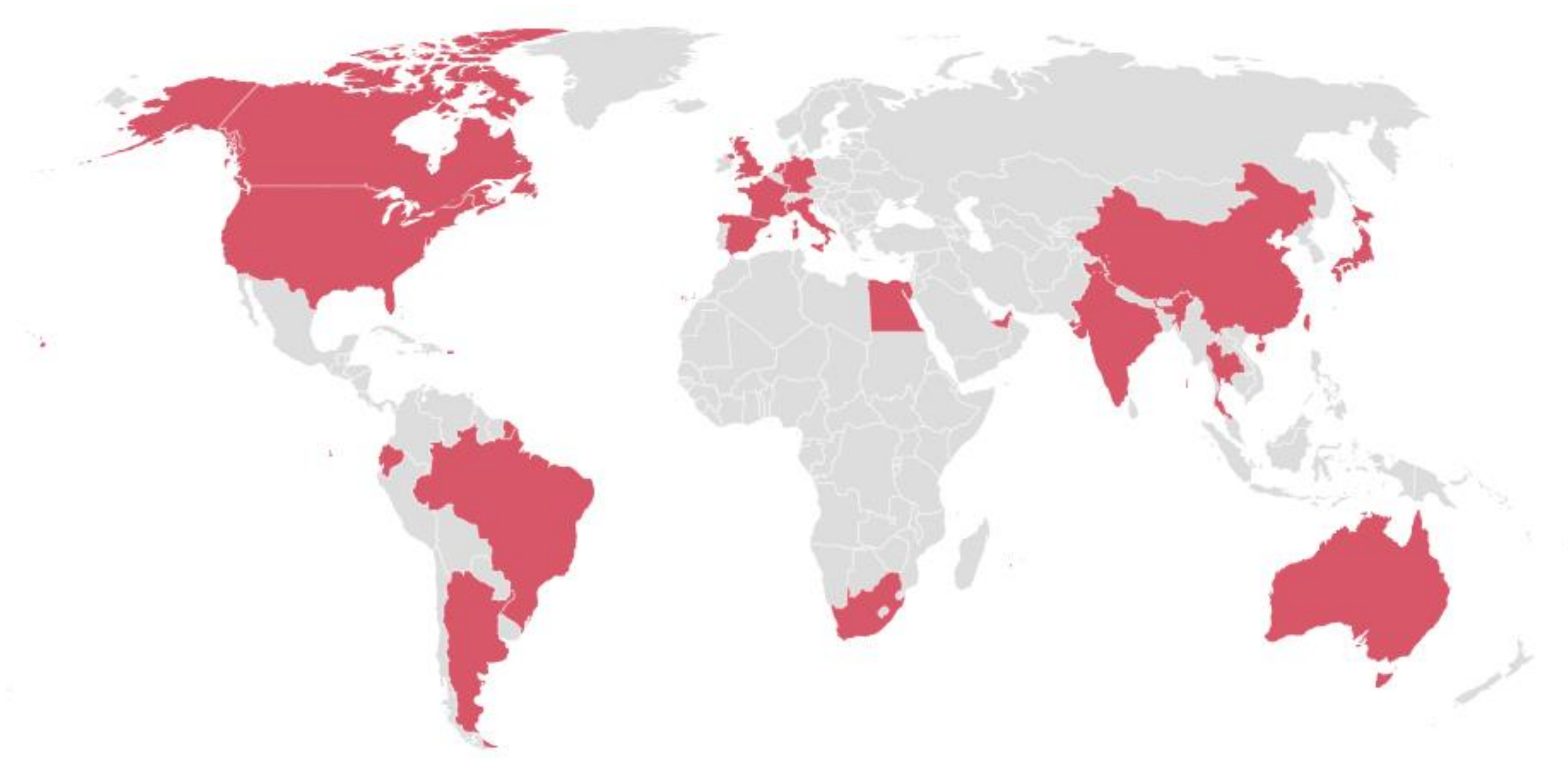


Weekly Ransomware Group Activity Report

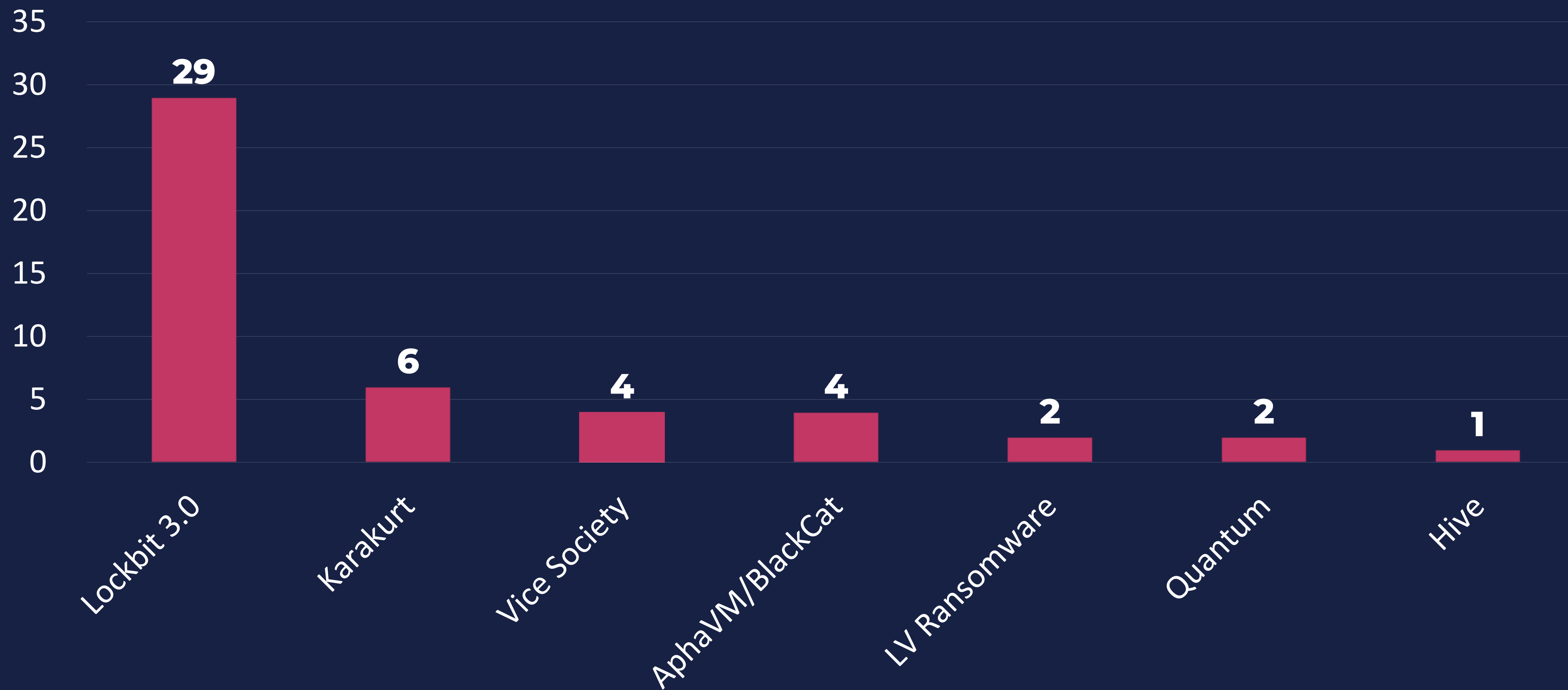
Who Has Been Targeted?

Victim Countries;

- **Australia**
- **Canada**
- **United Kingdom**
- **United States of America**
- **Germany**
- **Egypt**
- **United Arab Emirates**
- **India**
- **South Africa**
- **Spain**
- **China**
- **Italy**
- **Japan**
- **France**
- **Thailand**
- **Netherlands**
- **Ecuador**
- **Argentina**
- **Taiwan**
- **Brazil**



Ransomware Group Statistics



Numbers of The Week



Targeted Companies

Company	Website
COS2000	cos.net.au
Reed Pope Law	reedpope.ca
Nelsons Law	nelsonslaw.co.uk
Continental Management	continentalmgt.com
Handler Bau GmbH	handler-group.com
Spinneys	spinneys.com
Site Technology	site-technology.com
Federal Bank	federalbank.co.in
LaVan & Neidenberg	disabilityhelpgroup.com
Ares Foods	aresfoods.ca
Integrate	integrate.ch
BizFrames's Enterprise Platform	bizframe.co.za
Riken Corporation	riken.co.jp
Columbia Grain	columbiagrain.com
Farma Office	fedefarma.com
CPIC	cpicfiber.com
Novita Rovagnati	rovagnati.it
Clestra Hauserman	clestra.com
Redox Brands	crbrandsinc.com
Cristina Spine Center	christianaspinecenter.com
A2 Pas	a2-pas.fr
CoastalMed Pharmacy	coastalmedps.com
Zulian	zulia.co.th
AddConsult	addconsult.nl
La Competencia	competencia.com.ec
Lexington National	lexingtonnational.com
Mack Enegy	mec.com
MWD	mwd.digital
Yong Mao Environmental Tech	

Targeted Companies

Company	Website
OCREX	ocrex.com
Bizerba	bizerba.com
The Town of St. Maries	townofstmarys.com
Normandise Petfood	lanormandise.fr
Lane Print	laneprint.com.au
Taylor Stafford	taylorstafford.com
Dayton Superior	daytonsuperior.com
OSDE	osde.com.ar
Roedean School	roedeanschool.co.za
Saudi Printing & Packaging	sppc.com.sa
Wärtsilä Corporation	wartsila.com
Delon Hampton & Associates	delonhampton.com
Broshuis Driving innovation	broshuis.com
Gensco	gensco.com
The Crum & Forster	fairfax.ca
CHDE POLSKA	eden-field.com.au
Edenfield	field.com.au
San Luis Coastal Unified School District	slcusd.org
XQUADRAT GmbH	xquadrat.ag
Metropolitan Associates	metapts.com
Solví Group	solvi.com
Turnberry Associates	turnberry.com
Sappi	sappi.com
Tom Barrow	tombarrow.com
Eka	eka1.com



Groups and Attacks



Weekly Ransomware Group Activity Report

•
•
•

Ransomware Group Activities: Black Basta

COS2000

COS is Australia's largest family owned and operated office products supplier. We have been in operation for over 45 years, with over 500 employees delivering thousands of products to businesses across Australia every day. We have invested heavily in creating a nation-wide presence, with an extensive network of sales offices, warehouses and distribution centres across Australia. Each branch is tailored to local requirements and delivers a local service experience. With

Published
0%


Visits
169

Read more

COS2000 Attack

...

Ransomware Group Activities: AlphaVM/Black Cat



Reed Pope Law
Tue Jul 19 2022
ALL DATA AVAILABLE FOR
DOWNLOADING!!!

Attachments — 5
Uploads — 2

Read more

Reed Pope Law Attack




Nelsonslaw LLP
Tue Jul 19 2022
Nelsons was formed in 1983 by Tim Hastings and two other solicitors in a small Nottingham office. Since then we have grown to become one of the leading law firms in the East Midlands with offices in Derby, Leicester and

Attachments — 5

Read more

Nelsons Law Attack



Continental Management
Tue Jul 19 2022
ALL DATA AVAILABLE FOR
DOWNLOADING!!!

Attachments — 6
Uploads — 3

Read more

Continental Management Attack



HANDLER Bau GmbH
Wed Jul 20 2022
Address: Walter Handler-Straße 1, 2853
Leitenviertel, Austria

Attachments — 2

Read more

Handler Bau GmbH Attack

Ransomware Group Activities: CLOP

[SPINNEYS.COM](https://spinneys.com)

Headquarters:

PO Box 9, Cairo, Cairo, Egypt

Phone:

+20 2 25163780

Website:


www.spinneys.com

Revenue:

\$283 Million

Spinneys Attack

Ransomware Group Activities: CUBA Ransomware



SITE TECHNOLOGY

More than 1000 employees in Abu Dhabi, Dubai, Riyadh, Jeddah, Khobar, Doha, Baghdad and Beirut

Driven by a common Vision, sharing common Values and inspired by a spirit of innovation, our people are still displaying unwavering dedication to put the Group at the forefront of the turnkey solution providers and maintain a leadership position. Site Technology is a supplier, system integrator, and a contractor, with a range of services that covers the design, procurement, installation, commissioning, operation and maintenance of new systems along with the upgrade, support and management of existing systems in different activity sectors:

- Technology
- Power
- Contracting
- Power Generation

After 26 years of operations, the group has more than 1000 employees operating in 8 different locations:
Abu Dhabi / Dubai/ Riyadh/ Jeddah/ Khobar/ Doha/ Beirut/ Baghdad

Combining this vast spectrum of efficacies with a highly trained team of specialists, we are able to offer system based turnkey solutions that are performance driven, cost-effective and remarkably straightforward. It is this signature quality that has consistently distinguished our services and garnered our clients' professional trust.

Site Technology has 12 business activities:

- 1- ELV & Integrated Security Systems
- 2- Network Integration Systems
- 3- Biometrics Systems
- 4- Audiovisual Systems
- 5- UPS Systems
- 6- Data Center
- 7- Power Production & Conversion
- 8- Infrastructure Contracting
- 9- General Contracting
- 10- Renewable Energy
- 11- Fossil Energy
- 12- Recoverable Energies

Date the files were received: 19 July 2022

website: <https://www.site-technology.com>

files: Financial documents, correspondence with bank employees, account movements, balance sheets, tax documents, compensation, source code.

Site Technology Attack

Ransomware Group Activities: Everest Ransom Team

FederalBank / Fedfina

The company has 48 hours to contact us

Otherwise, 1130 GB of internal data will be published and decryption key will be deleted

Data includes

Financial documents(loans,budgets,....)

Internal correspondence

KYC data

Personal data and documents of employees

Clients personal data and documents including balances and debts

Personal data and documents of management and directors

File tree below: <https://dropmefiles.com/pZ5vU>

Federal Bank Attack

Ransomware Group Activities: Hive

LaVan & Neidenberg

Website

disabilityhelpgroup.com

Revenue

\$10M

Encrypted at

16

June 2022

13:45:30

Disclosed at

20 July 2022

13:16:00

Share

f

Disclosed Links

1 link

LaVan & Neidenberg Attack

TLP: White – Report Number : HRSSIR25072022

15

Digital Risk Protection Service – brandefense.io

Ransomware Group Activities: LockBit 3.0

<div>aresfoods.ca</div> <div>3D 21h 18m 06s\$ 90000</div> <div>Founded by the Christopoulos family in 1999, Ares Foods started out in a small butcher shop on Bernard Avenue in the Mile-End. From its humble beginning, the</div> <div>Updated: 20 Jul, 2022, 09:25 UTC953</div> <div>Ares Foods Attack</div>	<div>integrate.ch</div> <div>22h 34m 47s</div> <div>INTEGRATE means integrate, integrate and combine. This is exactly what we have been doing since the company was founded in 1996. We are a reliable partner with</div> <div>Updated: 21 Jul, 2022, 08:53 UTC987</div> <div>Integrate Attack</div>	<div>bizframe.co.za</div> <div>4D 15h 06m 27s\$ 70000</div> <div>BizFrame's Enterprise Platform as a Service (PaaS) enables companies to quickly develop, run and manage any web-based business application without the traditional</div> <div>Updated: 21 Jul, 2022, 11:15 UTC977</div> <div>BizFrames's Enterprise Platform Attack</div>	<div>riken.co.jp</div> <div>11D 01h 33m 42s\$ 348034</div> <div>RIKEN CORPORATION: Manufacturer of functional parts for automotive and industrial machinery.</div> <div>Updated: 24 Jul, 2022, 14:48 UTC231</div> <div>Riken Corporation Attack</div>
<div>columbiagrain.com</div> <div>9D 23h 44m 55s\$ 6653514</div> <div>We value every member of the Columbia Grain team who demonstrate daily our core values of innovation, reliability, respect, and have the dedication to work hard to cultivate</div> <div>Updated: 19 Jul, 2022, 18:15 UTC1049</div> <div>Columbia Grain Attack</div>	<div>fedefarma.com</div> <div>10D 13h 49m 22s</div> <div>Farmaoffice go, digitaliza tu farmacia con un clic Hacer realidad el reto de digitalizar tu farmacia es posible. Desde fede farma te ayudamos a conseguir facilitándote una web</div> <div>Updated: 19 Jul, 2022, 12:06 UTC776</div> <div>Farma Office Attack</div>	<div>cpicfiber.com</div> <div>10D 07h 54m 50s\$ 7654109</div> <div>CPIC is the first manufacturer to produce E-glass fiber by the direct-melt process in China, in year of 1986.</div> <div>Updated: 19 Jul, 2022, 18:09 UTC902</div> <div>CPIC Attack</div>	<div>rovagnati.it</div> <div>11D 07h 01m 19s\$ 2654498</div> <div>Novità Rovagnati, un "dominio" internazionale Nasce il sito Rovagnati.com, una piattaforma in lingua inglese che parla dell'azienda a tutto il mondo. Scopri di più</div> <div>Updated: 19 Jul, 2022, 18:03 UTC1222</div> <div>Novita Rovagnati Attack</div>

Ransomware Group Activities: LockBit 3.0

<div> <div>clestra.com</div> <div>10D 13h 06m 56s \$ 150 000</div> <div>Clestra Hauserman is the result of a powerful story written by the energy of successive generations of passionate men and women. It is the story of Clestra</div> <div>Updated: 19 Jul, 2022, 18:05 UTC 914</div> </div> <div>Clestra Hauserman Attack</div>	<div> <div>crbrandsinc.com</div> <div>12D 03h 10m 57s</div> <div>Redox Brands was a marketing company formed in 2000 by Todd Wichmann and Richard Owen, former executives with the multinational consumer products firm</div> <div>Updated: 19 Jul, 2022, 18:10 UTC 833</div> </div> <div>Redox Brands Attack</div>	<div> <div>cristianaspinecenter.com</div> <div>11D 05h 13m 57s</div> <div>Christiana Spine Center is the only practice in the region dedicated specifically to taking care of patients with spinal disorders. We are able to provide superior care by having</div> <div>Updated: 19 Jul, 2022, 18:06 UTC 864</div> </div> <div>Cristina Spine Center Attack</div>	<div> <div>a2-pas.fr</div> <div>00h 18m 01s \$ 50 000</div> <div>Upload about of 20Gb private clients data exclusive information about their clients and companies and more passports scans cofidal.fr kadim-invest.fr abel-</div> <div>Updated: 19 Jul, 2022, 12:37 UTC 397</div> </div> <div>A2 Pas Attack</div>
<div> <div>coastalmedps.com</div> <div>3D 22h 36m 50s \$ 90 000</div> <div>Emphasis on Service Medchoice provides exceptional service with our qualified staff and streamlined ordering processes. At Medchoice, only licensed pharmacists enter</div> <div>Updated: 21 Jul, 2022, 10:14 UTC 592</div> </div> <div>CoastalMed Pharmacy Attack</div>	<div> <div>zhulian.co.th</div> <div>4D 01h 05m 48s</div> <div>About us: The date of establishment of the company - Zulian (Thailand) Co., Ltd. was founded on June 14, 1996 with an authorized capital of 10,000,000 baht for the</div> <div>Updated: 22 Jul, 2022, 09:25 UTC 147</div> </div> <div>Zulian Attack</div>	<div> <div>addconsult.nl</div> <div>3D 03h 14m 49s \$ 50 000</div> <div>Stolen data: bank documents, customer data, financial documents. About company: Service, quality, inlevingsvermogen and pragmatic aanpak to belangrijke</div> <div>Updated: 21 Jul, 2022, 09:29 UTC 604</div> </div> <div>AddConsult Attack</div>	<div> <div>competencia.com.ec</div> <div>3D 23h 26m 53s \$ 70 000</div> <div>About: La Competencia S.A. inicia en 1963, durante su tiempo de vida se ha dedicado a la importación, venta y distribution de distintos productos innovadores, las</div> <div>Updated: 21 Jul, 2022, 08:59 UTC 615</div> </div> <div>La Competencia Attack</div>

Ransomware Group Activities: LockBit 3.0

<div><div>lexingtonnational.com</div><div>6D 20h 54m 26s\$ 200000</div><div>Lexington National Insurance Corporation is a national property and casualty insurance company rated A- by A.M. Best and U.S. Treasury listed. Lexington National</div><div>Updated: 20 Jul, 2022, 21:21 UTC473</div></div> <div>Lexington National Attack</div>	<div><div>mec.com</div><div>11D 05h 56m 17s\$ 300000</div><div>Mack Energy Corporation was founded by Mack.C..Chase, President, in 1990. It was formed as an independent energy company engaged in the exploration, development,</div><div>Updated: 20 Jul, 2022, 21:24 UTC511</div></div> <div>Mack Enegy Attack</div>	<div><div>mwd.digital</div><div>2D 02h 06m 51s\$ 80000</div><div>It is the set of specialized skills in Data Management, Digital Strategy, Security, Application Development, Hosting, Social Media & Content Management, Digital ADV.</div><div>Updated: 21 Jul, 2022, 10:35 UTC453</div></div> <div>MWD Attack</div>	<div><div>Yong Mao Environmental Tech. Co.,Ltd</div><div>6D 10h 03m 03s\$ 80000</div><div>Yun Mao Ecological technology. Design Co., Ltd was approved in 2015 and has been in the construction industry ever since. Cooperate with many big companies in</div><div>Updated: 22 Jul, 2022, 18:00 UTC89</div></div> <div>Yong Mao Environmental Tech Attack</div>
<div><div>ocrex.com</div><div>4D 23h 25m 29s\$ 80000</div><div>OCREX was formed in 2009 and specialises in the development of OCR software solutions. OCREX has developed AutoRec which automates the process of performing</div><div>Updated: 21 Jul, 2022, 15:34 UTC401</div></div> <div>OCREX Attack</div>	<div><div>bizebra.com</div><div>5D 02h 57m 25s</div><div>Bizerba SE & Co. KG is a German provider of weighing and slicing technologies for industry and trade and is a worldwide leading specialist in industrial weighing and</div><div>Updated: 22 Jul, 2022, 04:26 UTC471</div></div> <div>Bizerba Attack</div>	<div><div>townofstmarys.com</div><div>7D 05h 15m 35s</div><div>The Town of St. Marys is located at the junction of the Thames River and Trout Creek, southwest of Stratford in southwestern Ontario. Rich in natural</div><div>Updated: 23 Jul, 2022, 00:01 UTC221</div></div> <div>The Town of St. Maries Attack</div>	<div><div>lanormandise.fr</div><div>9D 06h 36m 29s\$ 150000</div><div>Normandise Petfood is a manufacturing and packaging plant specializing in the custom manufacturing of high-quality food products.</div><div>Updated: 22 Jul, 2022, 19:06 UTC106</div></div> <div>Normandise Petfood Attack</div>

Ransomware Group Activities: LockBit 3.0

laneprint.com.au

11D 18h 34m 00s
\$ 85000

We have been providing print and mail services across Australia for almost 50 years, so we know how to do it exceptionally well. We are the preferred supplier of

Updated: 22 Jul, 2022, 19:04 UTC
105

Lane Print Attack

taylorstafford.com

10D 00h 32m 52s
\$ 80000

taylorstafford.com We provide a broad range of legal services for businesses, insurance companies, and their insureds in all types of civil litigation, from medical

Updated: 22 Jul, 2022, 17:03 UTC
151

Taylor Stafford Attack

daytonsuperior.com

6D 09h 04m 07s
\$ 590000

Updated: 24 Jul, 2022, 14:12 UTC
134

Dayton Superior Attack

osde.com.ar

13D 14h 05m 52s
\$ 300000

OSDE is a network of medical care services in Argentina created in 1972. 2 In 1991 it became the first network of medical-care services in Argentina , with a system of open

Updated: 23 Jul, 2022, 06:28 UTC
164

OSDE Attack

roedeanschool.co.za

6D 20h 30m 10s

Stolen: passports, finances, personal photos, documents and more Roedean School was founded in 1885 to provide 'a thorough physical, intellectual and moral'

Updated: 23 Jul, 2022, 07:01 UTC
43

Roedean School Attack

Ransomware Group Activities: LV Ransomware

SPPC.COM.SA - HACKED AND MORE THEN 900GB DATA LEAKED

publication at 22.07.22 23:00 GMT

Saudi Printing & Packaging

Headquarters Headquarters: Nakheel Tower- King Fahad Rd, Riyadh, Ar Riyad, Saudi Arabia
Phone Number Phone Number: +966 9200 15665
Website Website: www.sppc.com.sa
Revenue Revenue: \$197 Million
Stock Symbol Stock Symbol: 4270

If we don't come to a contract and payment, all of your information will be published in the public domain.

This blog will be supplemented with your private documents before publication, as well as all information from your data in the absence of dialogue, will be used against your customers and partners.

Saudi Printing & Packaging Attack

WARTSILA.COM - HACKED AND MORE THEN 2000 GB DATA LEAKED

publication at 22.07.22 23:00 GMT



Wärtsilä Corporation (Wärtsilä Oyj Abp)

Who is Wärtsilä Corporation

Wärtsilä is one of the largest manufacturers of machinery and electrical equipment for the marine and energy markets worldwide.

The company has more than 18 000 employees working in 200 offices in 80 countries. The main sales markets are in Europe, Asia, Africa, North and South America. The company is included in the rating of the most socially responsible corporations in the world "2018 Global 100".

Wärtsilä Corporation Attack

Ransomware Group Activities: Quantum



117GB

2022-07-18


Broshuis | Driving innovation

Broshuis B.V. is a 100% family owned, Dutch company and one of the largest specialty trailer manufacturers in Europe.

READ MORE

5.8K 

Broshuis | Driving innovation Attack




817GB

2022-07-19

Delon Hampton & Associates, Chartered

In January 1973, Delon Hampton and Associates, Chartered was founded with the sole objective of creating a world-class engineering consulting firm specializing

READ MORE

5.5K 

Delon Hampton & Associates Attack

Ransomware Group Activities: Ragnar Locker

Gensco Inc



Gensco, founded in 1947 and headquartered in Tacoma, Washington, is a wholesale distributor of HVAC supplies and equipment






Headquarters: 4402 20th St E, Tacoma, Washington, 98424, United States

Phone Number: (253) 620-8203

Website: www.gensco.com

Gensco Attack

Ransomware Group Activities: Ransom House

<h2>Fairfax - Crum & Forster</h2> <p>The Crum & Forster companies are wholly owned subsidiaries of Crum & Forster Holdings Corp., which is a wholly owned subsidiary of Fairfax Financial Holdings Limited. Fairfax Financial Holdings Limited is a financial services holding company whose corporate objective is to achieve a high rate of return on invested capital and build long-term shareholder value.</p>	<div>  <div> <div>Encrypted</div> <div>20/03/2022</div> <div>Downloaded</div> <div>5Tb</div> </div> </div>	<div>Share</div> <div>   </div> <div>Contact us</div> <div>  </div>
<div> <div>Website</div> <div> https://www.cfins.com https://www.fairfax.ca </div> </div> <div> <div>Revenue Employees</div> <div> <div>\$2Billion</div> <div>2919</div> </div> </div>	<div>  <div> <div>Status:</div> <div>EVIDENCE</div> </div> </div> <div> <div>4016</div> <div>21/07/2022</div> </div>	
<div>Evidence packs:</div> <div>Download</div>	<div>Password:</div> <div>no password</div>	

The Crum & Forster Attack

Ransomware Group Activities: Vice Society

XQUADRAT GmbH
<http://www.xquadraLag/>
Germany

XQUADRAT stands for interior design from a single source. From creation to planning to realization, we provide our customers with all-round support. This way, you benefit from having only one contact person who covers the entire process for you. After all, that's what makes good service.

View documents >>

XQUADRAT GmbH Attack

San Luis Coastal Unified School District
<http://www.slcsd.org/>
United States

Small neighborhood schools are a hallmark of the District where students are educated from preschool through twelfth grade and a world-class adult school program offers unique, life-improving courses to thousands of community members.

View documents >>

San Luis Coastal Unified School District Attack

Edenfield
<http://www.eden-field.com.au/>
Australia

Our Management Team boasts decades of experience in running successful aged care facilities in South Australia. Our focus on having the right people, with the right skills and the right experience ensures that our residents receive the highest quality of care and a fulfilling and vibrant lifestyle.

View documents >>

Edenfield Attack

CHDE POLSKA
<http://www.eden-field.com.au/>
Poland

CHDE POLSKA is located in Rzeszow, podkarpackie, Poland and is part of the Drugs and Druggists Sundries Merchant Wholesalers Industry.

View documents >>

CHDE POLSKA Attack

Ransomware Group Activities: Karakurt



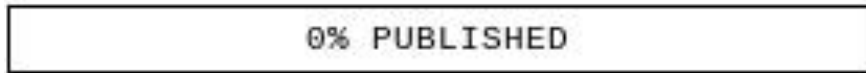
Metropolitan Associates

WEBSITE

REAL ESTATE

1123 N ASTOR ST, MILWAUKEE, WISCONSIN, 53202, UNIT...

Metropolitan Associates is a real estate company that specializes in property management and apartment living in Milwaukee & Madison



READ MORE

172

Metropolitan Associates Attack



Solví Group

WEBSITE

UTILITIES

AVENIDA GONÇALO MADEIRA, SUITE 400, SAO PAULO, BR...

Founded in 1997, Solvi offers solutions in waste, sanitation and energy recovery, operating and managing concessions and contracts for public and private customers



READ MORE

296

Solví Group Attack



Turnberry Associates

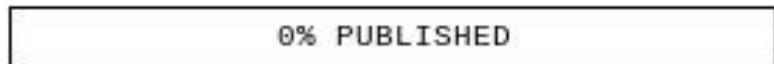
WEBSITE

REAL ESTATE

19501 BISCAYNE BLVD, STE 400, AVENTURA, FLORIDA, 33...

Founded in 1967 Turnberry Associates is real estate development and property management company headquartered in Aventura, Florida. In this release we will provide you with a lot of data (1tb) such as

EXPAND



READ MORE

141

Turnberry Associates Attack



Sappi

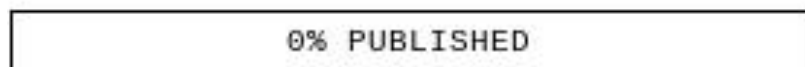
WEBSITE

MANUFACTURING

PO BOX 52264 SAXONWOLD JOHANNESBURG, 2132 SOUT...

Sappi Ltd produces and sells a variety of paper and paper-related products. The two categories of products are specialized cellulose and paper. Specialized cellulose, which is dissolved wood pulp, is u

EXPAND



READ MORE

412

Sappi Attack

Ransomware Group Activities: Karakurt



Tom Barrow

WEBSITE

MANUFACTURING

4131 OGEECHEE RD, STE 127, SAVANNAH, GEORGIA 31405...

Tom Barrow Company is a manufacturer's representative for commercial HVAC products. We carry a broad range of products manufactured by the finest brands in the HVAC business. With offices in Tennessee, EXPAND

0% PUBLISHED

READ MORE

49

Tom Barrow Attack



Eka(Business/Productivi...

WEBSITE

TECHNOLOGY

EMBASSY TECH VILLAGE SEZ, PHASE II, ASTER BUILDING ...

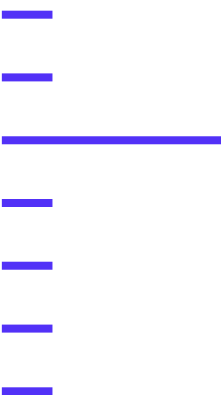
Developer of a digital commodity management platform designed to provide specialized tools for commodity trading and risk management. The company's platform provides cloud, blockchain, machine learning EXPAND

0% PUBLISHED

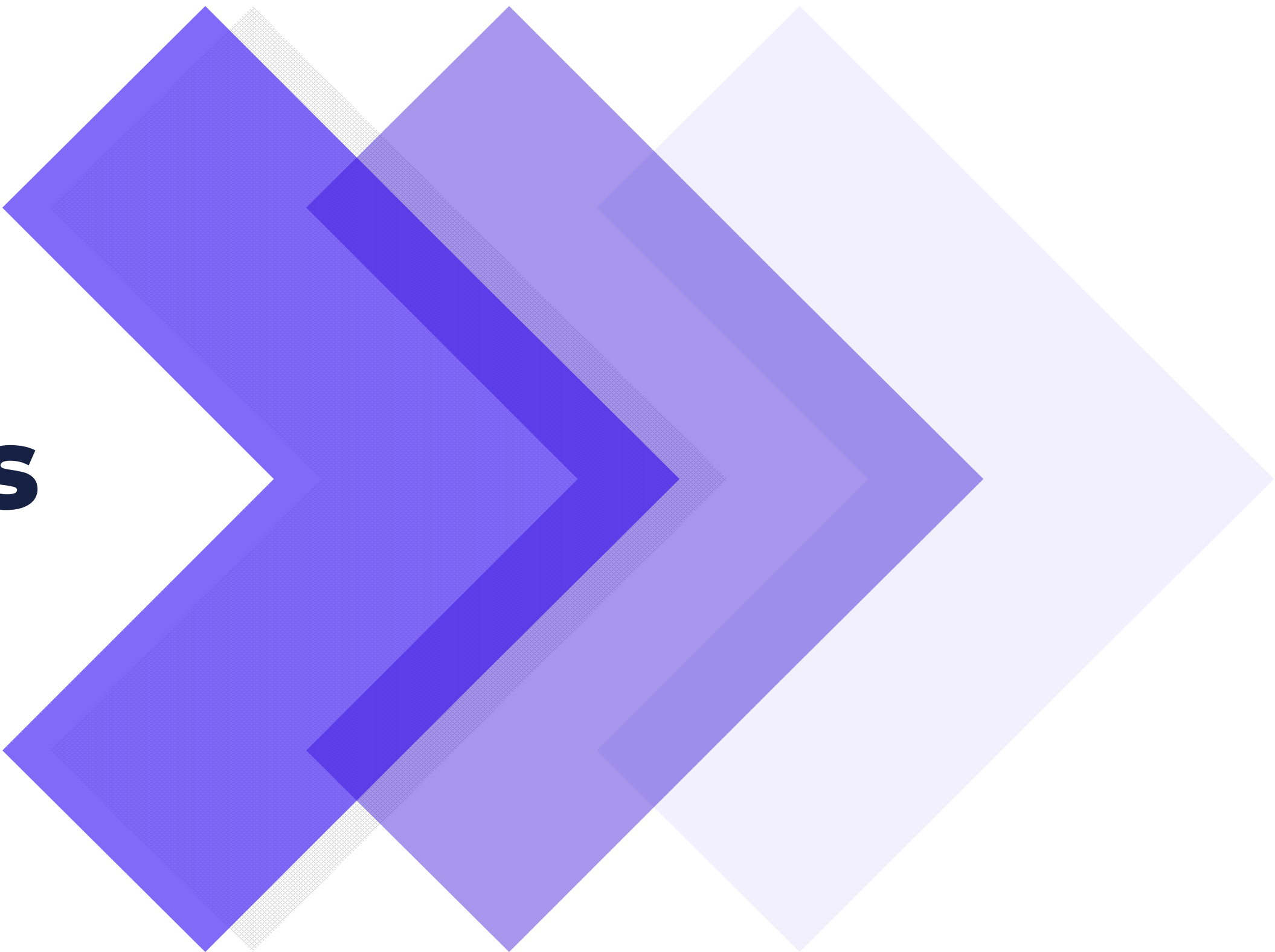
READ MORE

107

Eka Attack



Key Results



Weekly Ransomware Group Activity Report

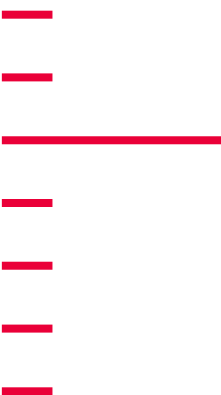
Key Results

The fact that cyber threats and awareness against the institutions are not adequately conveyed by employees of the institution gives opportunity for attackers to develop new methods and tools, who take advantage of the lack of training in terms of awareness.

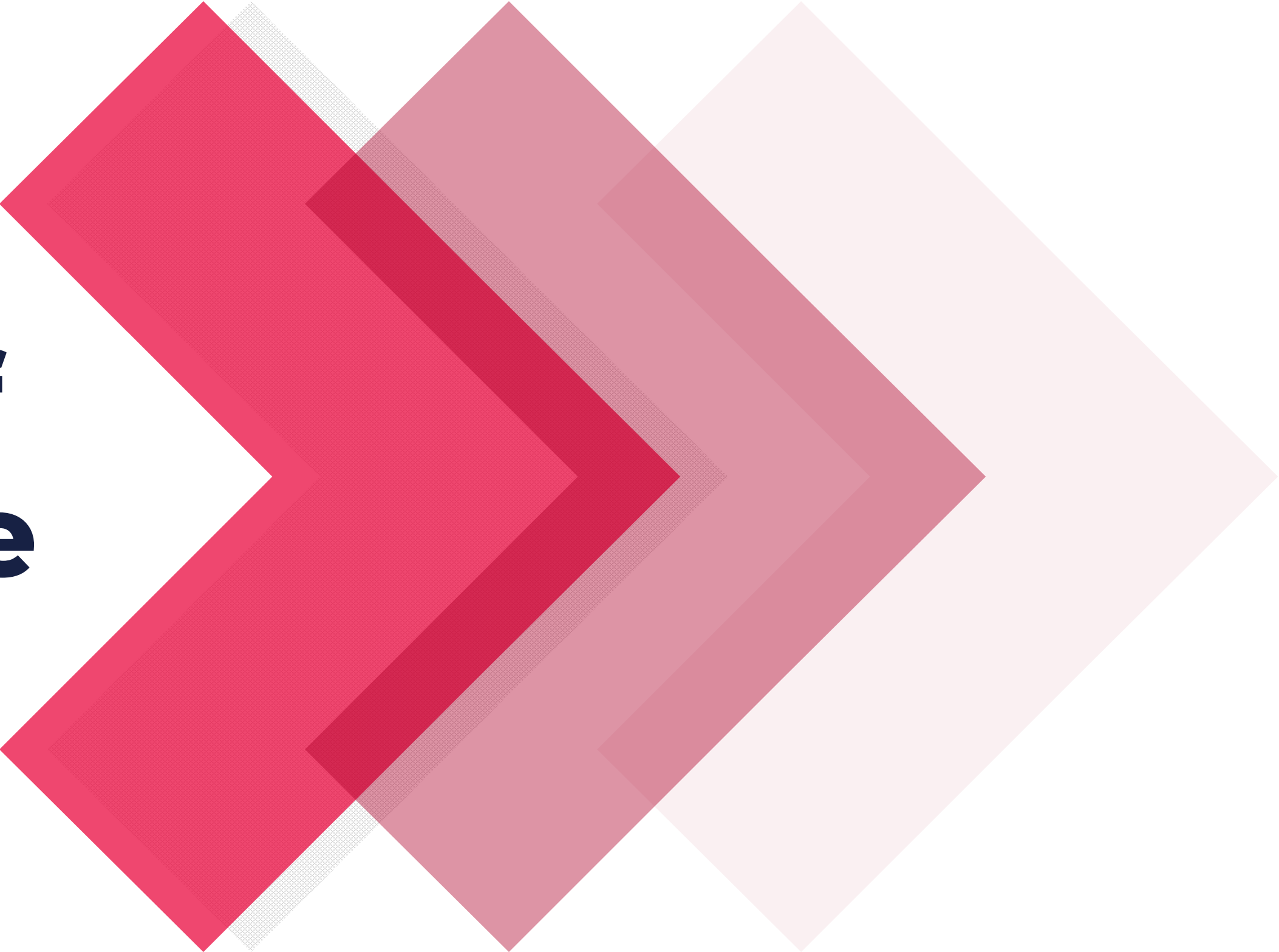
Although the existence of a wide variety of cyber threats and their increasing number are predictable and acceptable in the era of digitalization, rising ransomware threats threatens institutions more than other cyber threats and the rate of encounter is higher. The goal is to gain high profits by concentrating its scope on small audiences (institutions rather than multiple individual targets) and presenting ransomware threats with low rental fees on underground forums as a popular trend called Ransomware-as-a-Service. In this way, it is possible for people without technical knowledge to perform ransomware operations.

Remembering that you are always a potential target of ransomware, it is possible to prevent ransomware threats to your organization through simple precautions. Our recommendations for protecting your organization against ransomware attacks are listed below. However, it is necessary to take into account that the recommendations here are not sufficient for protection from Ransomware attacks, that attackers may have tools and methods that have not yet been revealed.

- ✓Provide regular training in order to raise awareness of cyber security among your employees,**
- ✓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,**
- ✓Behave suspiciously against e-mails of unknown origin and the file attachments they contain, if possible, do not open them,**
- ✓Use licensed and up-to-date operating systems,**
- ✓Use reliable anti-virus solutions,**
- ✓Block all IoC (Indicator of Compromise) findings in this report by security devices.**



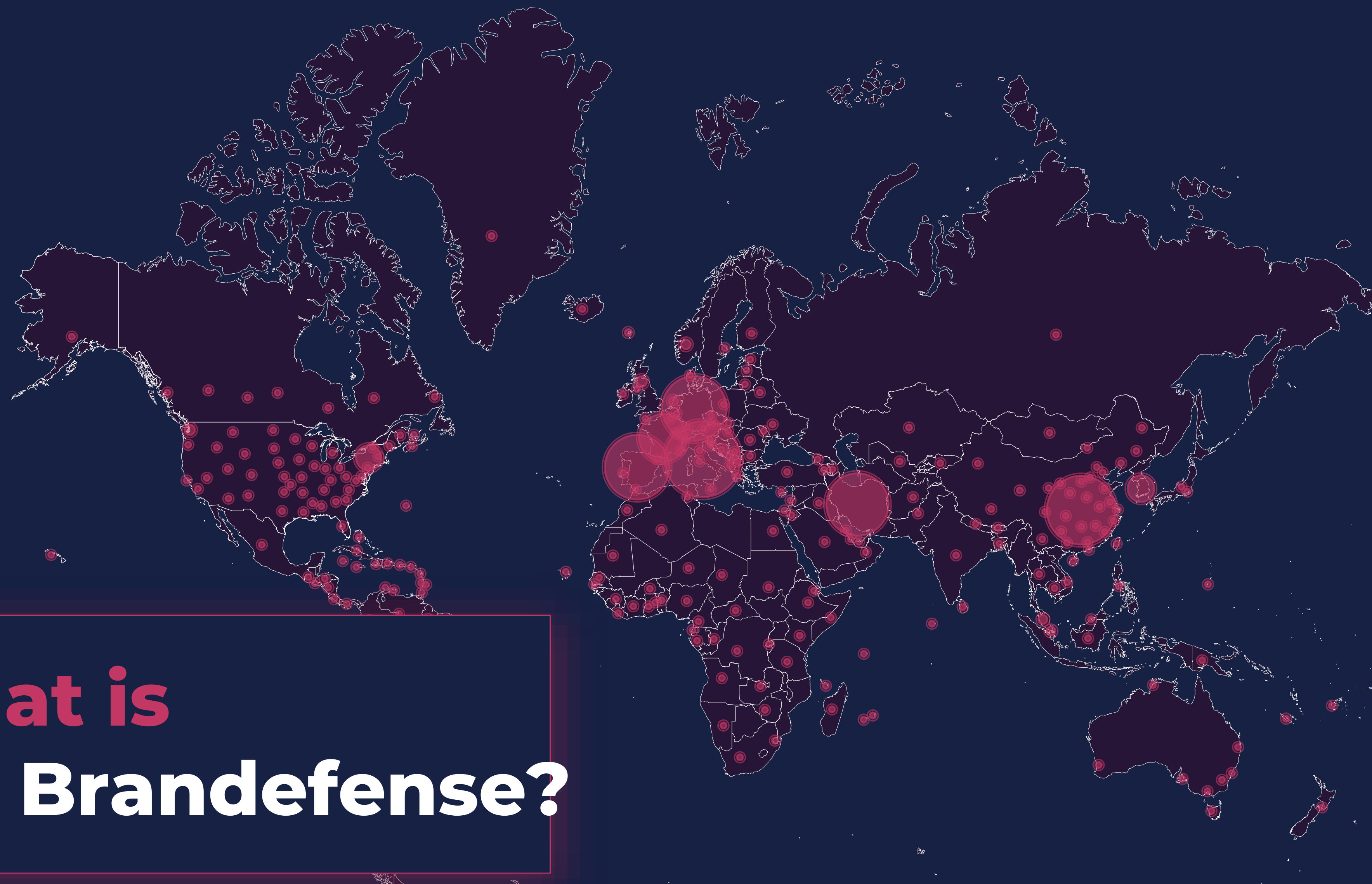
Indicator of Compromise



Weekly Ransomware Group Activity Report

Indicator of Compromises

FileHash-SHA256
6e07b835203ff9a7296200f08014321ba058284f0172d5a00f99a5fbd2e79df3
27bc983f99238813802cea064380d6832f631243cf581eeee4c5917a89f87373
1af1b092c81fd950eacc1caadedbb53b41c86de0a72945265c7f02e3d39154ab
611b1e1bf7590f0694d4c548f77967c46834e49a0a01c7e0de8ed5664e6faa32
c155c62f431a687c42824db7c9f4020006af909117ee66d1a276b16be96a18e8
c3f0bffffe865e3b8de9cb96dada72c743bec39626010d9ebe926c9d326b56fdc



What is the Brandefense?



Brandefense

Digital Risk Protection Service

It provides continuous and real-time **cyber intelligence** and **digital risk protection** service.

Furthermore, it makes **false-positive elimination** and tries to solve its clients' time/effort problems by utilizing machine learning and analyst powers to their full potential.

Brandefense provides **company-specific data leak intelligence** by constantly monitoring **hundreds of data sources** within the scope of threat intelligence, as well as automatic discovery of the company's internet-open **attack surface** and assessment of potential risks within the scope of attack surface analysis.

Product Features

BRAND & REPUTATION

- **Brand Monitoring**
- **Reputation Monitoring**
- **Data Breach Monitoring**
- **Phishing Monitoring**
- **Botnet Monitoring**
- **Hacked Sites Monitoring**
- **Takedown Service**

INTELLIGENCE

- **Threat Intelligence**
- **Vulnerability Intelligence**
- **Darkweb Intelligence**
- **Security News**
- **Sector Based Intelligence**
- **Custom APT Reports**
- **Malware Analysis Reports**
- **Fraud Protection Feeds**
- **Stolen Credit Card Feeds**
- **TTP Feeds**

EXPOSURE

- **Vulnerability Management**
- **Risk Monitoring**
- **Attack Surface Monitoring**
- **Digital Risk Scan**
- **Change Detections**
- **HSE Detections**
- **Uptime Monitoring**

TOOLS

- **Custom Investigation Tools**
- **Security Checks**
- **Botnet Lookup**
- **Email Breach Lookup**
- **DNS Lookup**
- **HTTP/HTTPs Lookup**



Find the perfect packages for you

You can create a custom Brandefense dashboard with our solutions you need and get an optimized price.

Protect your brand

Hackers can target your institution at any time. Brandefense can be your eyes and ears among hackers.

Integrate with your technologies

You can take more effective security measures by feeding your technologies false-positive free intelligence.

Start using right now

You can start using Brandefense instantly and receive both general and corporate threat intelligence data.

DEMO REQUEST / FREE TRIAL

brandefense.io / sales@brandefense.io