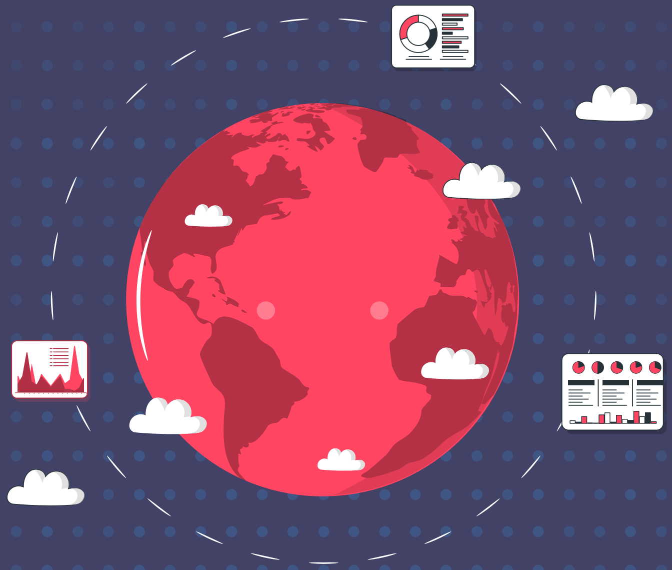


Country Threat Landscape Report

SOCRadar LABS mission is to inspire and enable the security community to identify threats before they turn info disruptive data breaches.

Belgium

Time Period: 2022/08/01 - 2023/08/01 | Report Date: 2022-08-01

SOCRadar®
Your Eyes Beyond

651 N Broad St, Suite 205
Middletown, DE 19709

☎ +1 (571) 249-4598

info@socradar.io

www.socradar.io

SOCRadar delivers intelligent digital risk protection platform against sophisticated cyber attacks for organizations of any size. Its portfolio of digital assets and perimeter monitoring platforms hardened with targeted threat intelligence — all automated and supported by a global team of qualified intelligence analysts — provides unparalleled visibility, management, and protection of digital risks. Prioritized, up-to-date, and relevant cyber threat insights empower customers to take action starting from the reconnaissance stage of the cyberattack life cycle.

Gartner Peer Insights™ 5/5 ★★★★★

Agenda

01 Dark Web Threats

02 Ransomware Threats

03 Top Target Industry

04 Stealer Logs

05 Phishing Threats

06 Threat Actors

©SOCRadar Cyber Intelligence Inc. All rights reserved.

48 Dark Web Threats in last one year.

Most Category are Selling and Sharing

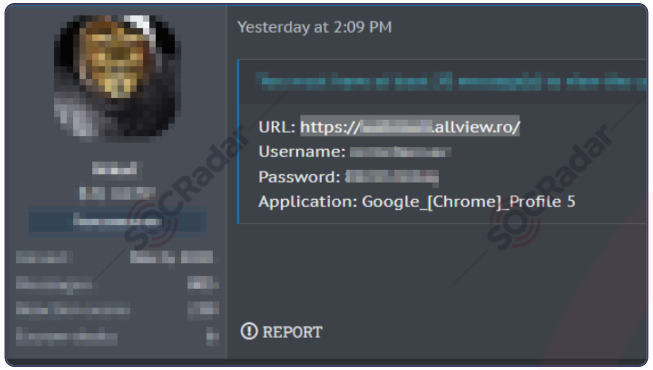
SOCRadar CTIA team has monitored the dark web to find trends and essential links. Throughout the this year, Belgium enterprises were bombarded with cyber attacks. Various threat actors have tried to sell and sometimes share the fruits of these successful cyberattacks on dark web hacker forums.

36 Dark web Threat Actors

- NikaC
- SPITZ
- FullzBazar
- opulent_accomplice
- Nimori

Classification [Confidential] Only For Designated Individuals
©SOCRadar Cyber Intelligence Inc. All rights reserved.

Dark Web Threats

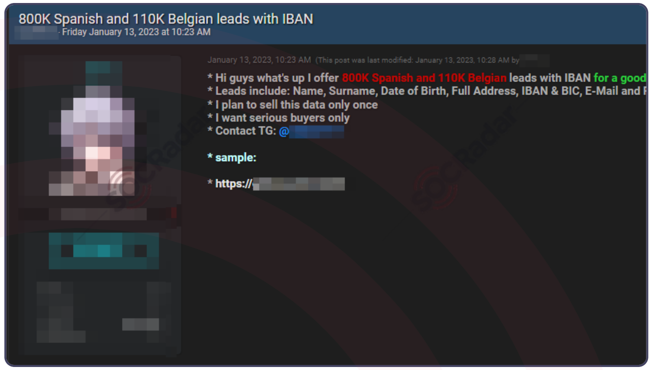


Yesterday at 2:09 PM

[redacted]

URL: https://[redacted]allview.ro/
Username: [redacted]
Password: [redacted]
Application: Google_[Chrome]_Profile 5

ⓘ REPORT



800K Spanish and 110K Belgian leads with IBAN
[redacted] · Friday January 13, 2023 at 10:23 AM

January 13, 2023, 10:23 AM (This post was last modified: January 13, 2023, 10:28 AM by [redacted]

* Hi guys what's up I offer 800K Spanish and 110K Belgian leads with IBAN for a good
* Leads include: Name, Surname, Date of Birth, Full Address, IBAN & BIC, E-Mail and
* I plan to sell this data only once
* I want serious buyers only
* Contact TG: @[redacted]

* sample:

* https://[redacted]

2023-01-23

Corporate Mails from Various Websites are Leaked

In a hacker forum monitored by SOCRadar, a new alleged corporate mail leak is detected for various websites.URL: https://****.allview.ro/Username: *******Password: *******Application: Google_[Chrome]_Profile 5URL: https://****.awedns.com:****/Usernam...

2023-01-13

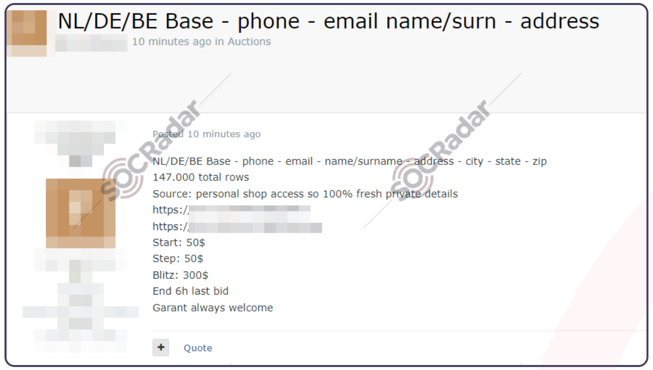
Leads Data of Spain and Belgium are on Sale

In a hacker forum monitored by SOCRadar, a new alleged leads data sale is detected for Spain and Belgium.* Hi guys what's up I offer 800K Spanish and 110K Belgian leads with IBAN for a good price.* Leads include: Name, Surname, Date of Birth, Full Ad...

Classification [Confidential] Only For Designated Individuals

©SOCRadar Cyber Intelligence Inc. All rights reserved.

Dark Web Threats

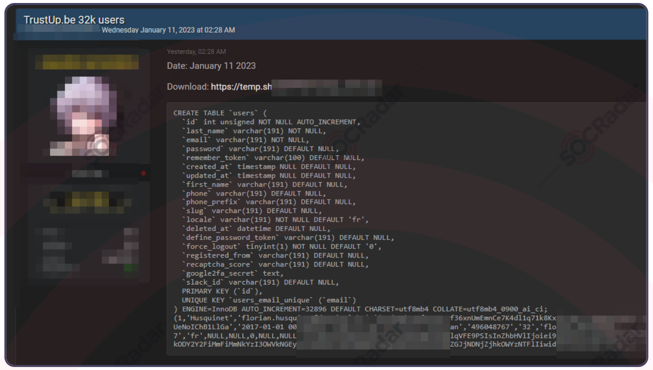


NL/DE/BE Base - phone - email name/surn - address

[redacted] 10 minutes ago in Auctions

Posted 10 minutes ago

NL/DE/BE Base - phone - email - name/surname - address - city - state - zip
147.000 total rows
Source: personal shop access so 100% fresh private details
https:/[redacted]
https:/[redacted]
Start: 50$
Step: 50$
Blitz: 300$
End 6h last bid
Garant always welcome



TrustUp.be 32k users

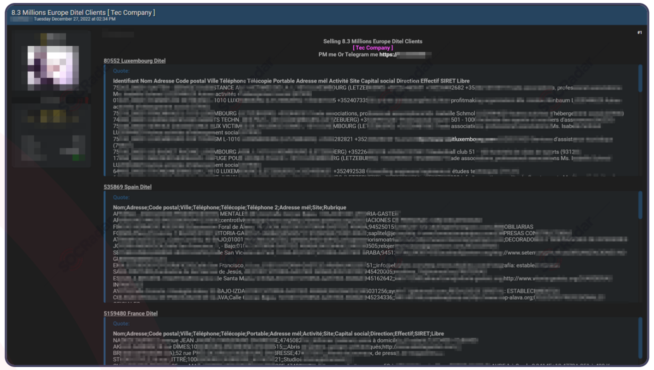
[redacted] · Wednesday January 11, 2023 at 02:28 AM

Yesterday, 02:28 AM

Date: January 11 2023

Download: https://temp.sh[redacted]

```
CREATE TABLE `users` (
  `id` int unsigned NOT NULL AUTO_INCREMENT,
  `last_name` varchar(191) NOT NULL,
  `email` varchar(191) NOT NULL,
  `password` varchar(191) DEFAULT NULL,
  `remember_token` varchar(100) DEFAULT NULL,
  `created_at` timestamp NULL DEFAULT NULL,
  `updated_at` timestamp NULL DEFAULT NULL,
  `first_name` varchar(191) DEFAULT NULL,
  `phone` varchar(191) DEFAULT NULL,
  `phone_prefix` varchar(191) DEFAULT NULL,
  `slug` varchar(191) DEFAULT NULL,
  `locale` varchar(191) NOT NULL DEFAULT 'fr',
  `deleted_at` datetime DEFAULT NULL,
  `define_password_token` varchar(191) DEFAULT NULL,
  `force_logout` tinyint(1) NOT NULL DEFAULT '0',
  `registered_from` varchar(191) DEFAULT NULL,
  `recaptcha_score` varchar(191) DEFAULT NULL,
  `google2fa_secret` text,
  `slack_id` varchar(191) DEFAULT NULL,
  PRIMARY KEY (`id`),
  UNIQUE KEY `users_email_unique` (`email`)
) ENGINE=InnoDB AUTO_INCREMENT=32896 DEFAULT CHARSET=utf8mb4 COLLATE=utf8mb4_0900_ai_ci;
(1,'Husquinet','florian.husqu[redacted]f36xnUmEmnCe7K4dl1q71k8Kx
UeNoIChB1LlGa','2017-01-01 00[redacted]an','496048767','32','flo
7','fr',NULL,NULL,0,NULL,NULL[redacted]lqVFE9PSIsInZhbHVlIjoiei9
kODY2Y2FiMmFiMmNkYzI3OWVkNGEy[redacted]ZGJjNDNjZjhkOWYzNTFlIiwid
```



8.3 Millions Europe Ditel Clients [Tec Company]

[redacted] Tuesday December 27, 2022 at 02:34 PM

#1

Selling 8.3 Millions Europe Ditel Clients
[Tec Company]
PM me Or Telegram me https://[redacted]

80552 Luxembourg Ditel

Quote:

Identifiant Nom Adresse Code postal Ville Téléphone Télécopie Portable Adresse mél Activité Site Capital social Direction Effectif SIRET Libre

[redacted]

535869 Spain Ditel

Quote:

Nom;Adresse;Code postal;Ville;Téléphone;Télécopie;Téléphone 2;Adresse mél;Site;Rubrique

[redacted]

5159480 France Ditel

Quote:

Nom;Adresse;Code postal;Ville;Téléphone;Télécopie;Portable;Adresse mél;Activité;Site;Capital social;Direction;Effectif;SIRET;Libre

[redacted]

2023-01-11

Database of Many Countries Cit...

In a hacker forum monitored by SO CRadar, a new alleged database sal e is detected for many countries citi zens.NL/DE/BE Base - phone - emai l - name/surname - address - city - s tate - zip147.000 total rowsSource: personal shop access so 100% fres h priva...

2023-01-11

Database of TrustUp is Leaked

In a hacker forum monitored by SO CRadar, a new alleged database lea k is detected for TrustUp.Date: Janu ary 11 2023Download: https://tem p.sh/*************CREATE TABLE ` users` (`id` int unsigned NOT NULL AUTO_INCREMENT, `last_name` va rchar(191) NOT ...

2022-12-27

Database of Ditel is on Sale

In a hacker forum monitored by SO CRadar, a new alleged database sal e is detected for Ditel.Selling 8.3 Mil lions Europe Ditel Clients[Tec Com pany]PM me Or Telegram me http s://**80552 Luxembourg DitelQuot e:Identifiant Nom Adresse Code pos tal Ville Té...

©SOCRadar Cyber Intelligence Inc. All rights reserved.

3 ransomware attacks in Belgium.

Ransomware attacks are among the most critical cyber attacks an organization can experience. The results can be destructive for an organization and lead to massive data loss and leaks of the victim company's sensitive data.

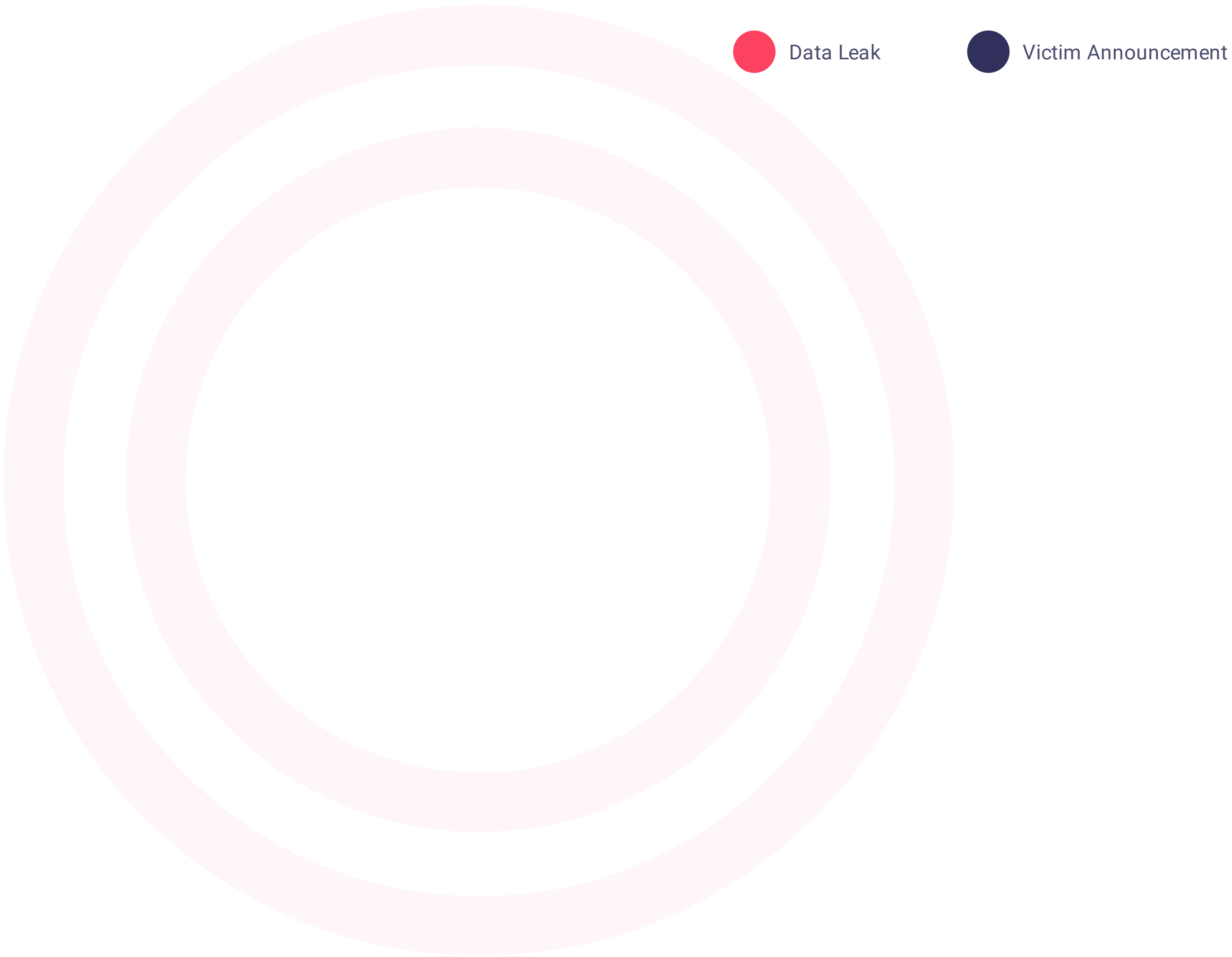
2 Ransomware Gangs

Lockbit 2.0

Conti

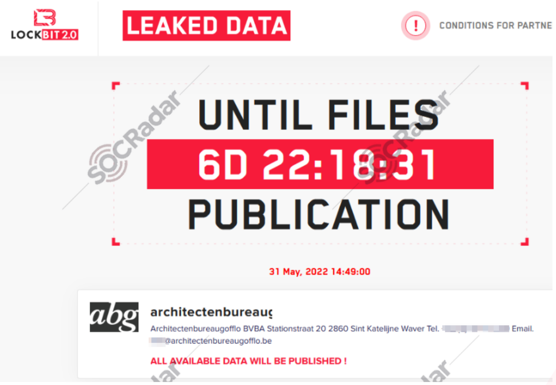
Classification [Confidential] Only For Designated Individuals
©SOCRadar Cyber Intelligence Inc. All rights reserved.

Ransomware Threats



©SOCRadar Cyber Intelligence Inc. All rights reserved.

Ransomware Threats



UNTIL FILES
6D 22:18:31
PUBLICATION

31 May, 2022 14:49:00

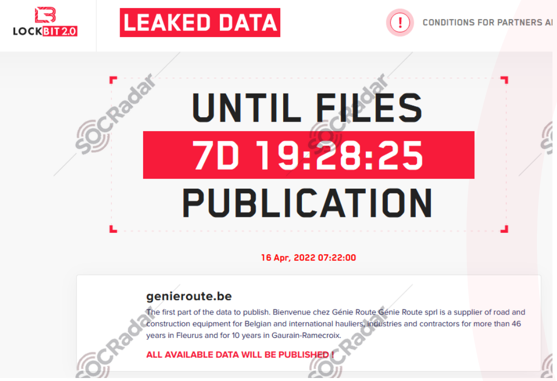
architectenbureauç

Architectenbureaugofflo BVBA Stationstraat 20 2860 Sint Katelijne Waver Tel. [redacted] Email. [redacted]@architectenbureaugofflo.be

ALL AVAILABLE DATA WILL BE PUBLISHED !

The New Ransomware Victim of Lockbit 2.0: Gofflo BVBA

In the Lockbit 2.0 ransomware group website monitored by SOCRadar, a new ransomware victim was allegedly announced as Gofflo BVBA.architectenbureaugofflo.beArchitectenbureaugofflo BVBA Stationstraat 20 2860 Sint Katelijne Waver Tel. ****** Email. ***...



UNTIL FILES
7D 19:28:25
PUBLICATION

16 Apr, 2022 07:22:00

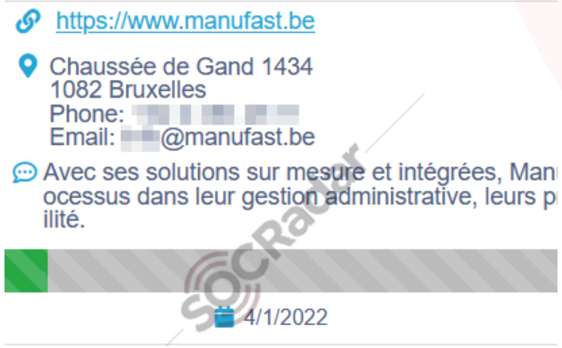
genieroute.be

The first part of the data to publish. Bienvenue chez Génie Route Génie Route sprl is a supplier of road and construction equipment for Belgian and international hauliers, industries and contractors for more than 46 years in Fleurus and for 10 years in Gaurain-Ramecroix.

ALL AVAILABLE DATA WILL BE PUBLISHED !

The New Ransomware Victim of Lockbit 2.0: Genie Route

In the Lockbit 2.0 ransomware group website monitored by SOCRadar, a new ransomware victim was allegedly announced as Genie Route.genieroute.beThe first part of the data to publish. Bienvenue chez Génie Route Génie Route sprl is a supplier of road an...



https://www.manufast.be

Chaussée de Gand 1434
1082 Bruxelles
Phone: [redacted]
Email: [redacted]@manufast.be

Avec ses solutions sur mesure et intégrées, Man
ocessus dans leur gestion administrative, leurs p
ilité.

4/1/2022

The New Ransomware Victim of Conti: Manufast

In the Conti ransomware group website monitored by SOCRadar, a new ransomware victim was allegedly announced as Manufast.“MANUFAST”https://www.manufast.be Chaussée de Gand 14341082 BruxellesPhone: *******Email: ***@manufast.be Avec ses solutions sur ...

©SOCRadar Cyber Intelligence Inc. All rights reserved.

Top Target Industry

59 Different industries targeted in Belgium

Dark Web Industry Threats

Ransomware Industry Threats

©SOCRadar Cyber Intelligence Inc. All rights reserved.

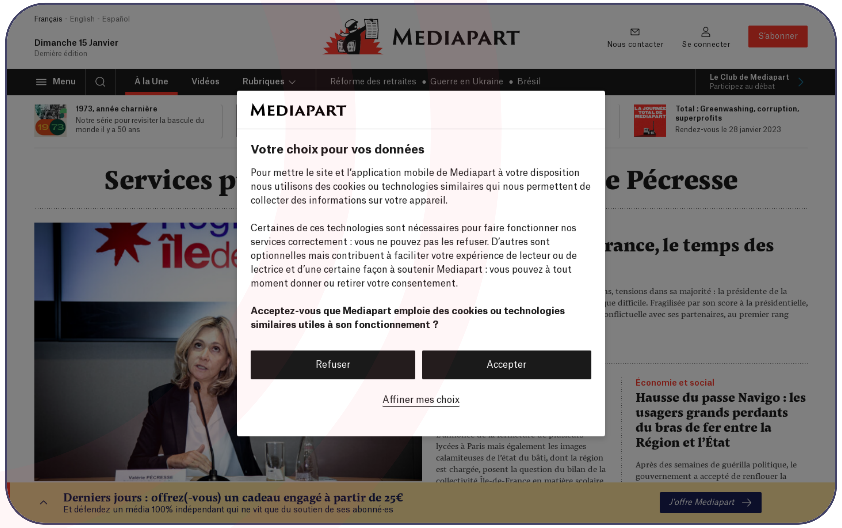
Phishing Threats

Brand impersonation takes place when a threat actor creates a social account pretending to be your brand. SOCRadar can spot fraudulent and fake domain. Also can spot fake social accounts by monitoring well-known social media platforms so that you can quickly take action to stop possible phishing scams.

Phishing Domain	Sector	Register Date
royalwebhosting.net		2023-01-24
digitalcreations.be		2023-01-20
acdecon.be		2023-01-15
acdecon.be		2023-01-15
acdecon.be		2023-01-15
acdecon.be		2023-01-15
acdecon.be		2023-01-14
[redacted]		2023-01-14
[redacted]		2023-01-14

+147 Phishing Threats

156 phishing domains detected in Belgium



Français - English - Español

Dimanche 15 Janvier
Dernière édition

MEDIAPART

Nous contacter | Se connecter | S'abonner

Menu | À la Une | Vidéos | Rubriques | Réforme des retraites • Guerre en Ukraine • Brésil | Le Club de Mediapart
Participez au débat

1973, année charnière
Notre série pour revisiter la bascule du monde il y a 50 ans

Total : Greenwashing, corruption, superprofits
Rendez-vous le 28 janvier 2023

Services p… e Pécresse

…rance, le temps des

…s, tensions dans sa majorité : la présidente de la …ue difficile. Fragilisée par son score à la présidentielle, …nflictuelle avec ses partenaires, au premier rang

MEDIAPART

Votre choix pour vos données

Pour mettre le site et l'application mobile de Mediapart à votre disposition nous utilisons des cookies ou technologies similaires qui nous permettent de collecter des informations sur votre appareil.

Certaines de ces technologies sont nécessaires pour faire fonctionner nos services correctement : vous ne pouvez pas les refuser. D'autres sont optionnelles mais contribuent à faciliter votre expérience de lecteur ou de lectrice et d'une certaine façon à soutenir Mediapart : vous pouvez à tout moment donner ou retirer votre consentement.

Acceptez-vous que Mediapart emploie des cookies ou technologies similaires utiles à son fonctionnement ?

Refuser | Accepter

Affiner mes choix

…lycées à Paris mais également les images calamiteuses de l'état du bâti, dont la région est chargée, posent la question du bilan de la collectivité Île-de-France en matière scolaire

Économie et social

Hausse du passe Navigo : les usagers grands perdants du bras de fer entre la Région et l'État

Après des semaines de guérilla politique, le gouvernement a accepté de renflouer la

Derniers jours : offrez(-vous) un cadeau engagé à partir de 25€
Et défendez un média 100% indépendant qui ne vit que du soutien de ses abonné·es

J'offre Mediapart

©SOCRadar Cyber Intelligence Inc. All rights reserved.

Stealer Logs

As one of the emerging underground market, threat actors are selling stolen identities from malware bot-infected devices frequently advertised as stealer logs. These bots-for-sale marketplaces affect not just users whose credentials and digital identities are stolen, but also the organizations that users are working for. SOCRadar provides you the continuous visibility to detect this evolving threat.

Related malware families

AZORult Trojan

The AZORult malware was first discovered in 2016 to be an information stealer that steals browsing history, cookies, ID/passwords, cryptocurrency information and more. It can also act as a downloader of other malware. It was sold on Russian underground forums to collect various types of sensitive information from an infected computer.

Raccoon Infostealer

Raccoon emerged as Malware as a Service (MaaS) in April 2019. The malware is capable of stealing login credentials, credit card information, cryptocurrency wallets, and browser information. Raccoon has basic infostealer functions but an aggressive marketing campaign and overall good user experience proved enough to make up for its lack of additional features.

1622 Stealer Logs in Belgium

Entity	Type	Date
https://t.me/+NshXICbUEZkxZDMy	url	2023-03-30
https://t.me/+NshXICbUEZkxZDMy	url	2023-03-30
https://t.me/+NshXICbUEZkxZDMy	url	2023-03-30
https://t.me/+NshXICbUEZkxZDMy	url	2023-03-30
https://auth.aftnet.be	url	2023-03-30
https://flightsim.to	url	2023-03-30
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

+1614 Stealer Logs

©SOCRadar Cyber Intelligence Inc. All rights reserved.

11 threat actors found in Belgium

Group Name	Aliases	Sectors
BRONZE SPRING	UNC302	Utilities , Chemical Manufacturing (Chemical &amp; Pharmaceutical Manufacturing) National Security and International Affairs ...
Inception Framework	ATK116 , OXYGEN , G0100 Clean Ursa ...	Utilities , National Security and International Affairs Transportation and Warehousing ...
Leviathan	APT40 , KRYPTONITE PANDA , Leviathan MUDCARP ...	Utilities , Justice, Public Order, and Safety Activities National Security and International Affairs ...
Lazarus Group	Operation GhostSecret , Hidden Cobra , WHOis Team Unit 121 ...	Space Research and Technology , Utilities Publishing Industries (except Internet) ...
Axiom	G0039 , BRONZE EXPORT , WICKED PANDA LEAD ...	Utilities , Chemical Manufacturing (Chemical &amp; Pharmaceutical Manufacturing) National Security and International Affairs ...
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]

+2 Threat Actors

Classification [Confidential] Only For Designated Individuals
©SOCRadar Cyber Intelligence Inc. All rights reserved.

Cyber Threat Intelligence for SOC Analysts

As an ‘Extension to SOC Teams’, CTI4SOC aims to provide you with actionable and contextualized TI with minimized false positives. A unique assistant to SOC teams with 12 functional modules.

Sign Up for Free CTI4SOC

Get Free CTI4SOC

SOCRadar®
Your Eyes Beyond

Trusted by world's leading organizations

Gartner Peer Insights™

5/5 ★★★★★