FORTINET | FortiRecon

Threat Intelligence Report

FortiGuard®
Threat Research

Navigating the Cyber Threat Landscape for Paris Olympics 2024

Summary:

The upcoming international sporting event, the 2024 Paris Olympic Games, is set to take place from July 26 to August 11, 2024. As one of the world's most prominent events, the Olympics have always been highly attractive targets for cybercriminals with different motivations. This year's events are also expected to face more threats due to their international significance. The event is highly susceptible to cyber attacks, including cyber espionage, disruptive and destructive operations, financially motivated activities, hacktivism, and information operations.

After the analyses of historical and ongoing cyber incidents associated with the Olympic events and French entities, FortiGuard Threat Research has prepared a comprehensive report on the potential threats and challenges to the Paris Olympics 2024. The report identifies a range of risks including cyber-attacks targeting critical infrastructure, event management systems, and personal data of athletes and attendees.

Historic threats observed include data breaches, espionage activities, and network access sales, posing severe risks to national security, economic stability, and public trust. The dark web and instant messaging platform Telegram offer stolen credentials, combo lists, phishing lures and exploit kits aimed at French entities. Additionally, we also observed that various hacktivist groups, such as Cyber Army Russia Reborn, NoName057(16), Garnesia Team, LulzSec, and Cyber Dragon, have explicitly declared their intent to target the Olympics and French entities. These groups are likely to employ tactics such as Distributed Denial of Service (DDoS) attacks, and website defacements.

The geopolitical landscape, especially France's stance on the Ukraine conflict and its role in international bodies like the EU and NATO, further exacerbates these threats. Political motivations include undermining France's support for Ukraine, leveraging the Olympics' visibility for propaganda, and challenging Western values. The report emphasizes the need for robust cybersecurity measures, including enhanced monitoring, incident response strategies, and public-private sector collaboration to safeguard the event from digital threats.

Content:

Overview of cyber threats to the Paris Olympics 2024

The Olympic Games, a premier international multi-sport event, have a rich history dating back to ancient Greece, with the modern iteration established in 1896. Held every four years, the Olympics bring together athletes from around the globe to compete in various sports. The games are divided into Summer and Winter Olympics, each featuring sports suited to their respective seasons. Over the years, the Olympics have grown in scope and scale, continually adapting to include new sports and technological advancements. The Olympics are a complex and multifaceted event, involving numerous stakeholders, including athletes, organizers, sponsors, and support services.

The upcoming Paris Olympics 2024, officially the Games of the XXXIII Olympiad, are set to take place from July 26 to August 11, 2024. This event marks the third time Paris will host the Olympics, coinciding with the centenary of the 1924 Games. The Paris Olympics will feature a mix of traditional and new sports, including surfing, skateboarding, sport climbing, and breaking, aimed at engaging younger audiences. According to the data, the Olympics will host athletes from 206 countries, while the Paralympics will feature participants from 184 countries. Additionally, Paris is expected to welcome over 15 million tourists during the Games.

The Paris Olympics 2024 faces a variety of cyber threats, reflecting the growing digitalization and interconnectedness of major international events. The following are some key cyber threats that could impact the Olympic Games, their partners, and France-based entities:

Threat Type Threats	Description	Impact

Espionage	Espionage Attacks	The espionage attacks often involve the theft of confidential information such as intellectual property, to gain strategic or competitive advantages and the disseminating of disinformation.	Increased risk of national security threats, and economic loss. These attacks could influence political decisions, and diplomatic relations and ultimately threaten the sovereignty and stability of targeted nations.
Darkweb	Data Breach and PII	Listings for the sale of French citizens' sensitive data and PII, often obtained from data breaches.	Increased risk of identity theft, phishing, financial fraud, proprietary information, and privacy violations.
	Network Access	Posts advertising access to the networks of French organizations, including governments, financial, healthcare, and critical infrastructure.	Unauthorized access to internal networks, potential for data theft, and operational disruptions.
	Sale of Stolen Credentials	Multiple forum posts offering stolen credentials could be used to gain unauthorized access to personal and organizational accounts.	Attackers can infiltrate systems, steal sensitive data, manipulate information, and conduct further attacks within compromised networks.
	Phishing Kits and Exploit Tools	Listings for phishing kits and exploit tools specifically targeting French users and organizations.	Increased risk of phishing attacks and exploitation of software vulnerabilities, leading to data breaches and unauthorized access.
	Combo Lists	Several listings on dark web forums and Telegram channels offer combo lists specifically targeting French citizens.	Increased risk of unauthorized access to accounts, leading to potential data breaches, financial fraud, and personal data theft. These lists compile credentials from various breaches and are sold for use in credential-stuffing attacks.
Hacktivist	DDoS attacks	Services offered to carry out DDoS attacks on French websites and online services.	Disruption of online services, including e-commerce, government portals, and media websites, leads to downtime and loss of accessibility.
	Website Defacements	Defacement attacks on French websites.	Damage to reputation and credibility, potential loss of trust from users, and disruption of website services.
Ransomware	Ransomware Attacks	Discussions and advertisements for ransomware campaigns aimed at French businesses and critical infrastructure.	Potential for significant operational disruptions, financial loss, and data encryption demanding ransom payments.

History of Cyber Attacks to Sports Events

Reports of cyberattacks on sports events have escalated dramatically over the past decade. In 10 years, the number of cyberattacks has increased 20-fold, rising from 212 million at the London 2012 Games to 4.4 billion at the Tokyo 2020 Games. These attacks often target financial gain or the acquisition of valuable data related to athletes, sponsors, or ticketing information. Targets have included individual teams like the San Francisco 49ers, streaming services like FuboTV during the World Cup, Major League Baseball, and soccer clubs such as Real Sociedad.

Targeted Country	Event	Year	Reference
USA	San Francisco 49ers (NFL)	Feb 2022	US National Football League (NFL) club the San Francisco 49ers confirmed it was hit by a ransomware attack one day before the Sunday Super Bowl.
	FuboTV (World Cup Streaming)	Nov 2022	Disrupted service for viewers during World Cup match
	Major League Baseball	2021 (Specific date unavailable)	Data breach of players and families through a third-party vendor
	National Basketball Association (NBA)	April 2021	NBA's Houston Rockets were targeted by ransomware attackers, who claimed to have stolen 500 gigabytes of Rockets' data.

Cyber espionage attacks on sports events also have a notable history, targeting the vast amount of sensitive data and the event's global IT infrastructure. Notable instances include the "Olympic Destroyer" malware attack during the PyeongChang 2018 Winter Olympics, which disrupted the opening ceremony's IT systems, and was linked to Russian hackers retaliating for the doping ban. Similarly, the Tokyo 2020 Olympics faced multiple cyber threats, including phishing and malware attacks, likely from state-sponsored actors in Russia.

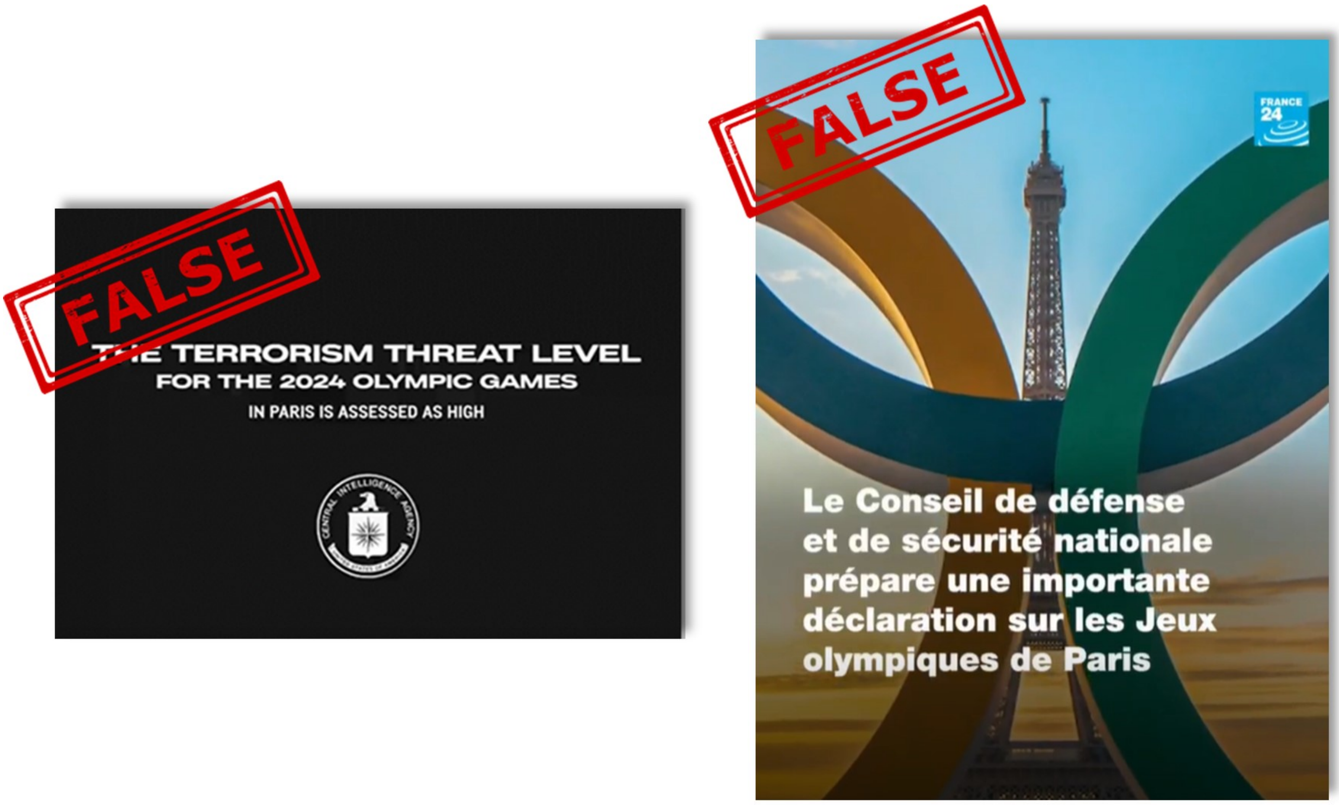
The following table provides an overview of significant cybersecurity incidents that have impacted the Olympic Games.

State Sponsered Country	Espionage Group	Targeted Olympic Games	Year	Reference
🇷🇺	Russian GRU, Lazarus Group	Tokyo Summer	2020	450 million cyberattacks attempted on Japan Olympics infrastructure
	Sandworm (APT44)	PyeongChang Winter	2018	Olympic Destroyer malware attack targeting the IT infrastructure, disrupting the opening ceremony.
	Fancy Bear (APT28)	Rio Summer	2016	Multiple cyber attacks, including data breaches and leaks of athletes' sensitive medical information.
🇨🇳	Chinese hacker groups (suspected state involvement)	Beijing Summer	2008	Cyber espionage activities aimed at stealing sensitive data related to the event's infrastructure and participating organizations.

According to the latest report, Russia has recently ramped up its disinformation campaigns targeting the 2024 Paris Olympics, focusing on defaming the International Olympic Committee (IOC) and creating fears of violence at the games using traditional tactics with the use of artificial intelligence (AI). Threat actors like Storm-1679 have released a film titled "Olympics Has Fallen," resembling a Hollywood thriller, to discredit the IOC. They've also spread fake videos suggesting terrorism risks in Paris and fabricated threats related to the Israel-Hamas conflict.

OLYMPICS
HAS FALLEN

(Russia-affiliated influence actor Storm-1679 using AI to target IOC)
(Image source: Microsoft)

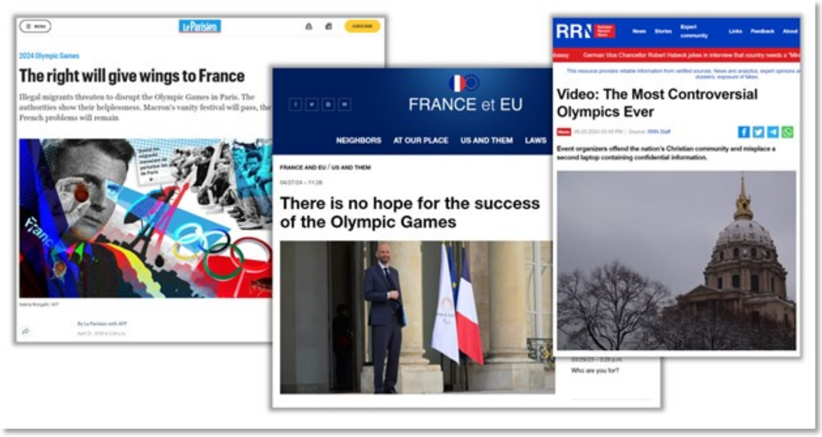


THE TERRORISM THREAT LEVEL FOR THE 2024 OLYMPIC GAMES IN PARIS IS ASSESSED AS HIGH

Le Conseil de défense et de sécurité nationale prépare une importante déclaration sur les Jeux olympiques de Paris

(Fake videos warning of terror threats at the 2024 Paris Summer Olympics, produced by Russia-linked actor Storm-1679)
(Image source: Microsoft)

Another threat actor, Storm-1099 also known as "Doppelganger", spreads anti-Olympics messages through fake news sites. These efforts may intensify as the Olympics approaches, potentially leveraging AI and social media bots to reach a broader audience.



The right will give wings to France

Illegal migrants threaten to disrupt the Olympic Games in Paris. The authorities show their helplessness. Macron's vanity festival will pass, the French problems will remain

There is no hope for the success of the Olympic Games

Video: The Most Controversial Olympics Ever

Event organizers offend the nation's Christian community and misplace a second laptop containing confidential information.

(Anti-Olympics messages being spread through fake news sites)
(Image source: Microsoft)

Cyber Threat Landscape for Paris Olympics 2024

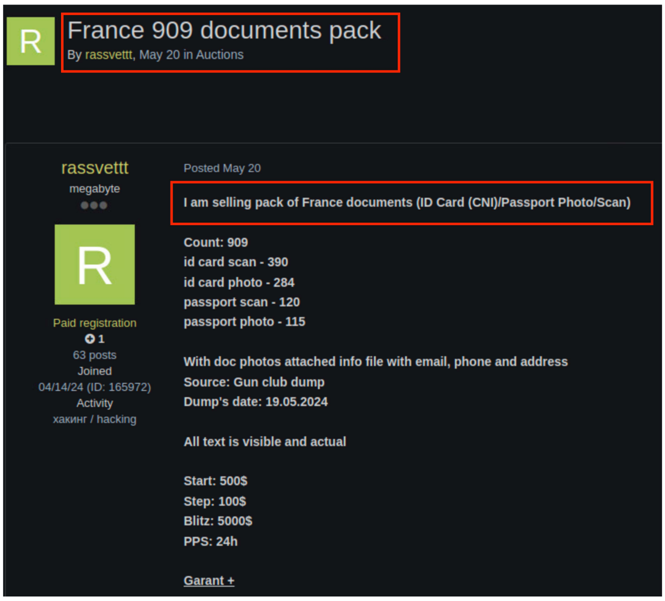
Darknet Threats

Darknet marketplaces play an important role in selling and advertising databases, personally identifiable information (PII), sensitive information, and network access for various organizations. As the Paris Olympics approaches, there is a high likelihood that threat actors will leverage this opportunity to target France-based entities. These threat actors are particularly interested in targeting partner organizations, support entities, and ticketing platforms involved in the event to leak user PII and other sensitive details such as financial information, aiming to create disruption and capitalize on the heightened activity and attention surrounding the games.

Database Advertisements

FortiGuard Threat Research has identified numerous data breaches and leaks involving France-based companies posted on the dark web. These posts often contain sensitive information such as full names, dates of birth, social security numbers, email addresses, phone numbers, residential addresses, and other personally identifiable information. The combination of high-profile events like the Olympics and the availability of extensive personal data on the dark web creates a fertile ground for cybercriminal activities. Cybercriminals can leverage this sensitive information in various ways, such as targeted phishing scams, social engineering attacks, malware distribution, and disinformation campaigns.

Below, we have listed various forum posts with the potential to target French entities. The following section provides a detailed breakdown of historic threats to France, as observed on these forums:



France 909 documents pack
By rassvettt, May 20 in Auctions

rassvettt
megabyte
Paid registration
1
63 posts
Joined
04/14/24 (ID: 165972)
Activity
хакинг / hacking

Posted May 20

I am selling pack of France documents (ID Card (CNI)/Passport Photo/Scan)

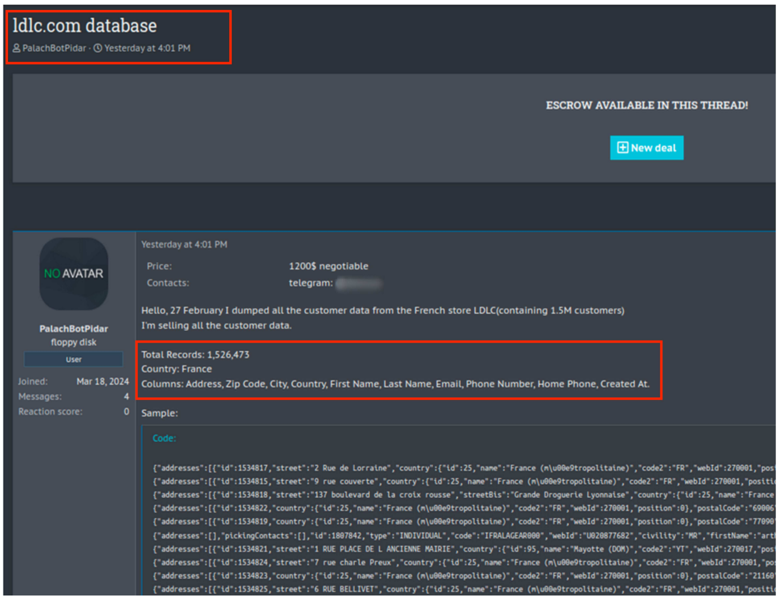
Count: 909
id card scan - 390
id card photo - 284
passport scan - 120
passport photo - 115

With doc photos attached info file with email, phone and address
Source: Gun club dump
Dump's date: 19.05.2024

All text is visible and actual

Start: 500$
Step: 100$
Blitz: 5000$
PPS: 24h

Garant +



ldlc.com database
PalachBotPidar · Yesterday at 4:01 PM

ESCROW AVAILABLE IN THIS THREAD!

NO AVATAR
PalachBotPidar
floppy disk
User
Joined: Mar 18, 2024
Messages: 4
Reaction score: 0

Yesterday at 4:01 PM

Price: 1200$ negotiable
Contacts: telegram: [redacted]

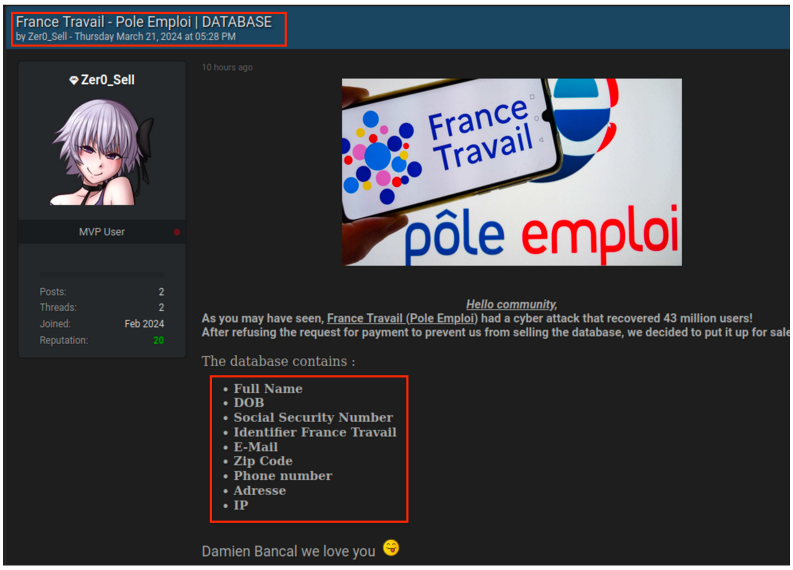
Hello, 27 February I dumped all the customer data from the French store LDLC(containing 1.5M customers)
I'm selling all the customer data.

Total Records: 1,526,473
Country: France
Columns: Address, Zip Code, City, Country, First Name, Last Name, Email, Phone Number, Home Phone, Created At.

Sample:

Code:

```
{"addresses":[{"id":1534817,"street":"2 Rue de Lorraine","country":{"id":25,"name":"France (m\u00e9tropolitaine)","code2":"FR","webId":270001,"pos
{"addresses":[{"id":1534815,"street":"9 rue couverte","country":{"id":25,"name":"France (m\u00e9tropolitaine)","code2":"FR","webId":270001,"positi
{"addresses":[{"id":1534818,"street":"137 boulevard de la croix rousse","streetBis":"Grande Droguerie Lyonnaise","country":{"id":25,"name":"France
{"addresses":[{"id":1534822,"country":{"id":25,"name":"France (m\u00e9tropolitaine)","code2":"FR","webId":270001,"position":0},"postalCode":"69006
{"addresses":[{"id":1534819,"country":{"id":25,"name":"France (m\u00e9tropolitaine)","code2":"FR","webId":270001,"position":0},"postalCode":"77090
{"addresses":[],"pickingContacts":[],"id":1807842,"type":"INDIVIDUAL","code":"IFRALAGEAR000","webId":"U020877682","civility":"MR","firstName":"art
{"addresses":[{"id":1534821,"street":"1 RUE PLACE DE L ANCIENNE MAIRIE","country":{"id":95,"name":"Mayotte (DOM)","code2":"YT","webId":270017,"pos
{"addresses":[{"id":1534824,"street":"7 rue charle Preux","country":{"id":25,"name":"France (m\u00e9tropolitaine)","code2":"FR","webId":270001,"po
{"addresses":[{"id":1534823,"country":{"id":25,"name":"France (m\u00e9tropolitaine)","code2":"FR","webId":270001,"position":0},"postalCode":"21160
{"addresses":[{"id":1534825,"street":"6 RUE BELLIVET","country":{"id":25,"name":"France (m\u00e9tropolitaine)","code2":"FR","webId":270001,"positi
```



France Travail - Pole Emploi | DATABASE
by Zero_Sell - Thursday March 21, 2024 at 05:28 PM

Zer0_Sell
MVP User
Posts: 2
Threads: 2
Joined: Feb 2024
Reputation: 20

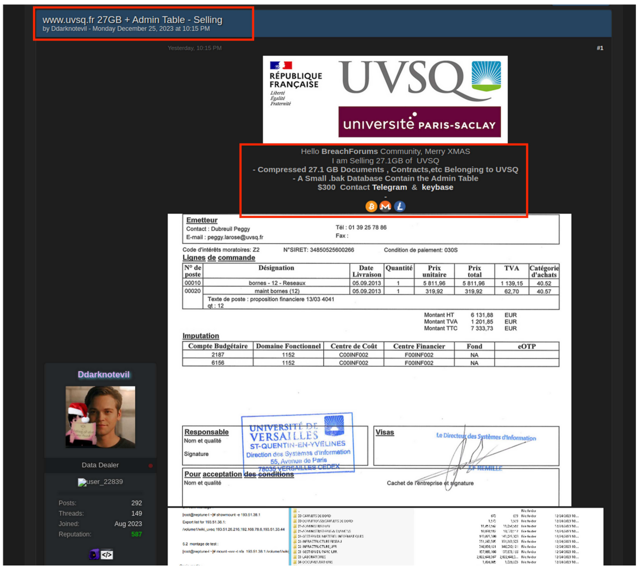
10 hours ago

Hello community,
As you may have seen, France Travail (Pole Emploi) had a cyber attack that recovered 43 million users!
After refusing the request for payment to prevent us from selling the database, we decided to put it up for sale

The database contains :

- **Full Name**
- **DOB**
- **Social Security Number**
- **Identifier France Travail**
- **E-Mail**
- **Zip Code**
- **Phone number**
- **Adresse**
- **IP**

Damien Bancal we love you 😋



www.uvsq.fr 27GB + Admin Table - Selling
by Ddarknotevil - Monday December 25, 2023 at 10:15 PM

Yesterday, 10:15 PM #1

Hello **BreachForums** Community, Merry XMAS
I am Selling 27.1GB of UVSQ
- Compressed 27.1 GB Documents , Contracts,etc Belonging to UVSQ
- A Small .bak Database Contain the Admin Table
$300 Contact Telegram & keybase

Ddarknotevil
Data Dealer
user_22839
Posts: 292
Threads: 149
Joined: Aug 2023
Reputation: 587

Emetteur
Contact : Dubreuil Peggy
E-mail : peggy.larose@uvsq.fr
Tél : 01 39 25 78 86
Fax :

Code d'intérêts moratoires: Z2 N°SIRET: 34850525600266 Condition de paiement: 030S

Lignes de commande

N° de poste	Désignation	Date Livraison	Quantité	Prix unitaire	Prix total	TVA	Catégorie d'achats
00010	bornes - 12 - Reseaux	05.09.2013	1	5 811,96	5 811,96	1 139,15	40.52
00020	maint bornes (12)	05.09.2013	1	319,92	319,92	62,70	40.57
	Texte de poste : proposition financiere 13/03 4041 qt : 12						

Montant HT 6 131,88 EUR
Montant TVA 1 201,85 EUR
Montant TTC 7 333,73 EUR

Imputation

Compte Budgétaire	Domaine Fonctionnel	Centre de Coût	Centre Financier	Fond	eOTP
2187	1152	C00INF002	F00INF002	NA	
6156	1152	C00INF002	F00INF002	NA	

Responsable
Nom et qualité
Signature

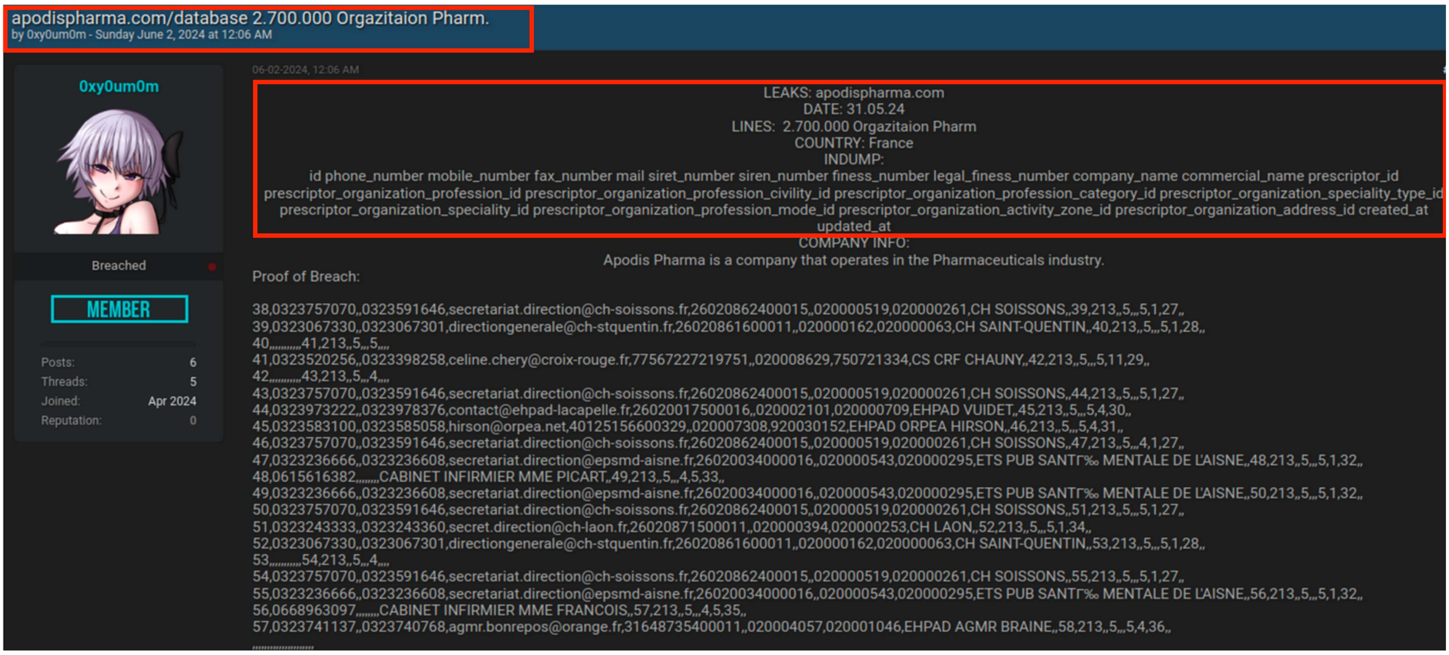
UNIVERSITÉ DE VERSAILLES
ST-QUENTIN-EN-YVELINES
Direction des Systèmes d'information
55, Avenue de Paris
78035 VERSAILLES CEDEX

Visas
Le Directeur des Systèmes d'Information
J.F. REMILLE

Pour acceptation des conditions
Nom et qualité
Cachet de l'entreprise et signature

[root@neptune-l ~]# showmount -e 193.51.38.1
Export list for 193.51.38.1:
/volume1/wiki_uvsq 193.51.26.216,192.168.78.6,193.51.33.44

6.2 montage de test :
[root@neptune-l ~]# mount -vvv -t nfs 193.51.38.1:/volume1/wiki



apodispharma.com/database 2.700.000 Orgazitaion Pharm.
by 0xy0um0m - Sunday June 2, 2024 at 12:06 AM

0xy0um0m

Breached

MEMBER

Posts: 6
Threads: 5
Joined: Apr 2024
Reputation: 0

06-02-2024, 12:06 AM

LEAKS: apodispharma.com
DATE: 31.05.24
LINES: 2.700.000 Orgazitaion Pharm
COUNTRY: France
INDUMP:
id phone_number mobile_number fax_number mail siret_number siren_number finess_number legal_finess_number company_name commercial_name prescriptor_id prescriptor_organization_profession_id prescriptor_organization_profession_civility_id prescriptor_organization_profession_category_id prescriptor_organization_speciality_type_id prescriptor_organization_speciality_id prescriptor_organization_profession_mode_id prescriptor_organization_activity_zone_id prescriptor_organization_address_id created_at updated_at
COMPANY INFO:
Apodis Pharma is a company that operates in the Pharmaceuticals industry.

Proof of Breach:

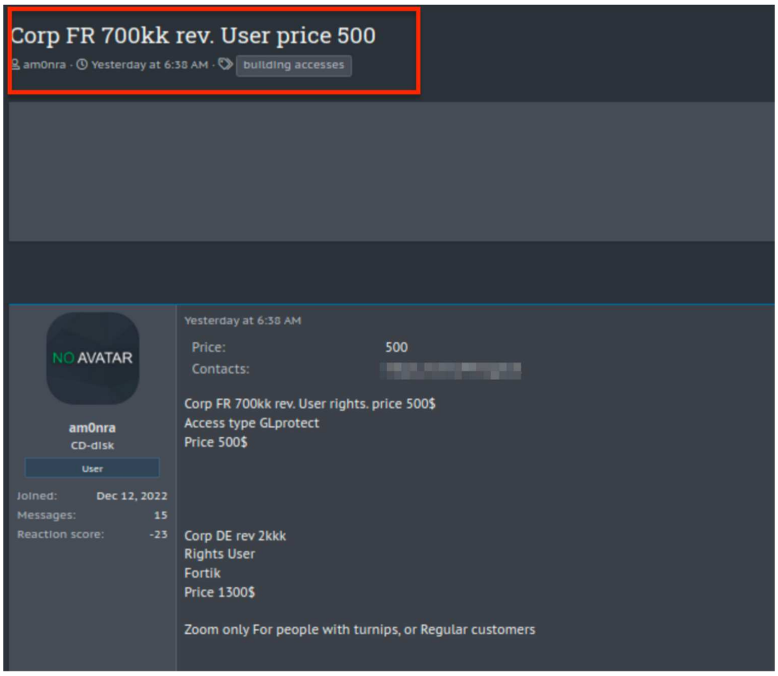
```
38,0323757070,,0323591646,secretariat.direction@ch-soissons.fr,26020862400015,,020000519,020000261,CH SOISSONS,,39,213,,5,,,5,1,27,,
39,0323067330,,0323067301,directiongenerale@ch-stquentin.fr,26020861600011,,020000162,020000063,CH SAINT-QUENTIN,,40,213,,5,,,5,1,28,,
40,,,,,,,,,,,41,213,,5,,,5,,,,
41,0323520256,,0323398258,celine.chery@croix-rouge.fr,77567227219751,,020008629,750721334,CS CRF CHAUNY,,42,213,,5,,,5,11,29,,
42,,,,,,,,,,,43,213,,5,,,4,,,,
43,0323757070,,0323591646,secretariat.direction@ch-soissons.fr,26020862400015,,020000519,020000261,CH SOISSONS,,44,213,,5,,,5,1,27,,
44,0323973222,,0323978376,contact@ehpad-lacapelle.fr,26020017500016,,020002101,020000709,EHPAD VUIDET,,45,213,,5,,,5,4,30,,
45,0323583100,,0323585058,hirson@orpea.net,40125156600329,,020007308,920030152,EHPAD ORPEA HIRSON,,46,213,,5,,,5,4,31,,
46,0323757070,,0323591646,secretariat.direction@ch-soissons.fr,26020862400015,,020000519,020000261,CH SOISSONS,,47,213,,5,,,4,1,27,,
47,0323236666,,0323236608,secretariat.direction@epsmd-aisne.fr,26020034000016,,020000543,020000295,ETS PUB SANTГ‰ MENTALE DE L'AISNE,,48,213,,5,,,5,1,32,,
48,0615616382,,,,,,,,CABINET INFIRMIER MME PICART,,49,213,,5,,,4,5,33,,
49,0323236666,,0323236608,secretariat.direction@epsmd-aisne.fr,26020034000016,,020000543,020000295,ETS PUB SANTГ‰ MENTALE DE L'AISNE,,50,213,,5,,,5,1,32,,
50,0323757070,,0323591646,secretariat.direction@ch-soissons.fr,26020862400015,,020000519,020000261,CH SOISSONS,,51,213,,5,,,5,1,27,,
51,0323243333,,0323243360,secret.direction@ch-laon.fr,26020871500011,,020000394,020000253,CH LAON,,52,213,,5,,,5,1,34,,
52,0323067330,,0323067301,directiongenerale@ch-stquentin.fr,26020861600011,,020000162,020000063,CH SAINT-QUENTIN,,53,213,,5,,,5,1,28,,
53,,,,,,,,,,,54,213,,5,,,4,,,,
54,0323757070,,0323591646,secretariat.direction@ch-soissons.fr,26020862400015,,020000519,020000261,CH SOISSONS,,55,213,,5,,,5,1,27,,
55,0323236666,,0323236608,secretariat.direction@epsmd-aisne.fr,26020034000016,,020000543,020000295,ETS PUB SANTГ‰ MENTALE DE L'AISNE,,56,213,,5,,,5,1,32,,
56,0668963097,,,,,,,,CABINET INFIRMIER MME FRANCOIS,,57,213,,5,,,4,5,35,,
57,0323741137,,0323740768,agmr.bonrepos@orange.fr,31648735400011,,020004057,020001046,EHPAD AGMR BRAINE,,58,213,,5,,,5,4,36,,

,,,,,,,,,,,,,,,,,,,,
```

(Forum Posts - Database advertisements)

Network Access Advertisements

During our research, we identified numerous darknet posts advertising access to France-based companies' networks. For instance, if a Virtual Private Network (VPN) or Remote Desktop Protocol (RDP) is compromised, it can lead to unauthorized entry into critical networks and data repositories. This poses significant security risks, as attackers could exploit this access to steal confidential information, deploy malware, or launch additional cyberattacks. Such breaches can result in substantial financial losses and reputational damage. Below are some of the screenshots of access advertisements observed on the forums.



Corp FR 700kk rev. User price 500

amOnra · Yesterday at 6:38 AM · building accesses

amOnra
CD-disk
User

Joined: Dec 12, 2022
Messages: 15
Reaction score: -23

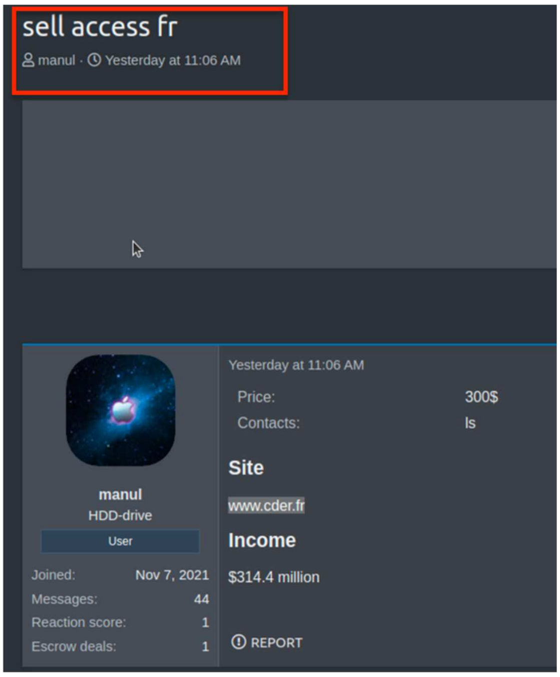
Yesterday at 6:38 AM

Price: 500
Contacts: [redacted]

Corp FR 700kk rev. User rights. price 500$
Access type GLprotect
Price 500$

Corp DE rev 2kkk
Rights User
Fortik
Price 1300$

Zoom only For people with turnips, or Regular customers



sell access fr

manul · Yesterday at 11:06 AM

manul
HDD-drive
User

Joined: Nov 7, 2021
Messages: 44
Reaction score: 1
Escrow deals: 1

Yesterday at 11:06 AM

Price: 300$
Contacts: ls

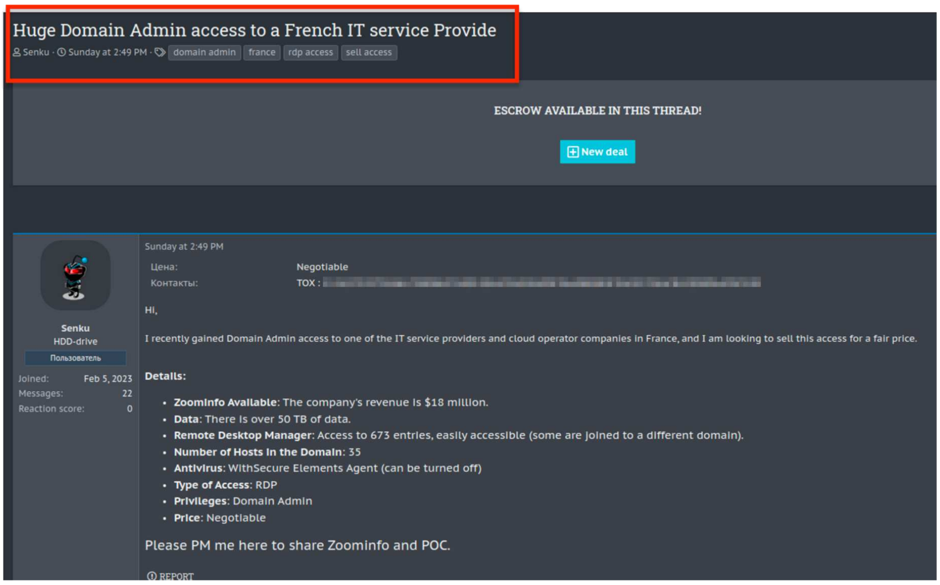
Site

www.cder.fr

Income

$314.4 million

REPORT



Huge Domain Admin access to a French IT service Provide

Senku · Sunday at 2:49 PM · domain admin · france · rdp access · sell access

ESCROW AVAILABLE IN THIS THREAD!

New deal

Senku
HDD-drive
Пользователь

Joined: Feb 5, 2023
Messages: 22
Reaction score: 0

Sunday at 2:49 PM

Цена: Negotiable
Контакты: TOX : [redacted]

Hi,

I recently gained Domain Admin access to one of the IT service providers and cloud operator companies in France, and I am looking to sell this access for a fair price.

Details:

- **Zoominfo Available**: The company's revenue is $18 million.
- **Data**: There is over 50 TB of data.
- **Remote Desktop Manager**: Access to 673 entries, easily accessible (some are joined to a different domain).
- **Number of Hosts in the Domain**: 35
- **Antivirus**: WithSecure Elements Agent (can be turned off)
- **Type of Access**: RDP
- **Privileges**: Domain Admin
- **Price**: Negotiable

Please PM me here to share Zoominfo and POC.

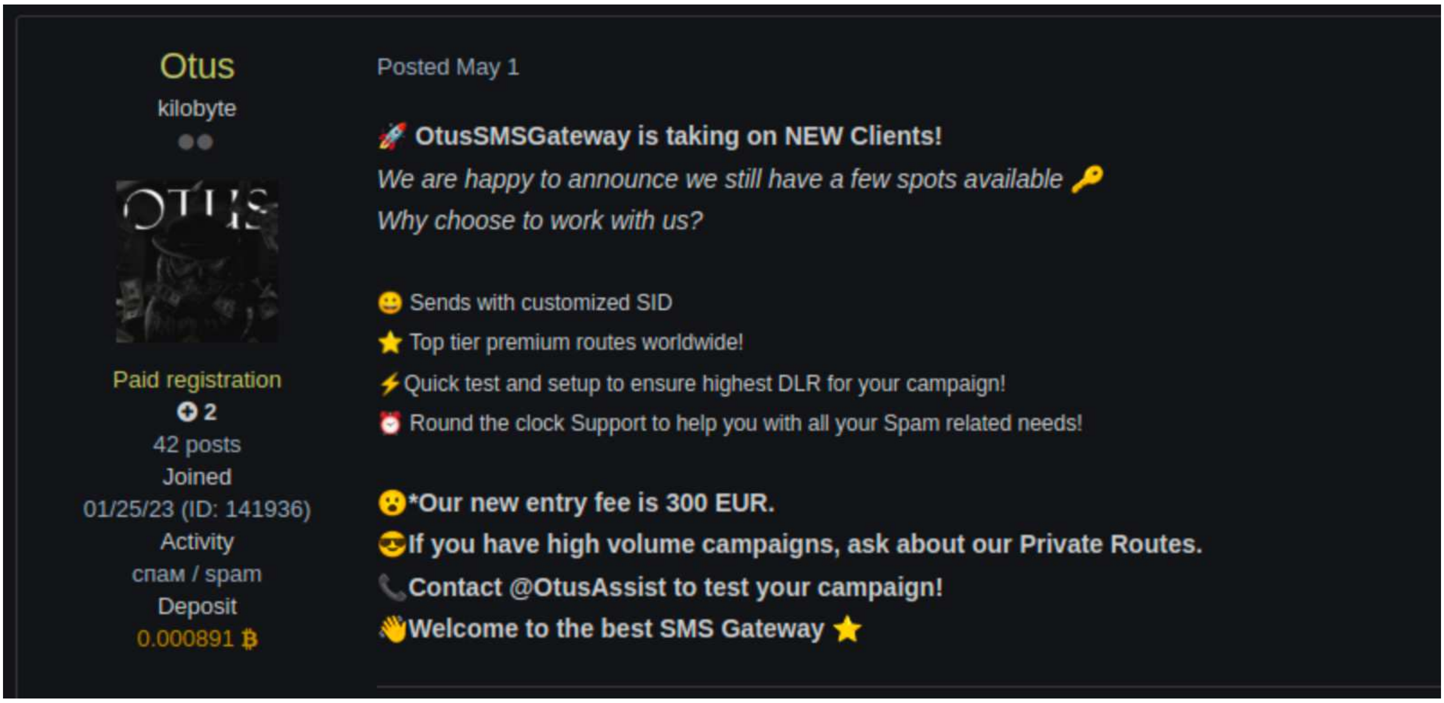
REPORT

(Forum Posts - Network access advertisements)

Dark Web Services with the Potential to Disrupt the Olympics

We have identified various services on the dark web that can pose threats to the Olympics. These include coding services for creating phishing websites and associated live panels, bulk SMS services for mass communication, and phone number spoofing services. These offerings can facilitate phishing attacks, spread misinformation, and disrupt communications by impersonating trusted sources, potentially causing significant operational and security challenges during the event.

An SMS gateway is a service that enables computers to send and receive SMS (Short Message Service) messages to and from mobile phones. It acts as a bridge between different mobile networks and the internet, allowing messages to be transmitted across these platforms seamlessly. Some SMS gateway providers allow the sender to manipulate address information, which can be exploited by threat actors to send bulk SMS messages with spoofed sender information. Threat actors can use spoofed SMS messages to impersonate official Olympic communications, tricking recipients into clicking malicious links. These links can lead to phishing websites that capture sensitive information such as personal details or payment information.



Otus
kilobyte

Paid registration
+2
42 posts
Joined
01/25/23 (ID: 141936)
Activity
спам / spam
Deposit
0.000891 ฿

Posted May 1

🚀 **OtusSMSGateway is taking on NEW Clients!**

We are happy to announce we still have a few spots available 🔑

Why choose to work with us?

😀 Sends with customized SID

⭐ Top tier premium routes worldwide!

⚡Quick test and setup to ensure highest DLR for your campaign!

⏰ Round the clock Support to help you with all your Spam related needs!

😮*Our new entry fee is 300 EUR.

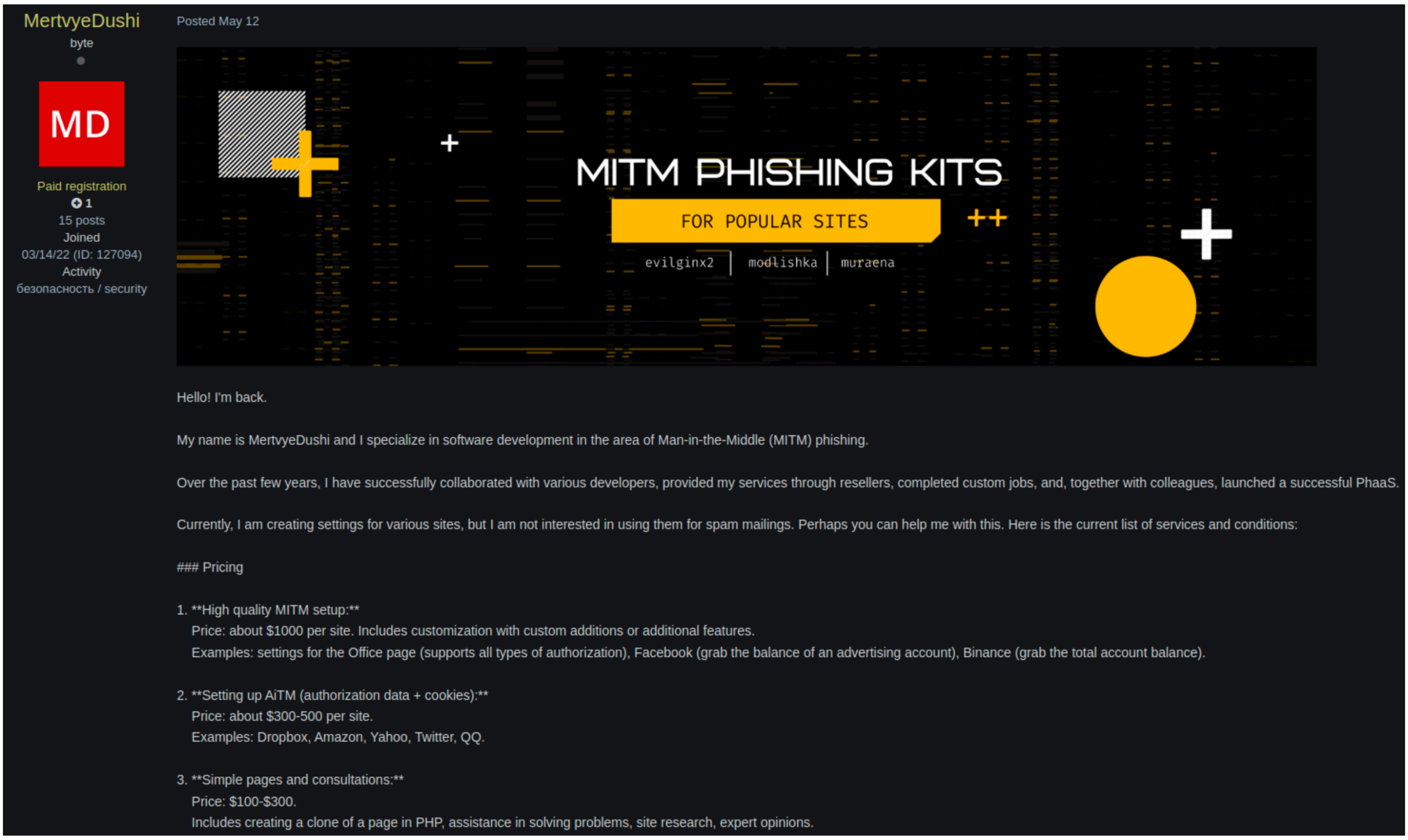
😎If you have high volume campaigns, ask about our Private Routes.

📞Contact @OtusAssist to test your campaign!

👋Welcome to the best SMS Gateway ⭐

(SMS gateway service for SMS spamming)

Phishing kits are pre-packaged tools that simplify the process of launching phishing attacks. These kits typically include all the necessary components, such as fake login pages, email templates, and scripts to capture user credentials. They are designed to be user-friendly, allowing even those with limited technical skills to deploy effective phishing campaigns. Below are some of the latest offerings posted on the dark web forums that allow individuals to create fake websites that mimic official Olympic-related portals, such as ticketing sites, volunteer registration pages, or media access points.



MertvyeDushi
byte

MD

Paid registration
+1
15 posts
Joined
03/14/22 (ID: 127094)
Activity
безопасность / security

Posted May 12

Hello! I'm back.

My name is MertvyeDushi and I specialize in software development in the area of Man-in-the-Middle (MITM) phishing.

Over the past few years, I have successfully collaborated with various developers, provided my services through resellers, completed custom jobs, and, together with colleagues, launched a successful PhaaS.

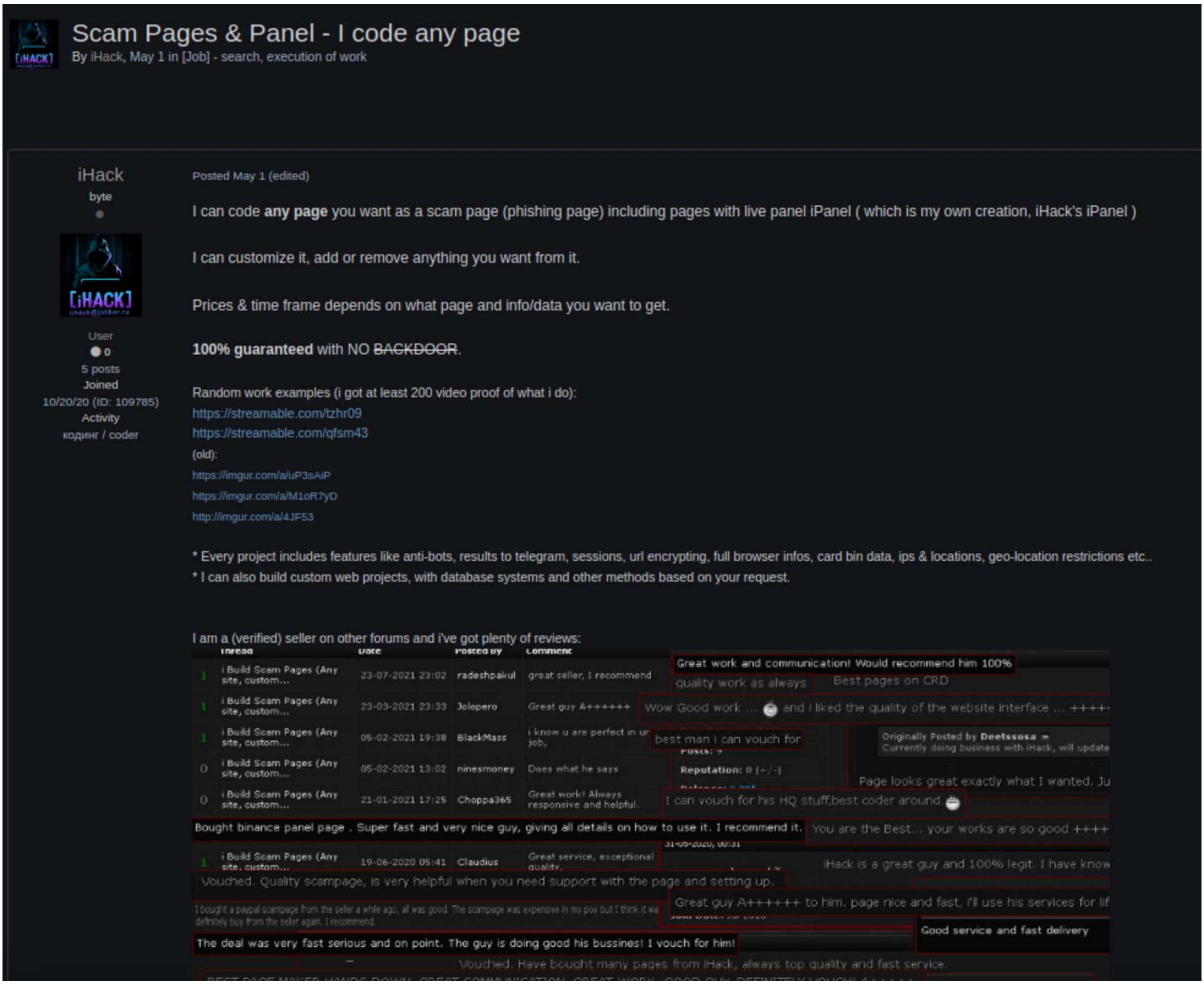
Currently, I am creating settings for various sites, but I am not interested in using them for spam mailings. Perhaps you can help me with this. Here is the current list of services and conditions:

Pricing

1. **High quality MITM setup:**
   Price: about $1000 per site. Includes customization with custom additions or additional features.
   Examples: settings for the Office page (supports all types of authorization), Facebook (grab the balance of an advertising account), Binance (grab the total account balance).

2. **Setting up AiTM (authorization data + cookies):**
   Price: about $300-500 per site.
   Examples: Dropbox, Amazon, Yahoo, Twitter, QQ.

3. **Simple pages and consultations:**
   Price: $100-$300.
   Includes creating a clone of a page in PHP, assistance in solving problems, site research, expert opinions.



Scam Pages & Panel - I code any page

By iHack, May 1 in [Job] - search, execution of work

iHack
byte
User
0
5 posts
Joined
10/20/20 (ID: 109785)
Activity
кодинг / coder

Posted May 1 (edited)

I can code **any page** you want as a scam page (phishing page) including pages with live panel iPanel (which is my own creation, iHack's iPanel)

I can customize it, add or remove anything you want from it.

Prices & time frame depends on what page and info/data you want to get.

100% guaranteed with NO ~~BACKDOOR~~.

Random work examples (i got at least 200 video proof of what i do):
https://streamable.com/tzhr09
https://streamable.com/qfsm43
(old):
https://imgur.com/a/uP3sAiP
https://imgur.com/a/M1oR7yD
http://imgur.com/a/4JF53

* Every project includes features like anti-bots, results to telegram, sessions, url encrypting, full browser infos, card bin data, ips & locations, geo-location restrictions etc..
* I can also build custom web projects, with database systems and other methods based on your request.

I am a (verified) seller on other forums and i've got plenty of reviews:

	Thread	Date	Posted by	Comment
1	i Build Scam Pages (Any site, custom...	23-07-2021 23:02	radeshpakul	great seller, I recommend
1	i Build Scam Pages (Any site, custom...	23-03-2021 23:33	Jolopero	Great guy A++++++
1	i Build Scam Pages (Any site, custom...	05-02-2021 19:38	BlackMass	i know u are perfect in ur job,
0	i Build Scam Pages (Any site, custom...	05-02-2021 13:02	ninesmoney	Does what he says
0	i Build Scam Pages (Any site, custom...	21-01-2021 17:25	Choppa365	Great work! Always responsive and helpful.
1	i Build Scam Pages (Any site, custom...	19-06-2020 05:41	Claudius	Great service, exceptional quality.

Great work and communication! Would recommend him 100%

quality work as always

Best pages on CRD

Wow Good work ... and i liked the quality of the website interface ... ++++

best man i can vouch for

Posts: 9

Reputation: 0 [+/-]

Originally Posted by **Deetssosa**
Currently doing business with iHack, will update

Page looks great exactly what I wanted. Ju

I can vouch for his HQ stuff,best coder around.

Bought binance panel page . Super fast and very nice guy, giving all details on how to use it. I recommend it.

You are the Best... your works are so good ++++

31-05-2020, 00:31

iHack is a great guy and 100% legit. I have know

Vouched. Quality scampage, is very helpful when you need support with the page and setting up.

I bought a paypal scampage from the seller a while ago, all was good. The scampage was expensive in my pov but I think it wa definitely buy from the seller again. I recommend.

Great guy A++++++ to him. page nice and fast, i'll use his services for lif

Good service and fast delivery

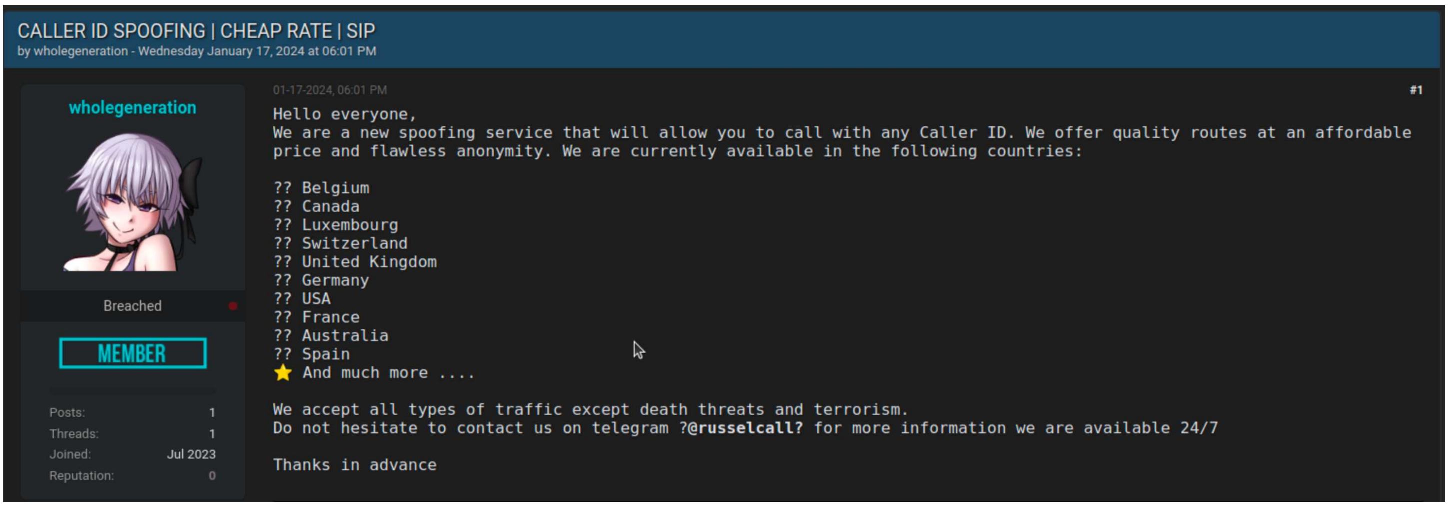
The deal was very fast serious and on point. The guy is doing good his bussines! I vouch for him!

Vouched. Have bought many pages from iHack, always top quality and fast service.

BEST PAGE MAKER HANDS DOWN, GREAT COMMUNICATION, GREAT WORK, GOOD GUY, DEFINITELY VOUCH! A++++++

(Service for phishing page development)

Additionally, we also identified "Spoofing Services" which allows the caller to manipulate the caller ID information to display a number other than the actual calling number. This can be done using VoIP (Voice over Internet Protocol) services or special hardware and software. Following services posted on the dark web allows attackers to impersonate Olympic officials or their partners. By doing so, they can trick recipients into providing sensitive information, such as passwords and credit card numbers.



CALLER ID SPOOFING | CHEAP RATE | SIP

by wholegeneration - Wednesday January 17, 2024 at 06:01 PM

wholegeneration
Breached
MEMBER
Posts: 1
Threads: 1
Joined: Jul 2023
Reputation: 0

01-17-2024, 06:01 PM #1

```
Hello everyone,
We are a new spoofing service that will allow you to call with any Caller ID. We offer quality routes at an affordable
price and flawless anonymity. We are currently available in the following countries:

?? Belgium
?? Canada
?? Luxembourg
?? Switzerland
?? United Kingdom
?? Germany
?? USA
?? France
?? Australia
?? Spain
⭐ And much more ....

We accept all types of traffic except death threats and terrorism.
Do not hesitate to contact us on telegram ?@russelcall? for more information we are available 24/7

Thanks in advance
```

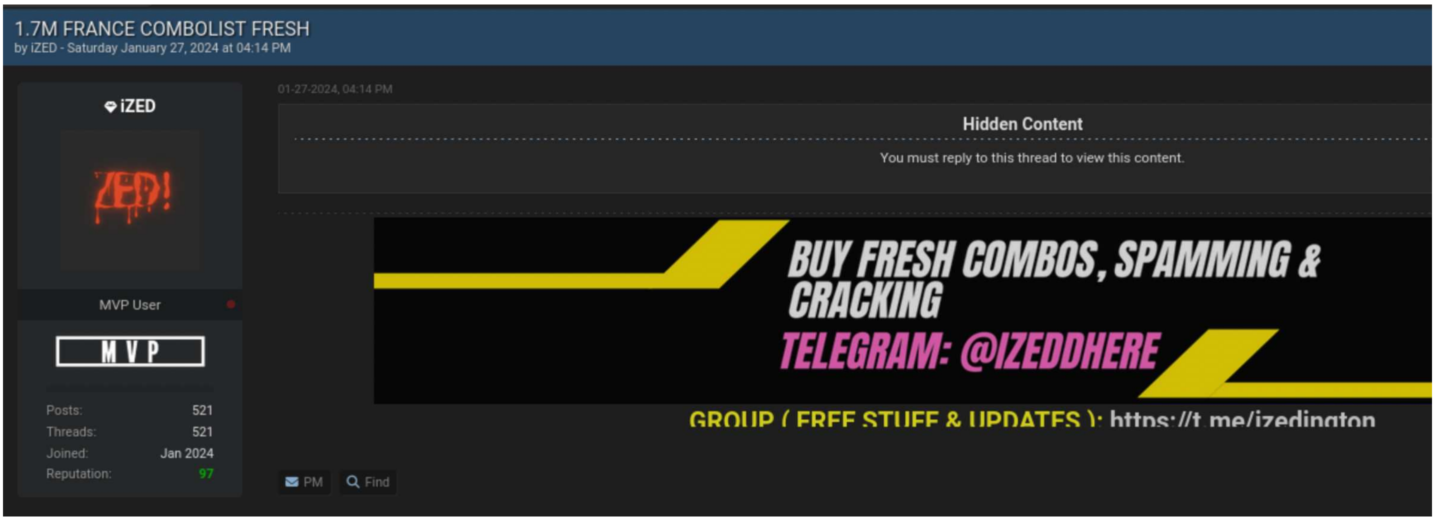
(Caller ID spoofing service)

Combolist Posing Threats to Individuals

A combo list is a compilation of usernames and passwords, often obtained from various data breaches and combined into a single file. Cybercriminals use these lists to launch credential-stuffing attacks, using automated tools to try these username-password combinations on multiple websites and services to gain unauthorized access. Below, we have listed several offerings of combo-lists by threat actors on darknet forums and Telegram channels:

Consequences of Combolist Attacks:

- Unauthorized Access: Cybercriminals can gain access to user accounts across different platforms, leading to potential data breaches and identity theft.
- Reputation Damage: Organizations that fall victim to these attacks can suffer significant reputational damage, losing the trust of their customers and partners.
- Service Disruption: Account takeovers can lead to disruptions in services, as compromised accounts might be used for spamming, launching further attacks, or other malicious activities.
- Data Loss: Sensitive data, including personal information, can be stolen and further exploited or sold on the dark web.



1.7M FRANCE COMBOLIST FRESH
by iZED - Saturday January 27, 2024 at 04:14 PM

iZED

MVP User

M V P

Posts: 521
Threads: 521
Joined: Jan 2024
Reputation: 97

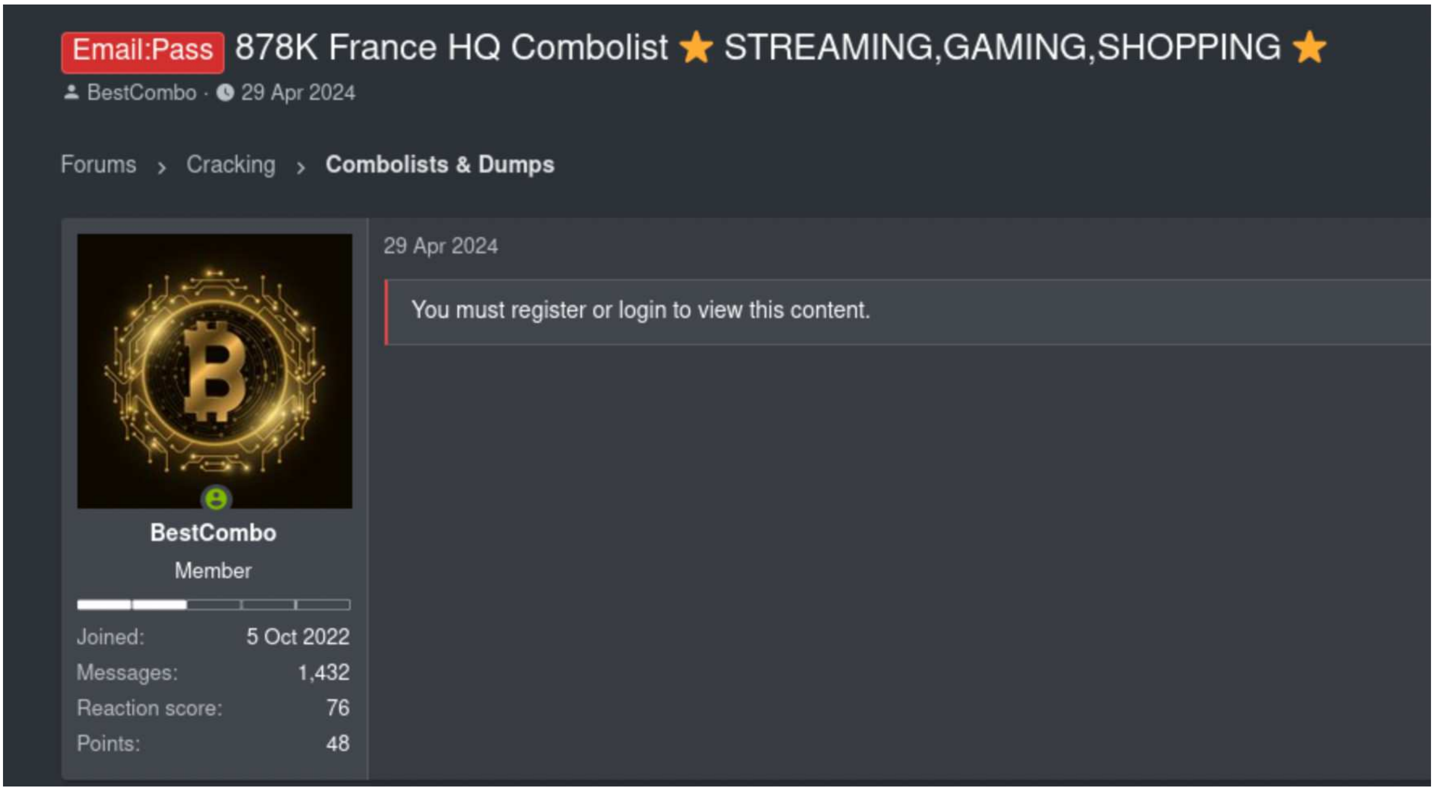
01-27-2024, 04:14 PM

Hidden Content

You must reply to this thread to view this content.

BUY FRESH COMBOS, SPAMMING & CRACKING
TELEGRAM: @IZEDDHERE

GROUP (FREE STUFF & UPDATES): https://t.me/izedington



Email:Pass 878K France HQ Combolist ★ STREAMING,GAMING,SHOPPING ★

BestCombo · 29 Apr 2024

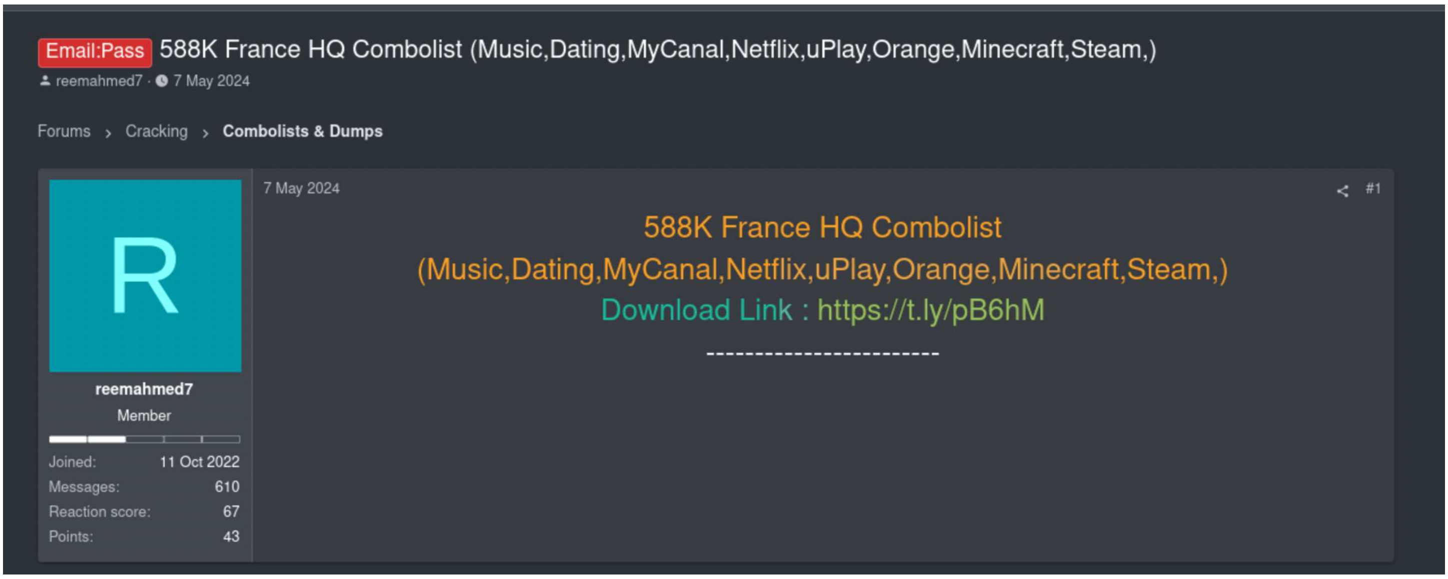
Forums › Cracking › Combolists & Dumps

BestCombo
Member

Joined: 5 Oct 2022
Messages: 1,432
Reaction score: 76
Points: 48

29 Apr 2024

You must register or login to view this content.



Email:Pass 588K France HQ Combolist (Music,Dating,MyCanal,Netflix,uPlay,Orange,Minecraft,Steam,)

reemahmed7 · 7 May 2024

7 May 2024 #1

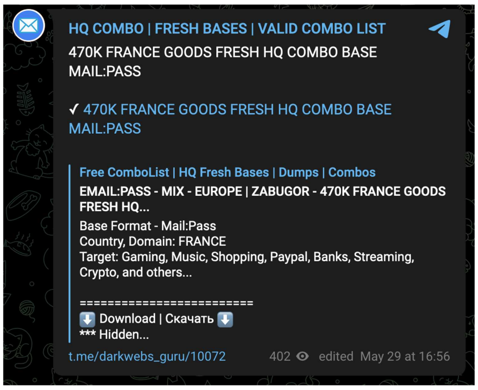
588K France HQ Combolist
(Music,Dating,MyCanal,Netflix,uPlay,Orange,Minecraft,Steam,)
Download Link : https://t.ly/pB6hM
----

reemahmed7
Member

Joined:	11 Oct 2022
Messages:	610
Reaction score:	67
Points:	43

(Forum posts - combo-lists advertisements)

Additionally, we have identified several Telegram channels offering combo lists specifically targeting France-based users.



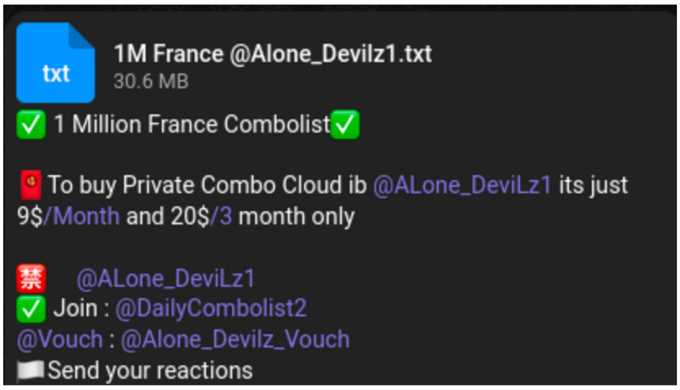
HQ COMBO | FRESH BASES | VALID COMBO LIST
470K FRANCE GOODS FRESH HQ COMBO BASE MAIL:PASS

✓ 470K FRANCE GOODS FRESH HQ COMBO BASE MAIL:PASS

Free ComboList | HQ Fresh Bases | Dumps | Combos
EMAIL:PASS - MIX - EUROPE | ZABUGOR - 470K FRANCE GOODS FRESH HQ...
Base Format - Mail:Pass
Country, Domain: FRANCE
Target: Gaming, Music, Shopping, Paypal, Banks, Streaming, Crypto, and others...

=========================
⬇️ Download | Скачать ⬇️
*** Hidden...

t.me/darkwebs_guru/10072 402 edited May 29 at 16:56



1M France @Alone_Devilz1.txt
30.6 MB
✅ 1 Million France Combolist✅

To buy Private Combo Cloud ib @ALone_DeviLz1 its just 9$/Month and 20$/3 month only

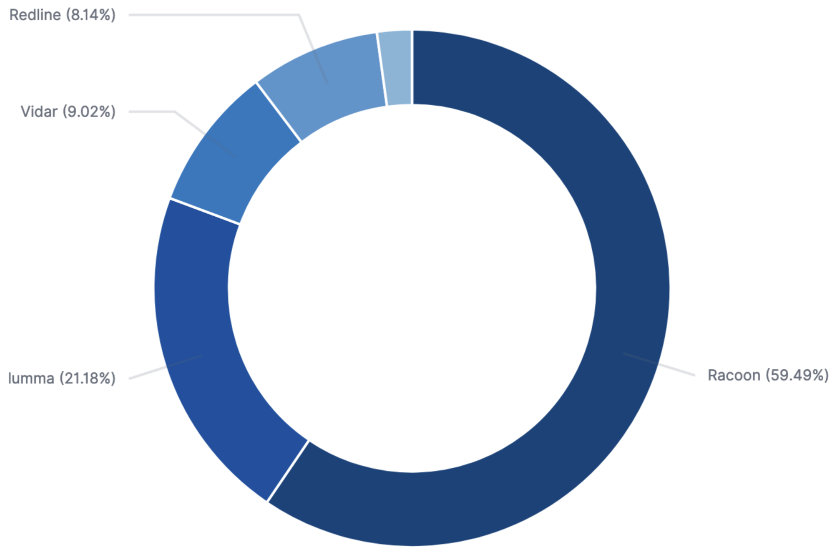
禁 @ALone_DeviLz1
✅ Join : @DailyCombolist2
@Vouch : @Alone_Devilz_Vouch
Send your reactions

(Telegram messages offering combo-lists)

Infostealers and Credential Leaks

Information stealer malware is designed to stealthily infiltrate a victim's computer or device and harvest sensitive information, such as login credentials, credit card details, and other personal data. We have also observed that threat actors are deploying various types of stealer malware to infect user systems and obtain unauthorized access. These types of accesses can be further leveraged by threat actors and initial access brokers (IABs) to execute ransomware attacks, causing substantial harm and financial loss to individuals and organizations.

The graph illustrates the most prevalent stealer malware in France. Our data indicates that Racoon is the most active info stealer, accounting for 59%, followed by Lumma at 21% and Vidar at 9%. These malware variants are known for their wide distribution and capability to infiltrate user devices to harvest sensitive information.



(Most active info stealer malware targeted France-based entities)

Escalating Hacktivist Activities Driven by Geopolitical Tensions

The Paris Olympics 2024 is not just a major sporting event but also a stage for political statements and actions. France's prominent role on the global stage, its stance on the Ukraine conflict, and its influence within international organizations have made it a target for various political reasons. These types of international events are always popular targets for hacktivist groups.

France has been a vocal supporter of Ukraine in its conflict with Russia, advocating for sanctions against Russia and providing support to Ukraine. The request for a UN ceasefire resolution specifically targeting Russia during the Olympics underscores France's position. This has made France a focal point for pro-Russian sentiments and actions, including potential cyberattacks by hacktivist groups aiming to disrupt the Olympics and protest against France's policies.

On June 16th, French President Emmanuel Macron requested the United Nations to introduce a ceasefire for the Olympic Games in Paris, specifically applying to Russia.

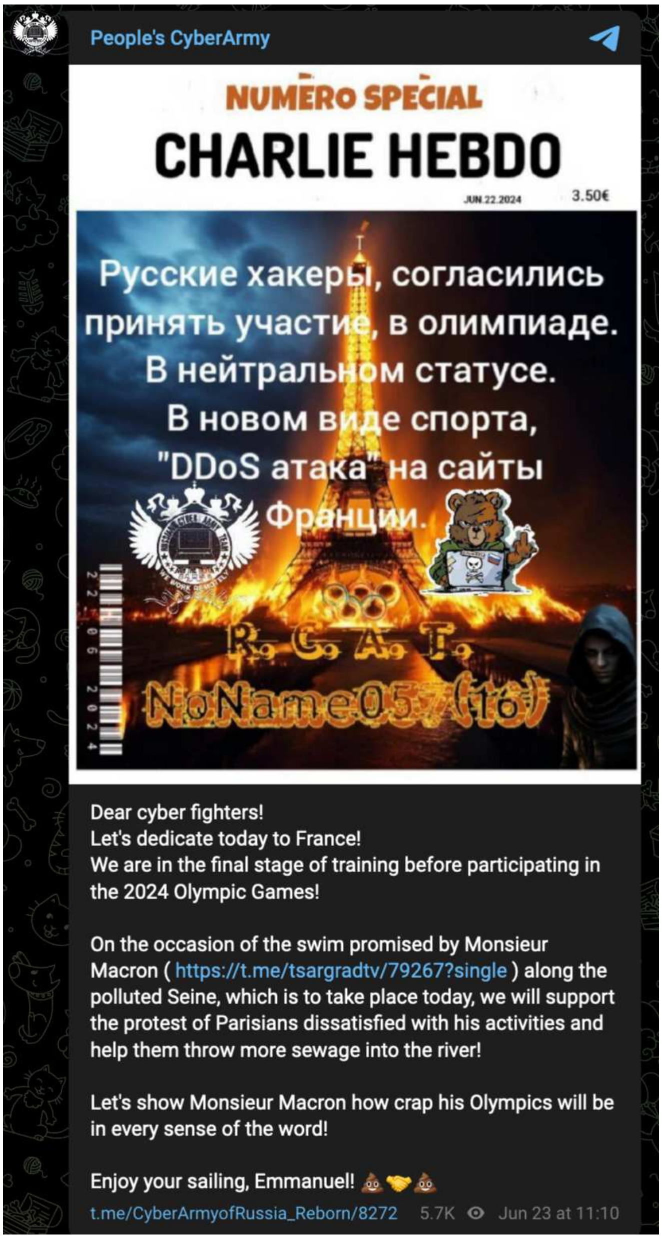
Macron stated: *"We will have a resolution that the UN General Assembly will adopt regarding the Olympic truce, but we do not consider this truce as an obligation regarding Ukraine. This is a call to Russia to stop its aggression."*

Earlier in March, Macron reiterated his support for the International Olympic Committee's (IOC) stance on promoting unity and reconciliation through sports. He stated:

"I *believe that sport should enable unity and reconciliation. The choice that has been made is one that we will collectively accept. We support Ukraine, and we have sanctioned Russia. Neutral athletes, under conditions of respectful conduct, must be able to pursue their work and their sport."*

However, Russian and Belarusian athletes will compete as neutrals, without their flags and anthems, and will be excluded from the opening parade. This decision followed Russia's invasion of Ukraine in February 2022. Amid these diplomatic tensions, cyber threats from pro-Russian hacktivist groups have emerged.

On June 23, 2024, several pro-Russian hacktivist groups, including Cyber Army Russia Reborn, NoName057(16), and Cyber Dragon, officially declared their intent to target the Paris Olympics and French entities. It is anticipated that other pro-Russian groups might join this campaign.



People's CyberArmy
NUMÉRO SPECIAL
CHARLIE HEBDO
JUN.22.2024
3.50€
Русские хакеры, согласились принять участие, в олимпиаде. В нейтральном статусе. В новом виде спорта, "DDoS атака" на сайты Франции.
R.C.A.T.
NoName057(16)

Dear cyber fighters!
Let's dedicate today to France!
We are in the final stage of training before participating in the 2024 Olympic Games!

On the occasion of the swim promised by Monsieur Macron (https://t.me/tsargradtv/79267?single) along the polluted Seine, which is to take place today, we will support the protest of Parisians dissatisfied with his activities and help them throw more sewage into the river!

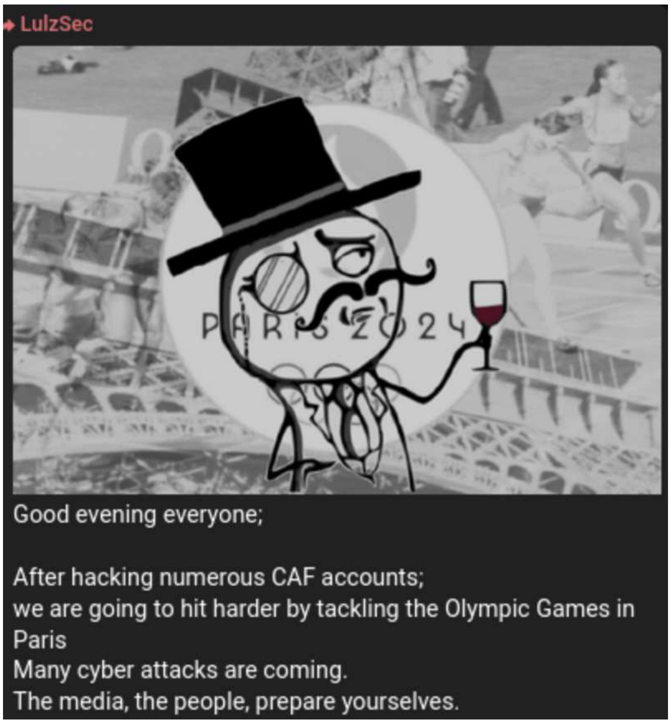
Let's show Monsieur Macron how crap his Olympics will be in every sense of the word!

Enjoy your sailing, Emmanuel! 💩🤝💩

t.me/CyberArmyofRussia_Reborn/8272 5.7K 👁 Jun 23 at 11:10

(Updates on the pro-Russian Telegram groups)

In addition to the threats mentioned above, we have identified a message posted by the hacktivist group LulzSec associated with the Paris Olympics. This group has publicly declared its intention to carry out cyberattacks on the Paris Olympic Games, warning organizers and participants to be prepared for these attacks. Such announcements highlight that hacktivist groups might target the Olympics website, media houses, broadcasting channels, or entities supporting the Paris Olympics, aiming to create chaos and disrupt the event.



LulzSec

Good evening everyone;

After hacking numerous CAF accounts;
we are going to hit harder by tackling the Olympic Games in Paris
Many cyber attacks are coming.
The media, the people, prepare yourselves.

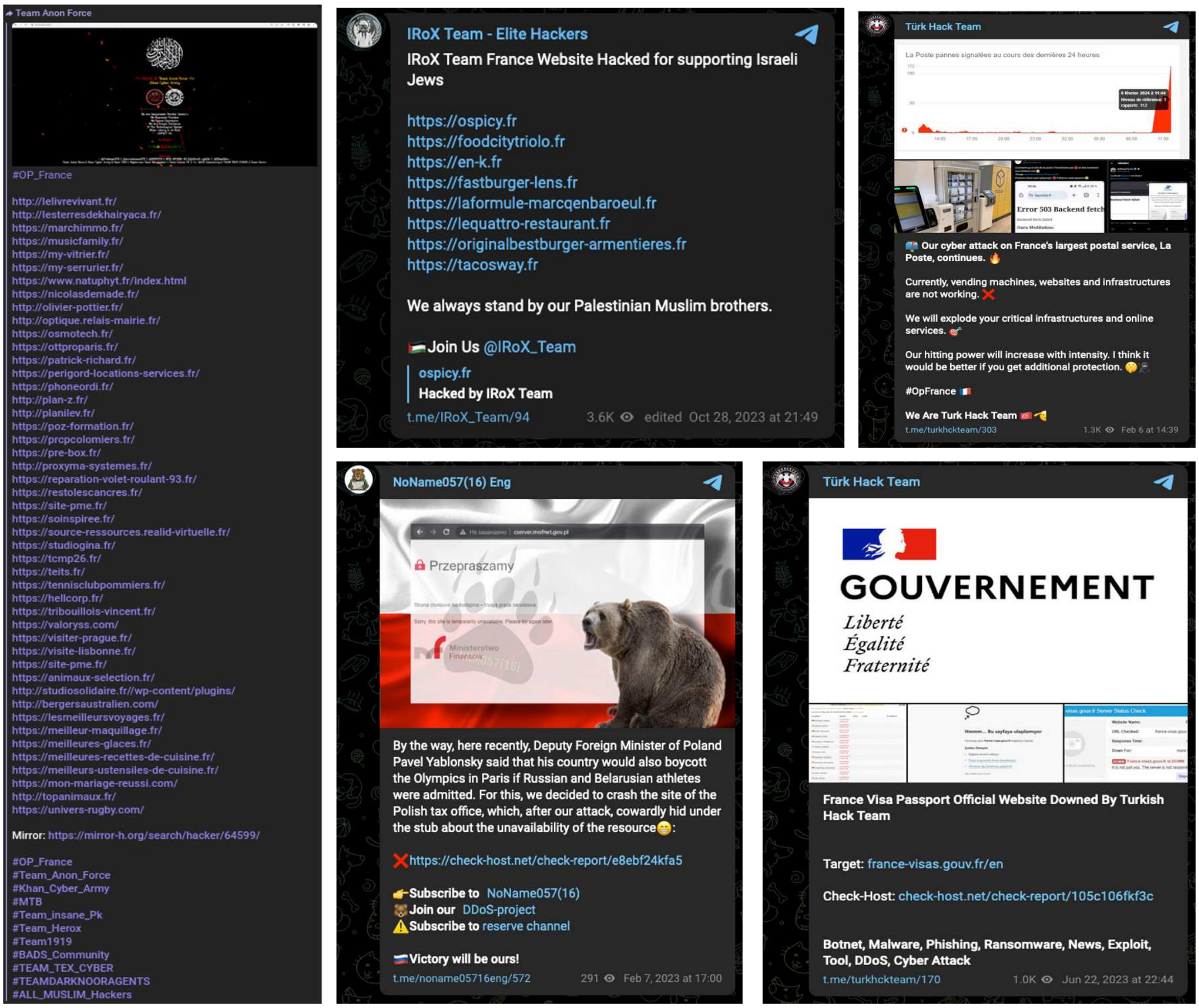
(Updates on the telegram channel of the LulzSec group)

In the past, we have observed that France and Paris have consistently been on the target list of various hacktivist groups under hashtags such as #OpFrance and #OpParis. These hacktivist groups typically target specific entities based on their political motives. Based on our observations, we have identified the following prominent hacktivist groups that have previously targeted or are likely to target French entities:

Group Name	Telegram Channel	Channel Created	Telegram Subscribers	Description
NoName057(16)	@noname05716	Aug 2022	58,400+	• The group is exclusively involved in DDoS attacks. • This group is known for supporting hacktivist campaigns in support of Russia in the ongoing war
Team Anon Force	@teamanonforce	Nov 2021	2,300+	• The group is exclusively involved in defacement attacks. • The group participated in OpIndia campaigns.
Turk Hack Team	@turkhckteam	Jan 2023	2400+	• The group is mainly involved in DDoS and website defacement attacks.
Garnesia Team	@garnesiateam	Jul 2023	2400+	• The group is mainly involved in DDoS, website defacement, and data breach attacks. • The group appears to be Indonesian based on the language used in Telegram messages, and most of the group's activities are in response to anti-Muslim incidents.
Anonymous Sudan	@xAnonymousSudan	Sep 2023	39,500+	• The group is now using a new channel, the previous channel used was removed by Telegram for violations of Telegram policies • The group claims to be Sudanese, and fighting for the rights of Muslims, however, researchers have linked the group to the Russian state. • Campaigns by the group, have included targeting Europe, the US, the Middle East, and the Gulf States, attacks have been across sectors and involved numerous campaigns
VSec	@lulzchat	Dec 2023	1000+	• This is a public channel of the LulzSec group. • The group is mainly involved in DDoS attacks.

Cyber Army Russia Reborn	@CyberArmyofRussia_Reborn	Apr 2022	52,000+	- This is the pro-Russian group and is mainly involved in DDoS, website defacement, and data breach attacks. - The group is highly active during the Russia-Ukraine war.
Cyber Dragon	@CyberDragon	Sep 2023	1300+	- This is the pro-Russian group and is mainly involved in DDoS, website defacement, and data breach attacks.

The following screenshots highlight notable attacks on France-based organizations by these hacktivist groups over the past year.



Team Anon Force

#OP_France

http://lelivrevivant.fr/
http://lesterresdekhairyaca.fr/
https://marchimmo.fr/
https://musicfamily.fr/
https://my-vitrier.fr/
https://my-serrurier.fr/
https://www.natuphyt.fr/index.html
https://nicolasdemade.fr/
http://olivier-pottier.fr/
http://optique.relais-mairie.fr/
https://osmotech.fr/
https://ottproparis.fr/
https://patrick-richard.fr/
https://perigord-locations-services.fr/
https://phoneordi.fr/
http://plan-z.fr/
http://planilev.fr/
https://poz-formation.fr/
https://prcpcolomiers.fr/
https://pre-box.fr/
http://proxyma-systemes.fr/
https://reparation-volet-roulant-93.fr/
https://restolescancres.fr/
https://site-pme.fr/
https://soinspiree.fr/
https://source-ressources.realid-virtuelle.fr/
https://studiogina.fr/
https://tcmp26.fr/
https://teits.fr/
https://tennisclubpommiers.fr/
https://hellcorp.fr/
https://tribouillois-vincent.fr/
https://valoryss.com/
https://visiter-prague.fr/
https://visite-lisbonne.fr/
https://site-pme.fr/
https://animaux-selection.fr/
http://studiosolidaire.fr//wp-content/plugins/
http://bergersaustralien.com/
https://lesmeilleursvoyages.fr/
https://meilleur-maquillage.fr/
https://meilleures-glaces.fr/
https://meilleures-recettes-de-cuisine.fr/
https://meilleurs-ustensiles-de-cuisine.fr/
https://mon-mariage-reussi.com/
http://topanimaux.fr/
https://univers-rugby.com/

Mirror: https://mirror-h.org/search/hacker/64599/

#OP_France
#Team_Anon_Force
#Khan_Cyber_Army
#MTB
#Team_insane_Pk
#Team_Herox
#Team1919
#BADS_Community
#TEAM_TEX_CYBER
#TEAMDARKNOORAGENTS
#ALL_MUSLIM_Hackers

IRoX Team - Elite Hackers

IRoX Team France Website Hacked for supporting Israeli Jews

https://ospicy.fr
https://foodcitytriolo.fr
https://en-k.fr
https://fastburger-lens.fr
https://laformule-marcqenbaroeul.fr
https://lequattro-restaurant.fr
https://originalbestburger-armentieres.fr
https://tacosway.fr

We always stand by our Palestinian Muslim brothers.

Join Us @IRoX_Team

ospicy.fr
Hacked by IRoX Team

t.me/IRoX_Team/94 3.6K edited Oct 28, 2023 at 21:49

Türk Hack Team

La Poste pannes signalées au cours des dernières 24 heures

Error 503 Backend fetch

Our cyber attack on France's largest postal service, La Poste, continues. 🔥

Currently, vending machines, websites and infrastructures are not working. ❌

We will explode your critical infrastructures and online services. 🎯

Our hitting power will increase with intensity. I think it would be better if you get additional protection. 🤫

#OpFrance 🇫🇷

We Are Turk Hack Team 🇹🇷

t.me/turkhckteam/303 1.3K Feb 6 at 14:39

NoName057(16) Eng

Przepraszamy

By the way, here recently, Deputy Foreign Minister of Poland Pavel Yablonsky said that his country would also boycott the Olympics in Paris if Russian and Belarusian athletes were admitted. For this, we decided to crash the site of the Polish tax office, which, after our attack, cowardly hid under the stub about the unavailability of the resource😁:

❌https://check-host.net/check-report/e8ebf24kfa5

👉Subscribe to NoName057(16)
🐻Join our DDoS-project
⚠️Subscribe to reserve channel

🇷🇺Victory will be ours!

t.me/noname05716eng/572 291 Feb 7, 2023 at 17:00

Türk Hack Team

GOUVERNEMENT
Liberté
Égalité
Fraternité

France Visa Passport Official Website Downed By Turkish Hack Team

Target: france-visas.gouv.fr/en

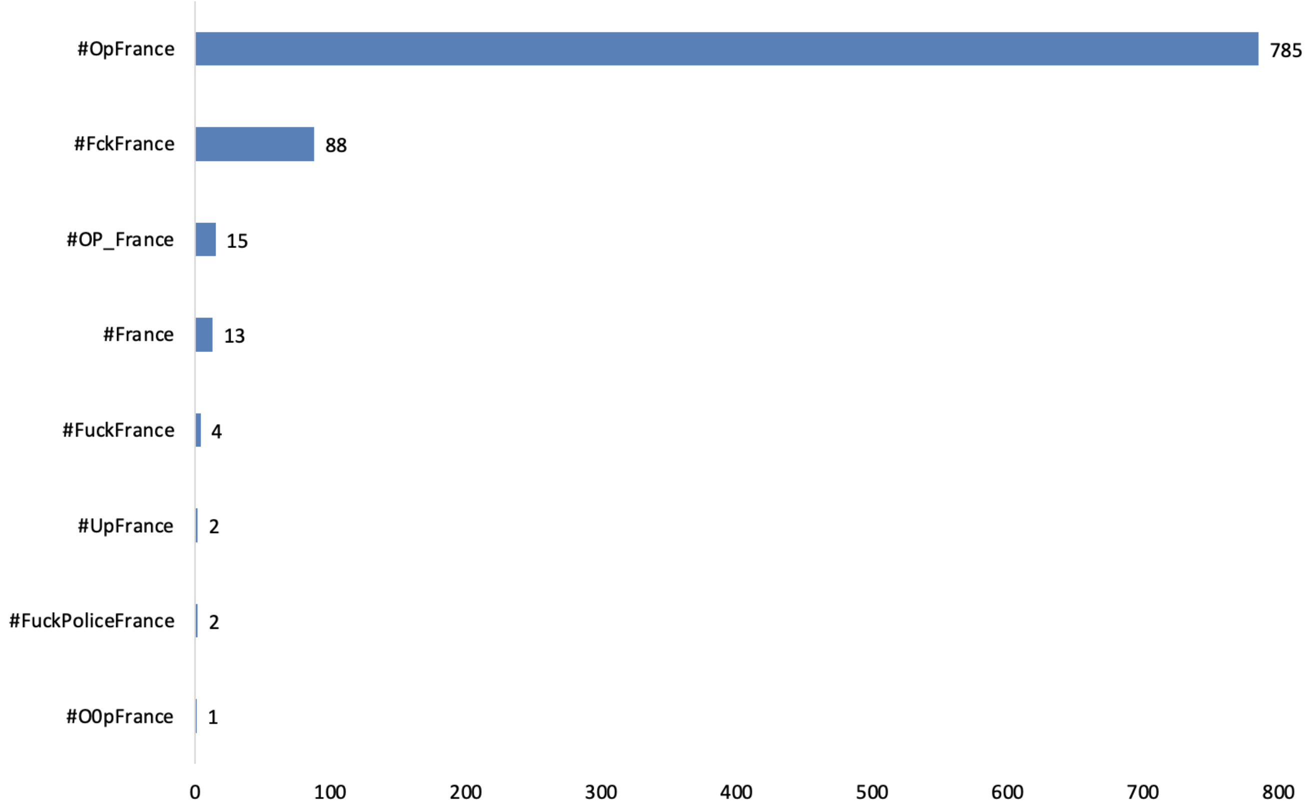
Check-Host: check-host.net/check-report/105c106fkf3c

Botnet, Malware, Phishing, Ransomware, News, Exploit, Tool, DDoS, Cyber Attack

t.me/turkhckteam/170 1.0K Jun 22, 2023 at 22:44

(DDoS/Defacements messages on Telegram channels)

The graphs below denote various hashtags used by hacktivist groups to target French entities over a year span.



(Hashtags used by Hacktivist Groups to target France 2023-2024 (Till date)

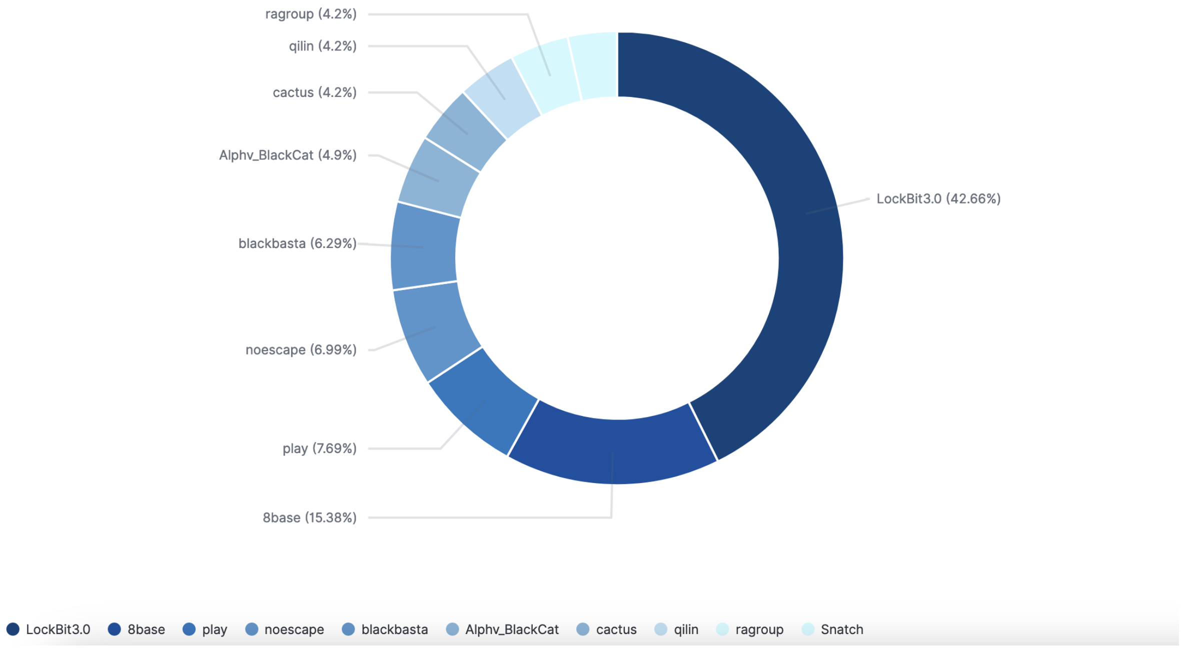
Ransomware Attacks Targeting France

As the Paris 2024 Olympics approaches, the threat of ransomware attacks raises concerns about the preparations and operations of the event.

Ransomware attacks involve cybercriminals infiltrating an organization's network, encrypting valuable data, and demanding a ransom payment in exchange for the decryption key. These attacks can impact an organization's ability to access critical information and systems, leading to operational failure and significant financial losses. Ransomware attacks have become one of the most prevalent and damaging forms of cyber threats in recent years. These attacks involve malicious software that encrypts a victim's data, rendering it inaccessible until a ransom is paid to the attackers. The impact of ransomware attacks on daily operations can be profound, affecting various aspects of an organization's functionality and overall stability.

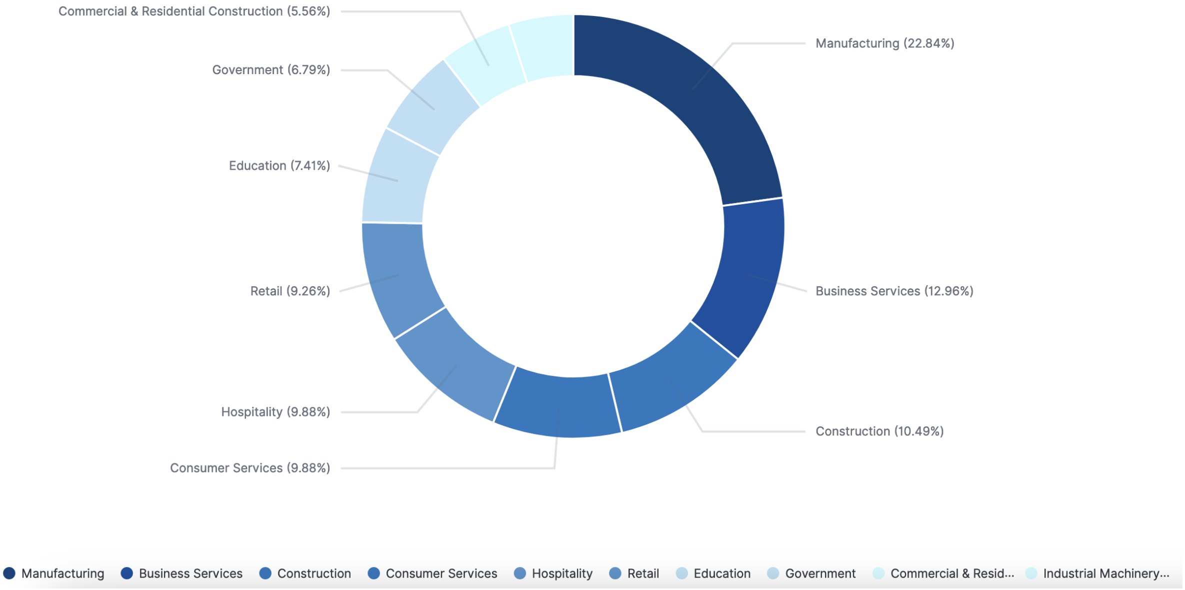
These ransomware groups tend to target and disrupt the organizations that support the Paris Olympics. These ransomware groups might attack and encrypt data, making it inaccessible and creating chaos due to the unavailability of critical information.

Additionally, data from the past year - till date indicates that Lockbit ransomware is the most active in targeting France-based entities, followed by the 8base and Play ransomware groups.



(Top ransomware groups targeting France-based entities)

In terms of industries, the manufacturing sector has been the most targeted, followed by business services and consulting organizations.



(Top targeted sectors by ransomware groups)

Phishing & Fraud Activities Targeting Paris 2024

UK Finance highlighted a surge in online scams, particularly involving fake Olympics and Taylor Swift tickets. Although overall fraud losses decreased slightly, victims lost £1.17 billion in 2023. Purchase scams increased by 28%, resulting in £86 million in losses from non-existent goods. The report emphasized the need for improved platform security by tech companies. In April 2024, Lloyds Bank disclosed that fans of Taylor Swift collectively lost £1 million to fraudulent ticket sales before her UK tour starting in July. More than 600 customers reported financial losses.

The following sections will provide a detailed analysis of phishing and fraudulent activities especially those associated with ticketing scams.

Typosquatting in Action

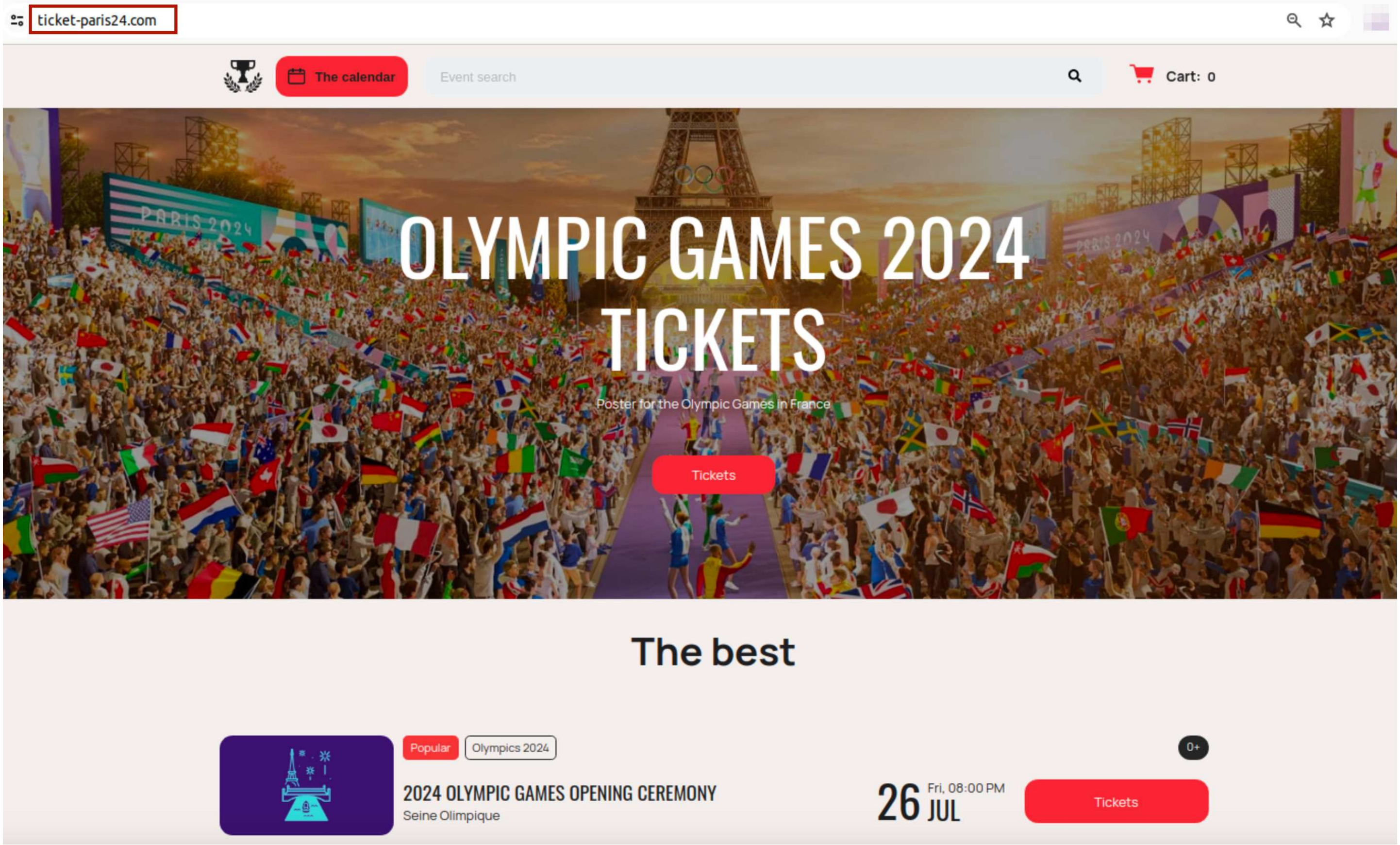
Typosquatting is a type of cyberattack where attackers register domain names that are similar to legitimate websites, often involving common misspellings or typographical errors. For example, they might register a domain like "olympics2024[.]com," which is similar to the original website "olympics[.]com." These fraudulent sites are designed to trick users into visiting them, believing they are on a legitimate website. These domains are often used for phishing attacks, defrauding website visitors, and malware distribution among others.

FortiGuard Threat Research has identified over 100+ domain names registered in the past six months mimicking the Paris Olympics event. Although there is no current evidence of these domains being used in any campaigns, they remain available for potential misuse. The following is the list of the identified potential typosquat domains registered:

Domain Name	Registrar	Registration Date
2024parisolympicathletes.com	GoDaddy.com, LLC	19-Jun-24
parisolympicsrosters.com	NameCheap, Inc.	17-Jun-24
olympicsg.com	Domain Science Kutatasi Szolgaltato Korlatolt Felelossegu Tarsasag	04-Jun-24
paris-olympics2024.com	GoDaddy.com, LLC	28-May-24
oympics.com	Dynadot Inc	22-May-24
olympcs.com	Dynadot Inc	22-May-24
olympic-bets-paris-2024.com	OVH sas	21-May-24
olympicgamesparisfr.com	NameCheap, Inc.	18-May-24
olympycs.com	IONOS SE	17-May-24
parisolympicshop.com	Tucows Domains Inc.	09-May-24

Note: The table contains only 10 recently registered domains. Please find the entire list of domains here.

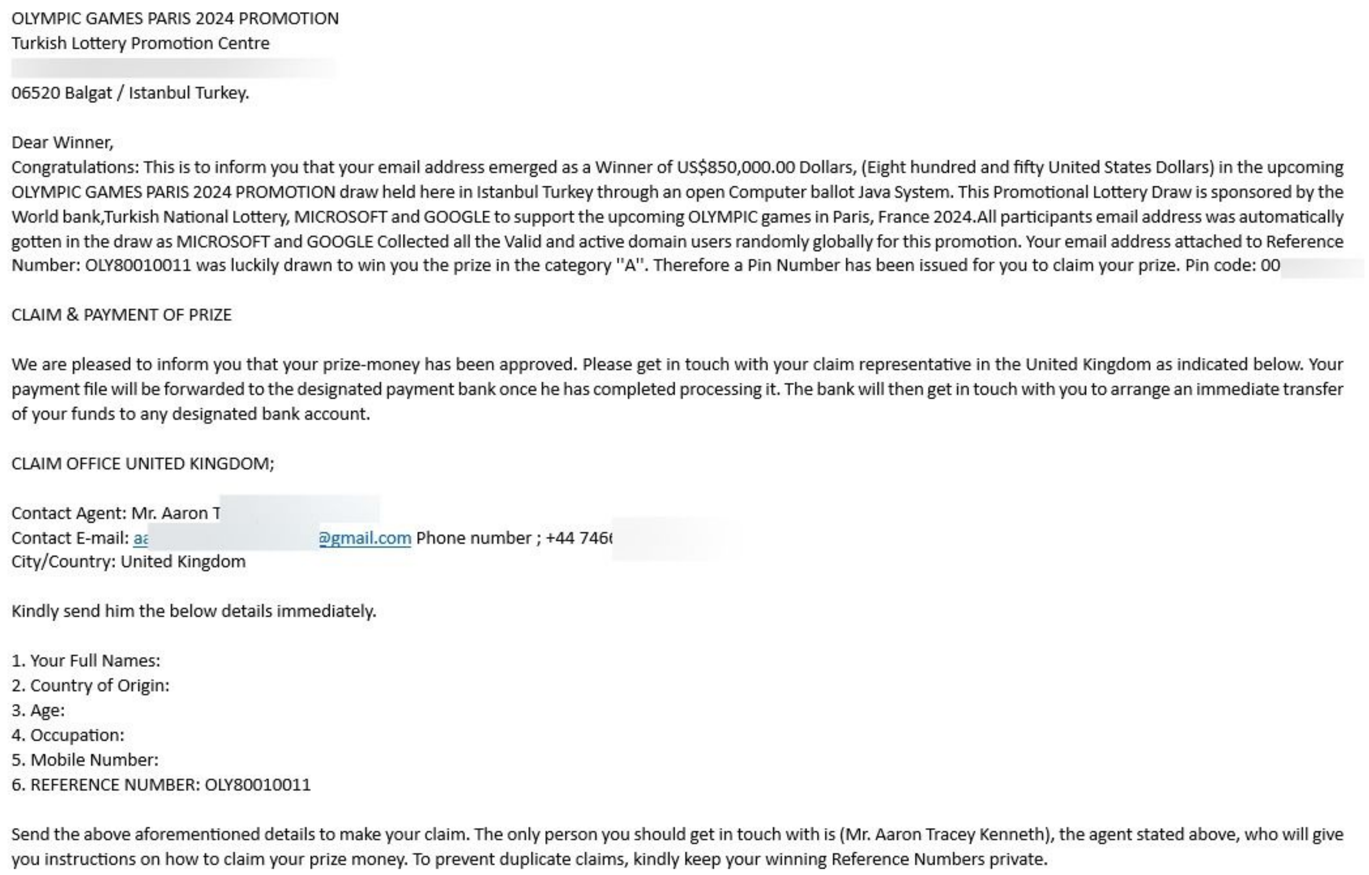
One such fraudulent website is ticket-paris24[.]com, which impersonates the legitimate Paris ticketing website (tickets.paris2024.org). Below is the attached screenshot of the fraudulent website.



(Fraudulent website impersonating the original Paris ticketing site)

Phishing in Action

A few weeks before the launch of the Paris 2024 Games, researchers at Bitdefender observed several Olympic Games-themed lottery scams. Cybercriminals are often using the names of national lotteries, financial institutions, and major tech companies to deceive unsuspecting internet users. Brands commonly impersonated in these scams include Coca-Cola, Microsoft, Google, the Turkish National Lottery, and the World Bank. The primary targets for these lottery scams are users in the US, Japan, Germany, France, Australia, the UK, and Slovakia.



OLYMPIC GAMES PARIS 2024 PROMOTION
Turkish Lottery Promotion Centre
[redacted]
06520 Balgat / Istanbul Turkey.

Dear Winner,
Congratulations: This is to inform you that your email address emerged as a Winner of US$850,000.00 Dollars, (Eight hundred and fifty United States Dollars) in the upcoming OLYMPIC GAMES PARIS 2024 PROMOTION draw held here in Istanbul Turkey through an open Computer ballot Java System. This Promotional Lottery Draw is sponsored by the World bank,Turkish National Lottery, MICROSOFT and GOOGLE to support the upcoming OLYMPIC games in Paris, France 2024.All participants email address was automatically gotten in the draw as MICROSOFT and GOOGLE Collected all the Valid and active domain users randomly globally for this promotion. Your email address attached to Reference Number: OLY80010011 was luckily drawn to win you the prize in the category ''A''. Therefore a Pin Number has been issued for you to claim your prize. Pin code: 00[redacted]

CLAIM & PAYMENT OF PRIZE

We are pleased to inform you that your prize-money has been approved. Please get in touch with your claim representative in the United Kingdom as indicated below. Your payment file will be forwarded to the designated payment bank once he has completed processing it. The bank will then get in touch with you to arrange an immediate transfer of your funds to any designated bank account.

CLAIM OFFICE UNITED KINGDOM;

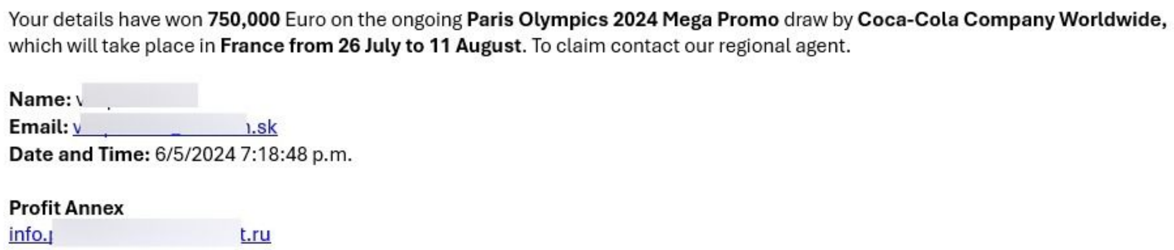
Contact Agent: Mr. Aaron T[redacted]
Contact E-mail: a[redacted]@gmail.com Phone number ; +44 746[redacted]
City/Country: United Kingdom

Kindly send him the below details immediately.

1. Your Full Names:
2. Country of Origin:
3. Age:
4. Occupation:
5. Mobile Number:
6. REFERENCE NUMBER: OLY80010011

Send the above aforementioned details to make your claim. The only person you should get in touch with is (Mr. Aaron Tracey Kenneth), the agent stated above, who will give you instructions on how to claim your prize money. To prevent duplicate claims, kindly keep your winning Reference Numbers private.

(Olympic Games-themed lottery scam phishing lures example - 1)



Your details have won **750,000** Euro on the ongoing **Paris Olympics 2024 Mega Promo** draw by **Coca-Cola Company Worldwide,** which will take place in **France from 26 July to 11 August**. To claim contact our regional agent.

Name: v[redacted]
Email: v[redacted].sk
Date and Time: 6/5/2024 7:18:48 p.m.

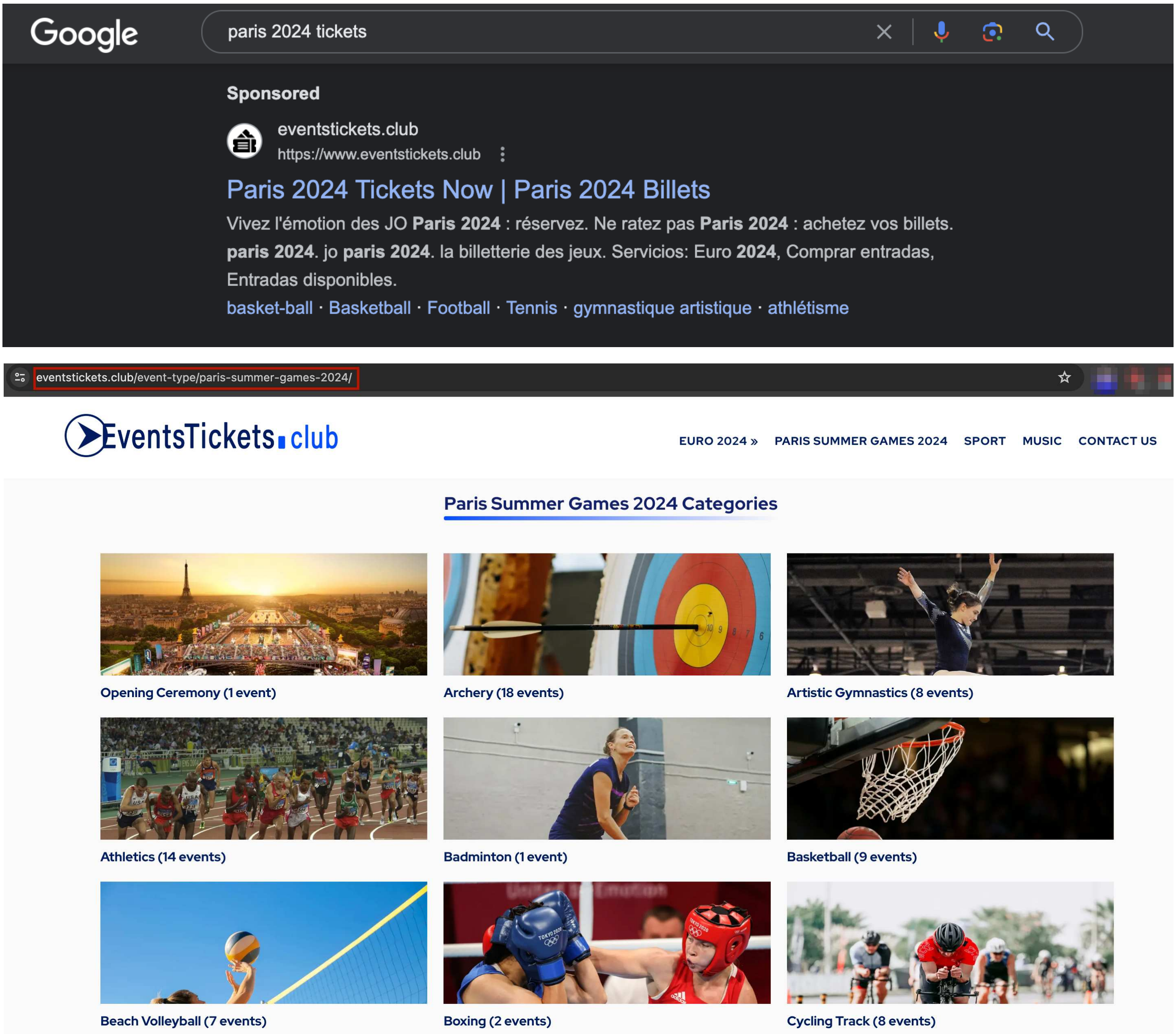
Profit Annex
info.[redacted]t.ru

(Olympic Games-themed lottery scam phishing lures example - 2)
(Image source: Bitdefender)

Ticketing Fraud in Action

In collaboration with Olympic partners, the French Gendarmerie Nationale has identified 338 fraudulent websites claiming to sell Olympic tickets. According to their data, 51 of these sites have been shut down, and 140 have received formal notices from law enforcement.

We have discovered one of such fraudulent sites appearing in the sponsored search results on Google. The website claims to be "a secondary marketplace for tickets to live events."



Google

paris 2024 tickets

Sponsored

eventstickets.club
https://www.eventstickets.club

Paris 2024 Tickets Now | Paris 2024 Billets

Vivez l'émotion des JO **Paris 2024** : réservez. Ne ratez pas **Paris 2024** : achetez vos billets. **paris 2024**. jo **paris 2024**. la billetterie des jeux. Servicios: Euro **2024**, Comprar entradas, Entradas disponibles.

basket-ball · Basketball · Football · Tennis · gymnastique artistique · athlétisme

eventstickets.club/event-type/paris-summer-games-2024/

EventsTickets.club

EURO 2024 » PARIS SUMMER GAMES 2024 SPORT MUSIC CONTACT US

Paris Summer Games 2024 Categories

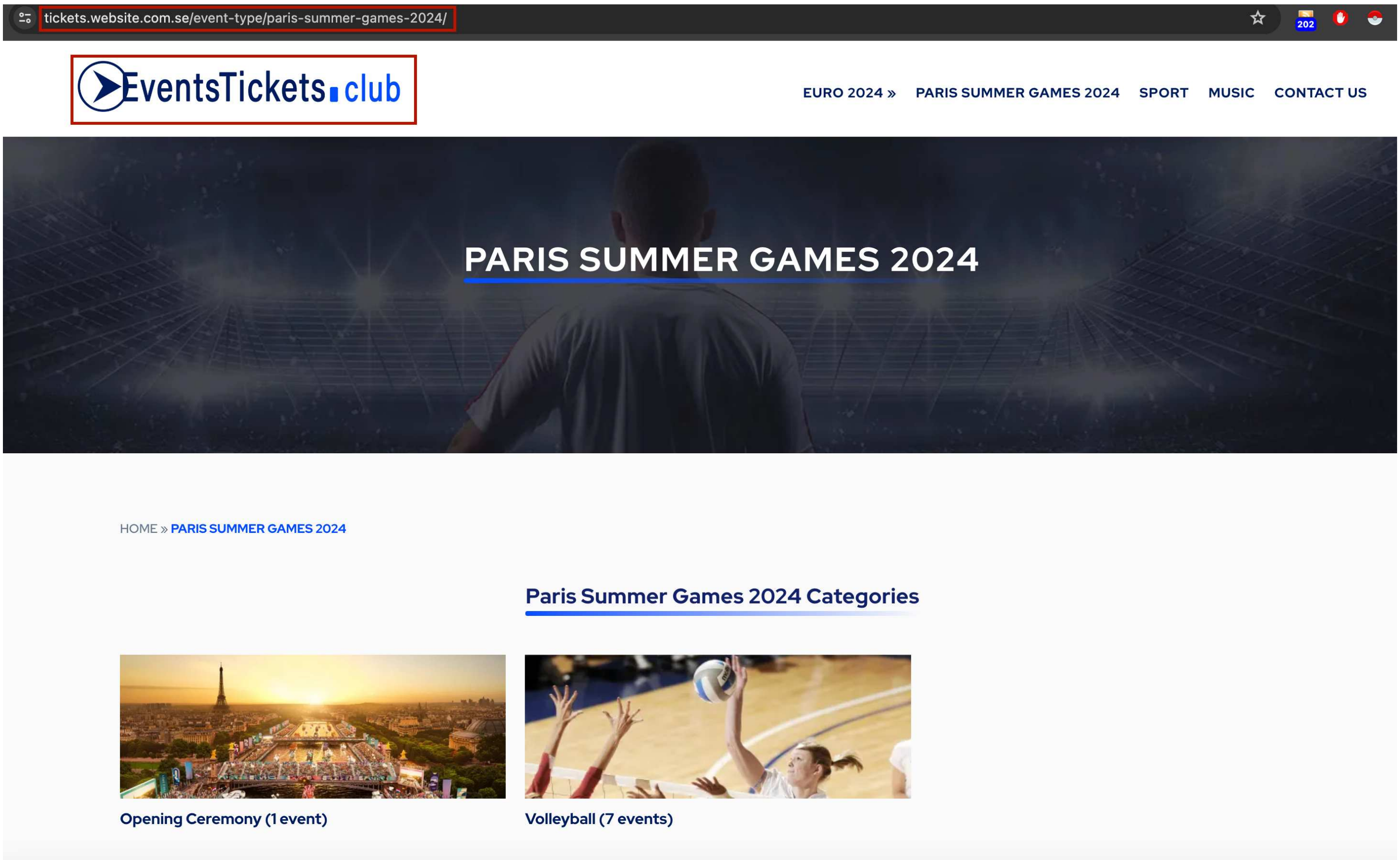
- Opening Ceremony (1 event)
- Archery (18 events)
- Artistic Gymnastics (8 events)
- Athletics (14 events)
- Badminton (1 event)
- Basketball (9 events)
- Beach Volleyball (7 events)
- Boxing (2 events)
- Cycling Track (8 events)

(Fraudulent sites impersonating the Paris Olympics 2024 appearing in the sponsored search results on Google)

Whois Details of **eventstickets[.]club**:

Registered	4th January 2024
Registrar	GoDaddy.com, LLC
Registrant Name	REDACTED FOR PRIVACY
Country	United States
IP Address	93.113.111[.]10
Hosting Provider	NetConnex Broadband Ltd.

We also have identified an identical website with a different domain name which could be operating by the same individual.



tickets.website.com.se/event-type/paris-summer-games-2024/

PARIS SUMMER GAMES 2024

HOME » PARIS SUMMER GAMES 2024

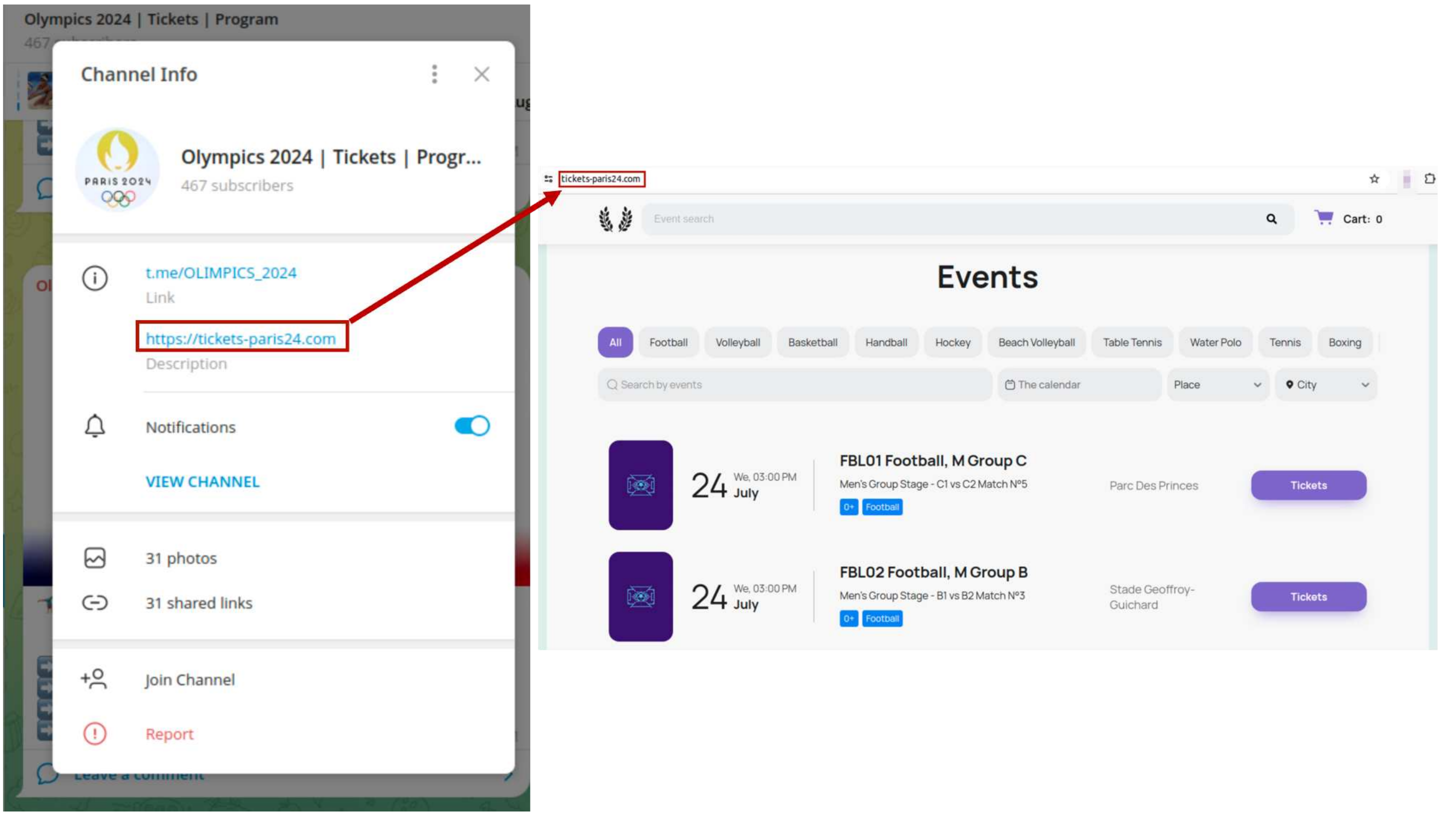
Paris Summer Games 2024 Categories

(Fraudulent websites impersonating the Paris Olympics 2024)

Whois Details of (**tickets[.]website[.]com.se)**:

Registered	1st July 2020
Registrar	Namecheap
Registrant Name	REDACTED FOR PRIVACY
Country	United States
IP Address	172.66.45[.]12 (Cloudflare) 172.66.46[.]244 (Cloudflare)

While analyzing these malicious activities, we made an interesting discovery of a recently created Telegram channel (https://t[.]me/OLIMPICS_2024) possibly being used to disseminate fraudulent websites. In the bio of this Telegram channel, we identified a fake website (tickets-paris24[.]com) designed to mimic the official Paris ticketing website.


Olympics 2024 | Tickets | Program

Channel Info

Olympics 2024 | Tickets | Progr...

467 subscribers

t.me/OLIMPICS_2024

Link

https://tickets-paris24.com

Description

31 photos

31 shared links

tickets-paris24.com

Events

24 We, 03:00 PM July	FBL01 Football, M Group C Men's Group Stage - C1 vs C2 Match N°5 0+ Football	Parc Des Princes	Tickets
24 We, 03:00 PM July	FBL02 Football, M Group B Men's Group Stage - B1 vs B2 Match N°3 0+ Football	Stade Geoffroy-Guichard	Tickets

(A fraudulent website impersonating the Paris 2024 appeared on Telegram)

Upon further analysis, we identified that both the domains **tickets-paris24[.]com** and **ticket-paris24[.]com** are pointing to the same IP address - **179.43.166[.]54**. Below are the WHOIS details and graphical representation.

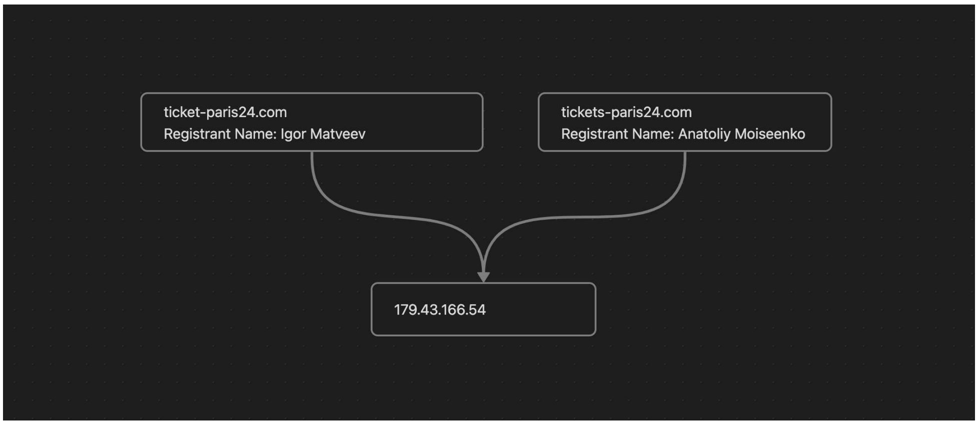
- Domain 1: tickets-paris24[.]com
- Domain 2: ticket-paris24[.]com
- IP Address: 179.43.166[.]54

Whois Details of (tickets-paris24.com):

Registered	9th March 2023
Registrar	Name.com, Inc.
Registrant Name	Anatoliy Moiseenko
Country	Russian Federation
IP Address	179.43.166[.]54
Hosting Provider	Private Layer INC

Whois Details of (ticket-paris24.com):

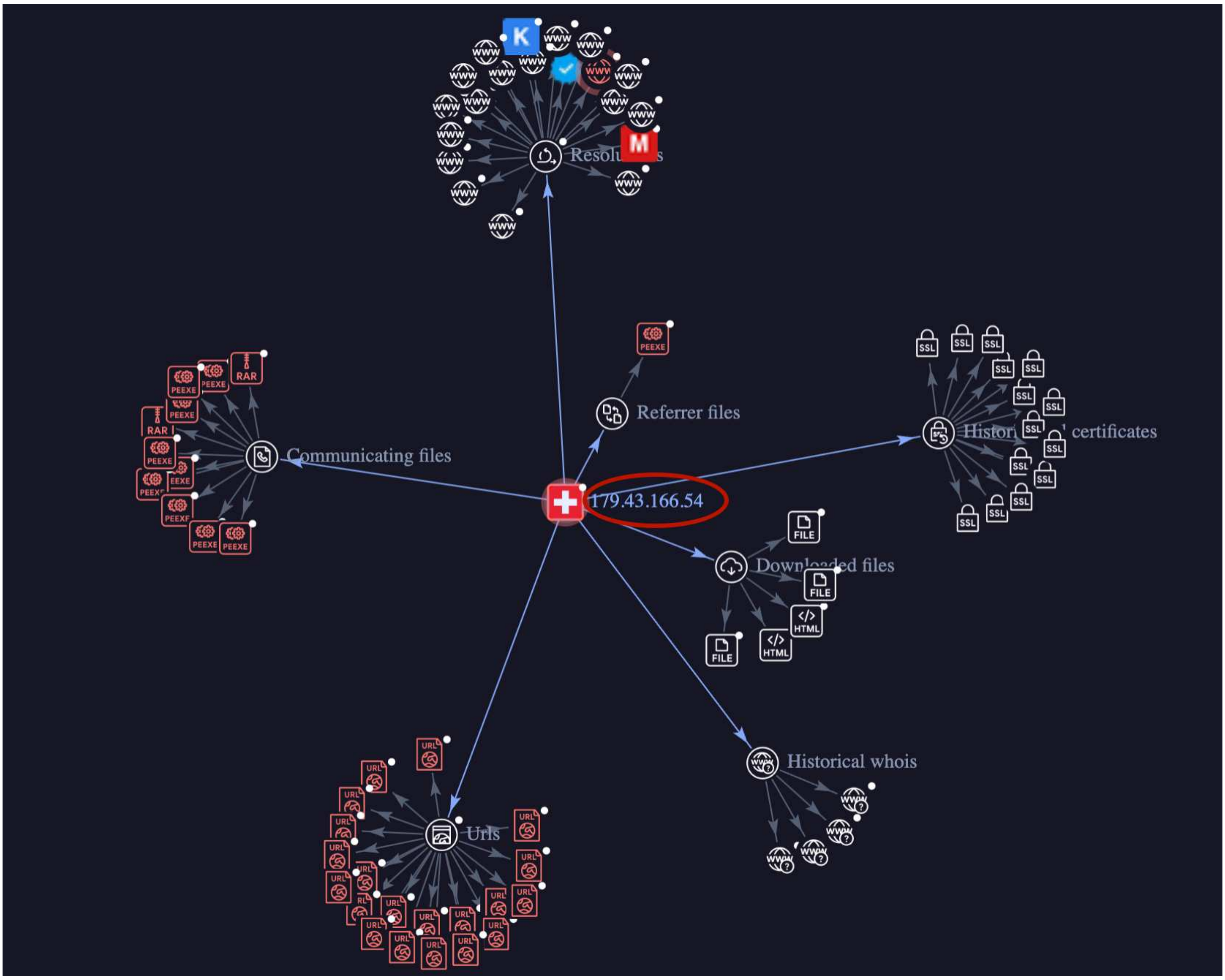
Registered	22nd February 2024
Registrar	Name.com, Inc.
Registrant Name	Igor Matveev
Country	Russian Federation
IP Address	179.43.166[.]54
Hosting Provider	Private Layer INC


ticket-paris24.com
Registrant Name: Igor Matveev
tickets-paris24.com
Registrant Name: Anatoliy Moiseenko
179.43.166.54

(Graphical representation of linkage between the domains)

We also extend our research on the registrant 'Anatoliy Moiseenko', who registered tickets-paris24[.]com, has also registered over 35 domain names through the registrar, name[.]com, impersonating various sporting events from 2023 to 2024.
The other registrant 'Igor Matveev', who registered ticket-paris24[.]com, has also registered 6 other domain names impersonating various sporting events between 2023 and 2024. These domains appear to have been registered with the intent to target upcoming events, as well as domains related to past sporting events. They are actively used to target the ticketing websites associated with these events.

An analysis of the IP address (179.43.166[.]54) using a public file scanning service indicates that this IP is known for malicious activities, which have been flagged by various antivirus engines.



(Malicious files communicating with the IP address. Image source: VirusTotal)

Anticipated Threats to Paris Olympics 2024

The Paris Olympics 2024 represents not only a celebration of global athleticism but also a high-stakes target for a myriad of cyber threats. As one of the world's most prominent events, the Olympics draws attention from cybercriminals, hacktivists, and state-sponsored actors alike, presenting significant challenges in safeguarding its infrastructure, participants, and spectators.

Cyber espionage poses a significant threat as adversaries aim to steal sensitive data related to broadcasting rights, sponsorships, and technological innovations. Intellectual property theft poses risks not only to competitive edge but also to national security and diplomatic relations. Additionally, groups such as Storm-1679 and Storm-1099 have escalated their disinformation campaigns against the Paris Olympics to manipulate public perception, sow discord, and destabilize the international event.

Cybercriminals leverage phishing scams and fraudulent schemes to exploit unsuspecting participants and spectators. Fake ticketing platforms, fraudulent merchandise, and identity theft tactics threaten financial loss and undermine public trust in event-related transactions.

The Paris Olympics 2024, due to France's political stances and international influence, are a prime target for various politically motivated groups. We anticipate that hacktivist groups will likely attack entities associated with the Paris Olympics to disrupt the event. These groups may target infrastructure, media channels, and affiliated organizations to disrupt event proceedings, undermine credibility, and amplify their messages on a global stage.

The pervasive threat of ransomware continues to evolve, with potential consequences ranging from financial extortion to operational paralysis. Attacks on critical infrastructure and supporting organizations could severely impact event logistics, spectator experience, and international perception.

Recommendations & Mitigation Strategies

FortiGuard Threat Research recommends the following best security practices to safeguard against cyber-attacks. By prioritizing cybersecurity, the Paris Olympics 2024 can safeguard the integrity of the Games, ensuring a safe and secure environment for all participants and spectators.

- Employee Training and Awareness: Conduct regular training sessions to highlight the risks of Olympics-related social engineering lures in the runup to and during the Games. Focus on recognizing deceptive emails and fake websites, and emphasize the importance of reporting suspicious activities promptly.

- Travel-related Cyber Threats: Organizations and individuals attending the Games should be aware of travel-related cyber threats, including the increased likelihood of public Wi-Fi interception, fraudulent activities linked to Olympics-related events, and targeted attacks against VIPs, such as government officials, senior executives, and key decision-makers.

- Public Awareness Campaigns: Launch comprehensive public awareness campaigns to educate attendees and participants about cybersecurity threats. Guide identifying phishing attempts, avoiding suspicious links, and reporting potential threats to designated authorities.

- Protect Sensitive Data: Utilize Security Orchestration, Automation, and Response (SOAR) tools to promptly detect and respond to unusual activities. Maintain encrypted backups of critical data stored securely offline to mitigate the impact of ransomware attacks.

- Monitor External Attack Surface: Continuously monitor and assess the IT infrastructure's external attack surface to identify vulnerabilities and potential risks. Implement measures to secure remote desktop protocol (RDP) access and prevent exploitation of web server misconfigurations.

- Enforce Multi-Factor Authentication and Strong Password Policies: Implement multi-factor authentication (MFA) across all systems and enforce a robust password policy. Monitor darknet channels for compromised credentials to proactively protect organizational portals.

- Endpoint Protection: Deploy antivirus and antimalware software on all devices to detect and mitigate phishing attempts and malware infections. Regularly update patches to safeguard against known vulnerabilities.

- Patch Management: Maintain up-to-date software and operating systems by promptly applying security patches. Prioritize critical vulnerabilities that could lead to remote code execution or denial-of-service attacks.

- DDoS Protection: Safeguard infrastructure with multi-layered DDoS prevention solutions, including firewalls, VPNs, and anti-spam filters. Monitor network traffic for anomalies that may indicate DDoS attacks and take preemptive actions.

- Preventing Ransomware Attacks: Implement proactive measures such as regular software updates, secure offline backups, and user education to prevent ransomware incidents. Utilize threat intelligence to monitor darknet activities for potential threats and data leaks.

- Website Defacement Prevention: Deploy Web Application Firewalls (WAFs) to filter and block malicious traffic, protecting against website defacement and unauthorized access attempts.

- Threat Hunting and Response: Conduct robust threat-hunting activities based on compromised account information. Isolate infected systems promptly and perform system reimaging as necessary to mitigate threats.

- Cyber Threat Intelligence (CTI): Utilize CTI to gather real-time data on emerging cyber threats and potential risks. Monitor darknet chatter for early indicators of cyber-attacks and data leaks to enable proactive incident response

Appendix A : Reliability Rating Criterion

FortiGuard Threat Research's Reliability rating is based upon the Admiralty System which is internationally accepted method for evaluating collected items of intelligence. The system comprises a two-character notation assessing the reliability of the source and the assessed level of confidence on the information.

Reliability of Source

A source is assessed for reliability based on a technical assessment of its capability, or in the case of Human Intelligence sources their history. Notation uses Alpha coding, A-F:

A	Reliable	No doubt about the source's authenticity, trustworthiness, or competency. History of complete reliability.
B	Usually reliable	Minor doubts. History of mostly valid information.
C	Fairly reliable	Doubts. Provided valid information in the past.
D	Not usually reliable	Significant doubts. Provided valid information in the past.
E	Unreliable	Lacks authenticity, trustworthiness, and competency. History of invalid information.
F	Cannot be judged	Insufficient information to evaluate reliability. May or may not be reliable.

Reliability of Information

An item is assessed for credibility based on likelihood and levels of corroboration by other sources. Notation uses a numeric code, 1-6.

1	Reliable	Logical, consistent with other relevant information, confirmed by independent sources.
2	Usually reliable	Logical, consistent with other relevant information, not confirmed.
3	Fairly reliable	Reasonably logical, agrees with some relevant information, not confirmed.
4	Not usually reliable	Not logical but possible, no other information on the subject, not confirmed.
5	Unreliable	Not logical, contradicted by other relevant information.
6	Cannot be judged	The validity of the information cannot be determined.

Appendix B : Relevance Rating Criterion

High

The Intelligence Report could be flagged with "High" Relevance under below criteria,

- Threat Actor leaked or selling data pertaining to the customer organization in Public/Private Forum.
- Threat Actor mentioned about customer organization in a Public/Private Forum
- Public reporting on Organization was targeted.
- Customer technology/product involved in an attack or being targeted.
- Potential reputation harm to customer brand.
- Customer related domains Typo-squat Fraudulent domains registered.
- Proprietary customer related data found on internet. (Ex: GitHub containing source code)
- Customer related domain email addresses found to be part of a data breach.
- Customer specific keywords match identified across FortiGuard Threat Research's produced Intelligence.

Medium

The Intelligence Report could be flagged with "Medium" Relevance under below criteria,

- Identification of Threat Actor targeting related Industry.
- Vulnerability disclosed Potentially impacting Organization.
- Public/Private breaches or incidents relating the organization's sector.
- Public/Private Incident identified is Unique and Provides insights into new TTPs.

Low

The Intelligence Report could be flagged with "Low" Relevance under below criteria,

- Public/Private Incident identified targeting non Customer specific industry.
- Public/Private Incident identified outside of Customer geography vertical.
- Public/Private Incident gaining significant Media Attention.
- Data breaches or exposed data potentially impacting customer organization.

Appendix C : TLP Criterion

TLP provides a simple and intuitive schema for indicating when and how sensitive information can be shared.

TLP Level	How may it be shared ?
TLP : Red Not for disclosure, restricted to FortiGuard Threat Research and it's customers who need to know the information.	Recipients may not share TLP:RED information with any parties outside of the organization. The information could only be shared within the organization and should be restricted to the ones who needs to know the information.
TLP : Amber Limited disclosure, restricted to FortiGuard Threat Research's customer organization	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm.
TLP : Green Limited disclosure, restricted to the community.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community.
TLP : White Disclosure is not limited.	TLP:WHITE information may be distributed without restriction