

SEKTÖREL RAPOR 2024



YILIN İLK
YARISINDA
HAVACILIK
SEKTÖRÜNE
YÖNELİK
SALDIRILAR

 @echocti

 @echocti

 echocti.com

İçerik

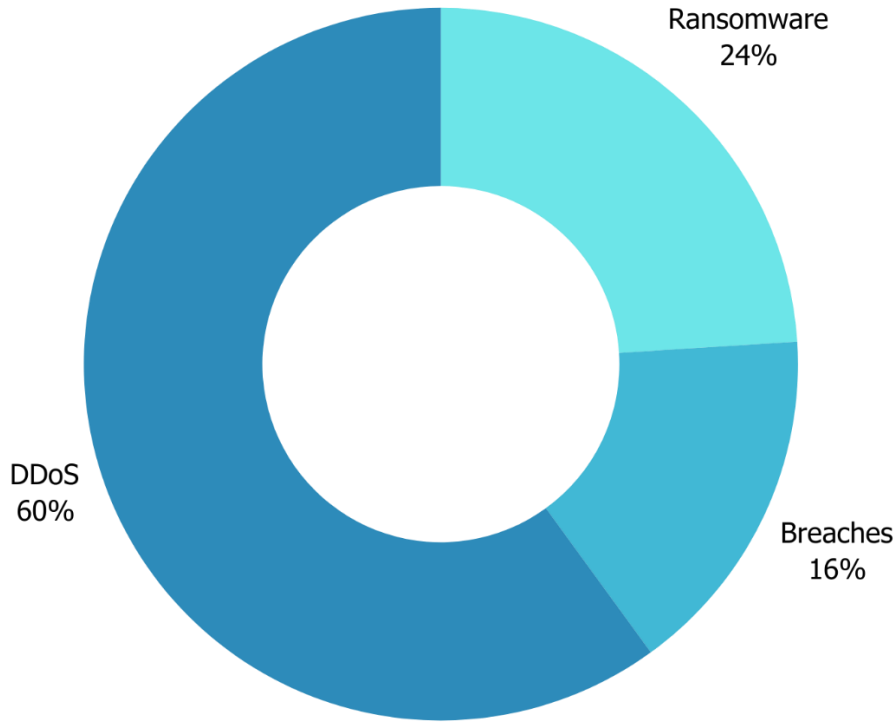
Yönetici Özeti	2
Fidye Yazılımı Saldırıları	3
Continental Aerospace Technologies PLAY Fidye Yazılımının Kurbanı Oldu	3
Saudia MRO 8BASE Fidye Yazılımının Kurbanı Oldu	4
Air Albania LockBit Fidye Yazılımı Grubunun Saldırısına Maruz Kaldı.....	5
Aerospace LockBit Fidye Yazılımı Saldırısına Uğradı.....	6
Veri Sızıntıları	7
Ghost Princess Siber Tehdit Grubu ABD'nin Havacılık Sektörünü Hedef Aldı.....	7
Qatar Airways Verilerinin R00TK1T ISC Siber Ekibi Tarafından Sızdırıldığı İddiası	8
SilitNetwork RwandAir Ltd'yi Hedefliyor	9
'Host Kill Crew Hackers' Kamboçya Angkor Air'i Hedef Aldı	10
DDoS Saldırıları.....	11
Tehdit Aktörü NoName057(16) Avrupa'daki Kritik Önemdeki Havalimanlarını Hedef Aldı.....	11
Tehdit Aktörü HackNet, Diğer Aktör ile Birlikte Güney Kore'nin En Büyük Havalimanı İşletmeleri'nden Incheon Airport'u Hedef Aldı.....	12
Tehdit Aktörü Народная CyberАрмия Bulgaristan Havacılık Sektörünü Hedef Aldıklarını İddia Etti	13
Tehdit Aktörü Dark Strom Team Fransa Havacılık Sektörünü Hedef Aldı	14
Tehdit Aktörü Anonymous Arabia Ürdün Havacılık Sektörünü Hedef Aldı.....	15
HackNeT İtalya Havacılık Sektörünü Hedef Aldı	16
Anonymous Collective Siber Tehdit Grubu Mısır Havacılık Sektörünü Hedef Aldı.....	17
Siber Tehdit Grubu UserSec Almanya Havacılık Sektörünü Hedef Aldı	18
PHOENIX İsveç Havacılık Sektörünü Hedef Aldıklarını İddia Ediyor	19
SYLHET GANG-SG Siber Tehdit Grubu Almanya Havacılık Sektörünü Hedef Aldı.....	20
CyberArmyofRussia_Reborn İtalya Havacılık Sektörünü Hedef Aldı	21
Dark Storm Team ABD Havacılık Sektörünü Hedef Aldı.....	22
Dark Strom Ekibinin Los Angeles Havalimanı'na DDOS Saldırısı Gerçekleştirildi	23
Gulf Air Siber Saldırıya Maruz Kaldı.....	24
Mysterious Team Bangladesh Suudi Arabistan Havalimanı Web Sitesini Hedef Aldı	25

Yönetici Özeti

Bu yönetici özeti, havacılık sektörünü hedef alan siber saldırıların önemini ve etkilerini ele almaktadır. Son yıllarda havacılık sektöründe gerçekleşen siber saldırılar, işletmeler için büyük bir tehdit haline gelmiştir. Bu saldırılar, havayolu şirketlerinin veri tabanları, rezervasyon sistemleri, uçuş sistemleri ve hatta hava trafik kontrol sistemleri gibi kritik altyapıları hedeflemektedir.

Havacılık sektörü, siber saldırılara karşı hassas bir hedef konumunda bulunmaktadır. Sektördeki kritik altyapıların ve verilerin korunması, operasyonel süreklilik ve yolcu güvenliği açısından büyük bir önem taşımaktadır. Siber saldırılar, veri hırsızlığı, operasyonel aksamalar, uçuş iptalleri ve hatta uçuş güvenliğinin tehlikeye atılması gibi ciddi sonuçlara yol açabilir.

Siber saldırganlar, sürekli olarak gelişen teknikler ve taktikler kullanarak güvenlik önlemlerini aşmayı hedeflemektedir. Saldırıların arkasında farklı motivasyonlar bulunmaktadır, bunlar arasında mali kazanç sağlama, ulusal güvenlik tehdidi, casusluk faaliyetleri veya siber saldırı yeteneklerini sergileme gibi amaçlar yer almaktadır.



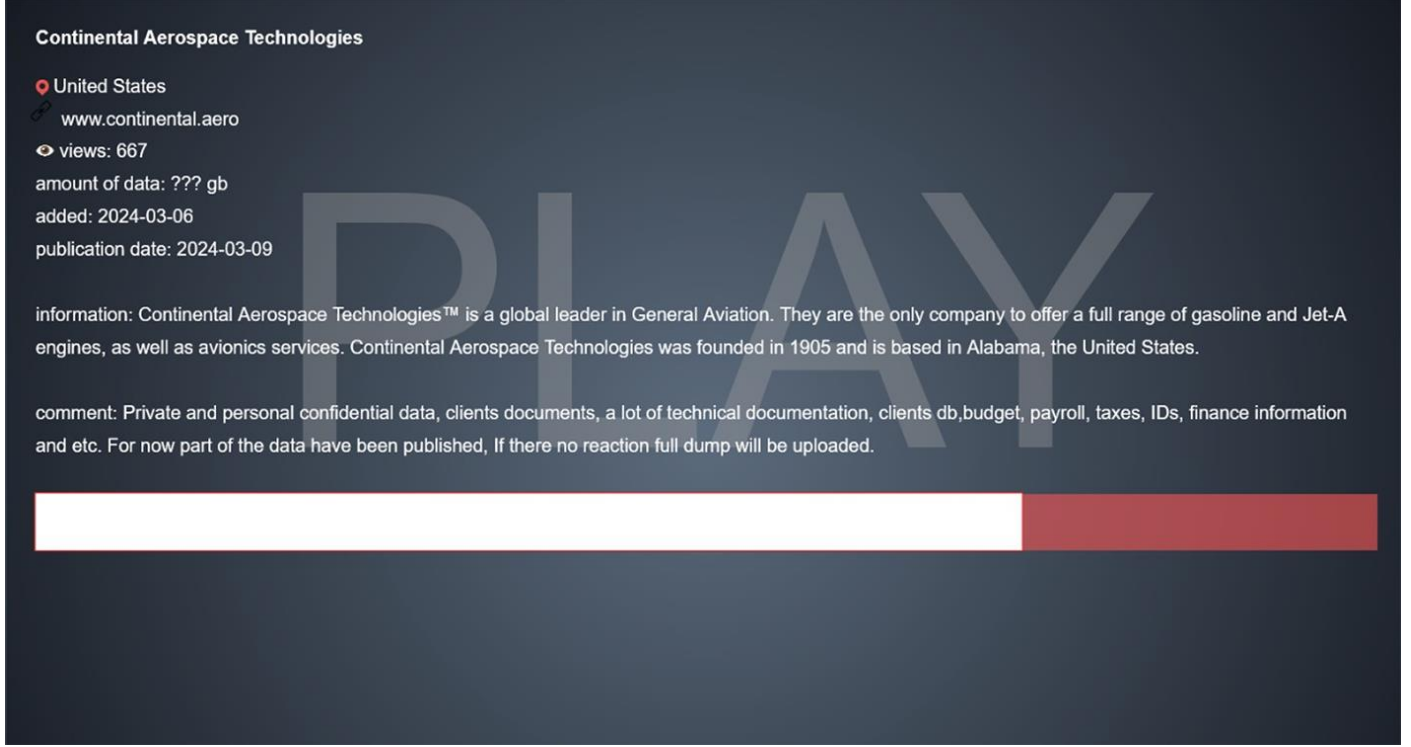
Şekil 1 Types of Attacks on the Aviation Sector

Havacılık sektörü, siber güvenlik konusunda sürekli olarak güncel kalması gereken bir alandır. Gelecekteki tehditlerin önlenmesi için sektör, güvenlik politikalarını sürekli gözden geçirmeli, personel eğitimine yatırım yapmalı ve teknolojik gelişmeleri yakından takip etmelidir.

Bu rapor, havacılık sektöründeki yöneticilerin, siber saldırı tehditlerine karşı bilinçlenmelerine ve gerekli önlemleri alarak şirketlerini korumalarına yardımcı olmayı amaçlamaktadır.

Fidye Yazılımı Saldırıları

Continental Aerospace Technologies PLAY Fidye Yazılımının Kurbanı Oldu



Alabama merkezli uçak motoru üreticisi Continental Aerospace Technologies, PLAY fidye yazılımıyla atfedilen bir siber saldırıya maruz kaldı. PLAY fidye yazılımı, dosyaları şifreleyerek fidye ödenene kadar erişilemez hale getiren sofistike bir kötü amaçlı yazılımdır. Bu saldırılar havacılık ve uzay sektörü için büyük bir tehdit oluştururken, saldırganlar genellikle finansal kazanç amacıyla savunmasızlıklardan yararlanmaktadır. Saldırının kurbanı olan Continental Aerospace Technologies'in ağına kimlik avı e-postaları, ele geçirilmiş yazılım veya güvenlik açıklarından faydalanma yoluyla sızıldığı düşünülmektedir. Saldırganlar, fidye ödeyerek şifre çözme anahtarını elde etmek için kuruluştan bir ödeme talep etmiştir. Bu saldırı, üretim süreçlerini durdurma, fikri mülkiyeti riske atma ve operasyonel verimliliği etkileme potansiyeline sahiptir. Continental Aerospace Technologies, olayı araştırmak, saldırıyı analiz etmek ve gelecekteki saldırılara karşı önlem almak için siber güvenlik uzmanları ve kolluk kuvvetleriyle iş birliği yapmıştır. Bu saldırı, havacılık sektöründe güvenlik değerlendirmelerinin ve önlemlerinin önemini vurgulamaktadır.

Saudia MRO 8BASE Fidyeye Yazılımının Kurbanı Oldu

Saudia MRO

Downloaded: 28.02.2024 Publish: 06.03.2024 views: 13

Proud to be partnered with the national airline of Saudi Arabia, Saudia Technic (formerly SAEI) serves our regional and global clients from a network of more than 100 locations around the globe. Saudia Technic provides end-to-end aircraft maintenance, repair and overhaul solutions. saudiamro.com

Comment:

Were uploaded to the servers:

Invoice

Receipts

Accounting documents

Personal data

Certificates

Employment contracts

A huge amount of confidential information

Confidentiality agreements

Personal files

Other

28 Şubat 2024 tarihinde, Suudi Arabistan Havayolları'nın MRO bölümü olan Saudia Technic, 8BASE fidye yazılımı çetesi tarafından yapılan ciddi bir siber saldırının hedefi oldu. Bu saldırı, havacılık altyapısındaki güvenlik açıklarını vurgulamış ve uçak bakımı ve operasyonel güvenlik üzerinde endişeleri artırmıştır. 8BASE, fidye ödenene kadar dosyalara erişimi engelleyen sofistike bir fidye yazılımıdır. Fidyeye yazılımı saldırıları finansal kazanç amacıyla çeşitli sektörlerdeki kuruluşları hedef almakta ve Boeing'in araştırmasına göre, bu saldırılar %600 oranında artmıştır. Saudia Technic'e yapılan saldırının kuruluşun ağına kimlik avı e-postaları yoluyla 8BASE fidye yazılımının dağıtımını içerdiği düşünülmektedir. Bu saldırının sonucunda kritik bakım ve operasyonel veritabanları, belgeler ve iletişim kanalları tehlikeye girmiştir ve Suudi Arabistan Havayolları hizmetlerinde kesintilere neden olmuştur. Bu saldırı, uçak bakım programlarında, operasyonel planlamada ve iletişim sistemlerinde önemli aksaklıklara yol açmış ve mali ve itibar hasarı meydana getirmiştir. Bu olay, havacılık sektöründe siber güvenliğin kritik önemini vurgulamaktadır.

Air Albania LockBit Fidye Yazılımı Grubunun Saldırısına Maruz Kaldı

lockbit3g3ohd3kataj6zaehxz4h4cnhmz5t735zplywhwpc6oy3id.onion/post/vVoukxvj0jVTWE2v65e37434a664c

LOCKBIT 3.0 **LEAKED DATA** [TWITTER](#) [PRESS ABOUT US](#) [HOW TO BUY BITCOIN](#) [CONTACT US](#) [AFFILIATE RULES](#) [MIRRORS](#)

Deadline: 02 Mar, 2024 20:47:16 UTC

[no logo] **airalbania.com.al**
 Help & Contact. +355 4 224 60 00. customer.care@airalbania.com.al. b2b@airalbania.com.al. groups@airalbania.com.al. 24/7 booking and customer services. Customer Service. You're an email away to become our business partner.

UPLOADED: 02 MAR, 2024 18:47 UTC UPDATED: 02 MAR, 2024 18:47 UTC

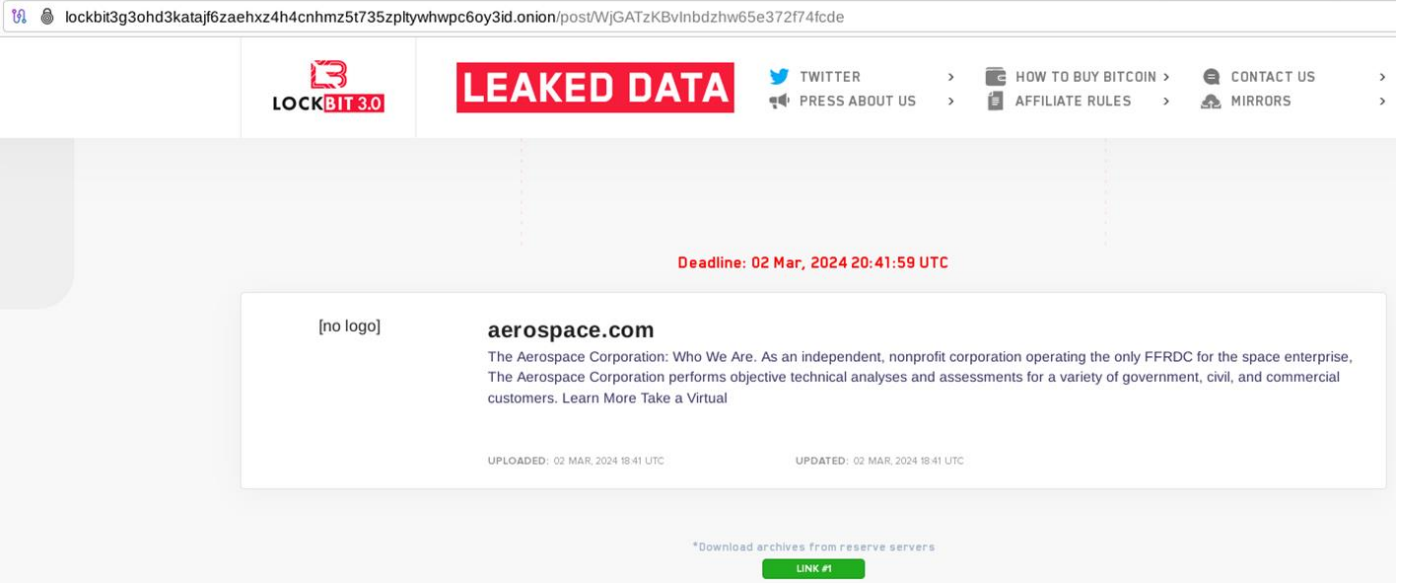
*Download archives from reserve servers

[LINK #1](#)

File Name	Size	Date
Contract & Procurement	-	March 9, 2024
Documentation	-	October 8, 2022
Emails	-	October 8, 2022
Finance	-	October 12, 2022
Flight Data	-	March 9, 2024
Flight Operations	-	October 12, 2022
Ground Operations	-	October 12, 2022
HR	-	October 12, 2022
IT Division	-	October 12, 2022
Management	-	October 6, 2022
Marketing & Sales	-	October 12, 2022
Meeting Minutes	-	October 6, 2022
Office of CEO	-	October 13, 2022
Official Letters	-	October 13, 2022
PAX No	-	October 13, 2022
Personal Folders	-	October 6, 2022
Share	-	October 13, 2022
Share Test	-	October 6, 2022
Training Department	-	October 14, 2022
metasploit-framework	-	October 13, 2022

Arnavutluk'un bayrak taşıyıcı havayolu şirketi Air Albania, LockBit fidye yazılımı grubunun hedefi oldu. Arnavutluk hükümeti, İran destekli tehdit aktörlerinin düzenlediği siber saldırılara karşı son aylarda artan bir şekilde karşı karşıya kaldı. Arnavutluk ve İran arasındaki ilişkiler gergin ve Arnavutluk'un, İran Halkın Mücahitleri (MEK) üyelerine sığınak sağladığı iddialarıyla daha da kötüleşmiştir. LockBit fidye yazılımı çetesi, havacılık sektörünü sık sık hedef almaktadır. Bangkok Airways, E.M.I.T Aviation Consulting ve Kuveyt Havayolları gibi önemli havayolu şirketlerine saldırdılar. Air Albania'nın nasıl ele geçirildiği tam olarak bilinmemekle birlikte, LockBit çetesi, sızdırılan veri setinde bir Metasploit Framework klasörüne işaret etti. Buradan çıkarım yapılarak, tehdit aktörlerinin, birkaç çalışandan ve mevcut dosya paylaşımlarından veri sızdırmak için framework kullandıkları söylenebilmektedir.

Aerospace LockBit Fidye Yazılımı Saldırısına Uğradı



Hindistan'ın Aerospace Laboratories (NAL) adlı büyük havacılık araştırma şirketi, kötü şöhretli fidye yazılım grubu LockBit tarafından saldırıya uğradı. LockBit, NAL'ı karanlık web sızıntı sitesine ekleyerek, kuruluşun verilerini yayınlamakla tehdit etti. Sızan bilgilere göre, LockBit, çalındığı iddia edilen sekiz belgeyi yayınladı, bunlar arasında gizli mektuplar ve bir çalışanın pasaportu da bulunuyor. NAL'ın web sitesi kapalı olduğu için şirket ya da Hindistan siber ajansı CERT-In henüz konuyla ilgili resmi bir açıklama yapmadı. Geçtiğimiz ay, LockBit, Çin Sanayi ve Ticaret Bankası'nın (ICBC) ABD şubesini hedef alarak ABD Hazine piyasasındaki işlemleri aksatmıştı ve bankanın fidye ödediği belirtilmişti. LockBit'in iş modeli, kötü amaçlı yazılımını diğer bilgisayar korsanlarına satmak olan "hizmet olarak fidye yazılımı" olarak biliniyor.

Veri Sızıntıları

Ghost Princess Siber Tehdit Grubu ABD'nin Havacılık Sektörünü Hedef Aldı



İlgili saldırı paylaşımı Ghost Princess adlı hacktivist grup tarafından gizli Telegram kanallarından yapıldı.

Tehdit Aktörü Ghost Princess, Los Angeles Uluslararası Havalimanı ABD'nin Kaliforniya eyaletinin Los Angeles şehrinde yer alan uluslararası havalimanı olan "**Los Angeles International Airport (LAX)**"ı hedef aldıklarını iddia etti. Tehdit aktörleri, yaptıkları siber saldırı sonucu veritabanını sızdırdıklarını iddia ediyor. İddia incelendiğinde "**Los Angeles International Airport (LAX)**'a" ait **2.5 milyon** kullanıcıyı ilgilendiren sızıntının olduğu, sızıntı içeriğinde "Özel uçak sahiplerinin Kullanıcı Verileri, Tam Adları, E-posta Adresleri, Şirket Adları, Uçak Model Numaraları ve CPA Numaraları" olduğu iddia ediliyor

Qatar Airways Verilerinin R00TK1T ISC Siber Ekibi Tarafından Sızdırıldığı İddiası

R00TK1T ISC CYBER TEAM

Attention, fellows!

We are R00TK1T, are here to remind you of the power we hold over the information and systems of Qatar Airways.

No company is safe from our grasp, and Qatar Airways is no exception!

ADOC N@vigator for Airbus 330 & 350: Unveiling the Secrets

We've managed to infiltrate Qatar Airways ADOC N@vigator system for their Airbus 330 and 350 aircraft.

With this access, we have unlocked a treasure trove of confidential flight data, maintenance schedules, and operational details.

The secrets of the skies are now in our hands!

Boeing 787 Toolbox Remote Data Package: Unleashing the Potential

But wait, there's more!

Our crew have also breached Qatar Airways' Boeing 787 Toolbox Remote Data Package.

This means we have access to critical software, maintenance logs, and even flight control systems.

The skies are our playground, and Qatar Airways is at our mercy!

Qatar Airways Interviews: Exposing Internal Discussions

In our quest for total disruption, we've obtained exclusive access to Qatar Airways internal interview recordings.

Prepare to witness the hidden conversations, hiring practices, and decision-making processes within the airline.

Qatar Airways Sample Docs: Unmasking the Inner Workings

Last but not least, we've decrypted Qatar Airways sample documents. From passenger manifests to cargo manifests, from boarding procedures to security protocols, we lay bare the inner workings of this airline.

Nothing is sacred, and the world will know the extent of our reach!

To all the news sites that dare underestimate the evidence we possess, consider this a warning:

We have prepared a special post just for you, exposing your ignorance and incompetence.

Remember, we are R00TK1T, and we will continue to expose the vulnerabilities of corporations, institutions, and all those who underestimate our power.

Stay tuned for more chaos, more revelations, and more tales of our conquests!

P.S.

We still have more than +400GB of data to go through, Qatar Airways are welcome to reach out to us and prevent the next publications

@R00TK1TOfficial

R00TK1T ISC CYBER TEAM

↓ QatarAirways A350 Airn@v software.zip
1787.2 MB

↓ QatarAirways A330 Airn@v software.zip
1390.8 MB

↓ QatarAirways interviews.zip
644.4 MB

↓ QatarAirways_Sample_Docs.zip
196.3 MB

↓ Boeing 787 Toolbox Remote Data Package.zip...
1371.2 MB

↓ Boeing 787 Toolbox Remote Data Package.zip...
2000.0 MB

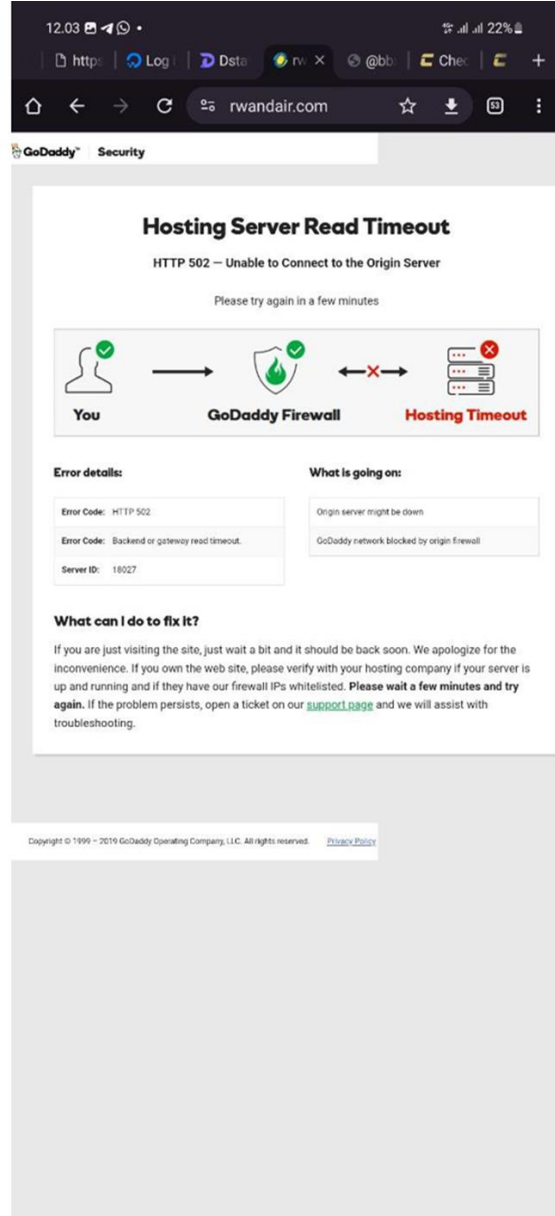
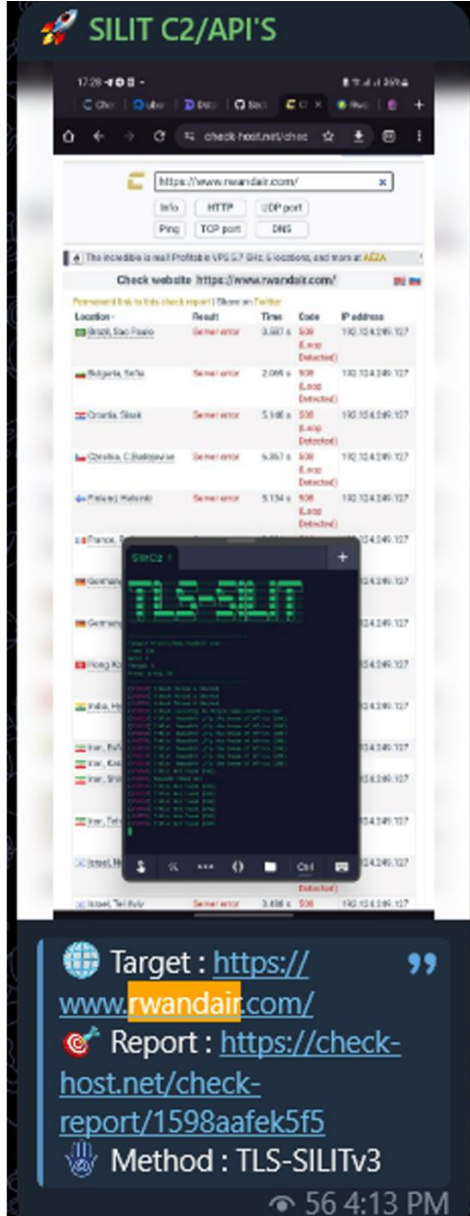
↓ Boeing 787 Toolbox Remote Data Package.zip...
2000.0 MB

↓ Boeing 787 Toolbox Remote Data Package.zip...
2000.0 MB

↓ Boeing 787 Toolbox Remote Data Package.zip...
2000.0 MB

29 Aralık 2023 tarihinde, "R00TK1T ISC Cyber Team" adlı tehdit aktörleri grubu, Qatar Airways'e başarılı bir saldırı gerçekleştirdiğini iddia etti. İlk olarak, grup Airbus A330 ve A350 uçakları için ADOC Navigator sistemini ele geçirdiklerini açıkladı. Bu ihlal, uçuş verileri, bakım programları ve operasyonel detaylara erişim sağladı. Saldırganlar ayrıca Boeing 787 Araç Kutusu Uzaktan Veri Paketi'ne de sızdıklarını söyleyerek, uçağın sistemlerini kontrol altına aldıklarını belirtti. İhlal içerisinde, Qatar Airways'in iç görüşmelerini, işe alım uygulamalarını ve karar alma süreçlerini ifşa ettiklerini iddia ettiler. İhlalin etkisiyle, yolcu manifestoları, kargo manifestoları, uçağa biniş prosedürleri ve güvenlik protokolleri de ortaya çıktı. Tehdit aktörleri, haber sitelerini uyararak ve ellerinde 400 GB'tan fazla veri olduğunu belirterek Qatar Airways'e pazarlık yapma ve daha fazla veri sızıntısını önleme fırsatı sundu. Saldırı, havacılık sektörünü hedef almayı amaçlayan daha cesur ve saldırganlar olduğunu gösteriyor ve sektörün bu tehditlere karşı daha uyanık olması gerekiyor.

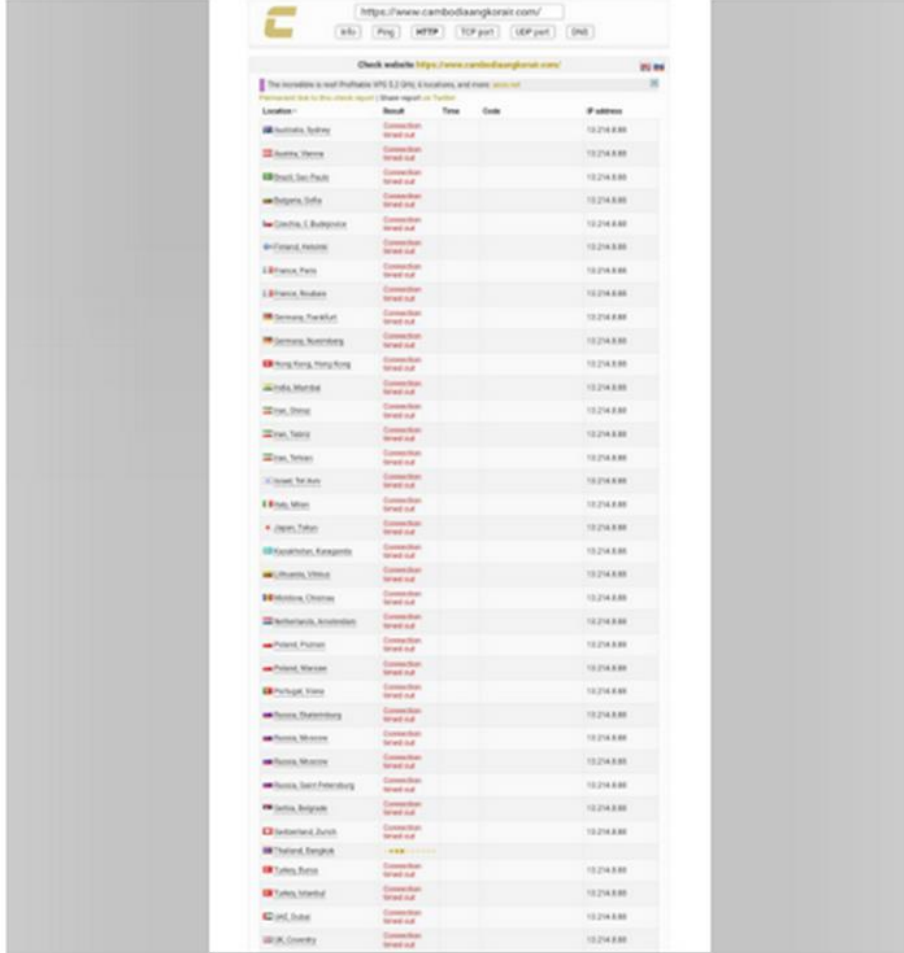
SilitNetwork RwandAir Ltd'yi Hedefliyor



16 Şubat 2024 tarihinde, bilgisayar korsanlığı grubu SilitNetwork, Ruanda'nın ulusal havayolu şirketi RwandAir Ltd'ye karşı bir siber saldırı gerçekleştirdi. Bu olay, havacılık sektörünün hassasiyetini ve havayolu operasyonları ile yolcu veri güvenliği üzerindeki potansiyel etkilerini vurgulamaktadır. SilitNetwork, genellikle mali kazanç, siyasi motivasyonlar veya bilgisayar korsanlığı yeteneklerini sergilemek amacıyla yüksek profilli hedeflere yönelik siber saldırılarda faaliyet gösteren bir grup olarak bilinmektedir. RwandAir Ltd'ye yapılan saldırı, havayolu şirketinin dijital altyapısını hedefleyen bir çabalıydı ve bilgisayar korsanları gelişmiş yöntemler kullanarak yetkisiz erişim sağladı. Bu saldırının ardındaki motivasyonlar spekülatif olsa da hassas yolcu bilgilerinin çalınması, havayolu operasyonlarının sekteye uğraması ve hatta gasp girişimleri gibi nedenler düşünülebilir. Saldırı, havayolu operasyonlarını etkileyebileceği gibi yolcu verilerinin gizliliğini ve bütünlüğünü de tehlikeye atma potansiyeline sahiptir. RwandAir, saldırıyı araştırmak ve güvenlik önlemleri almak için siber güvenlik kurumlarıyla iş birliği yapmaktadır. Bu saldırı, havacılık sektöründe güçlü siber güvenlik önlemlerinin önemini bir kez daha göstermektedir.

'Host Kill Crew Hackers' Kamboçya Angkor Air'i Hedef Aldı

HOST-KILL-CREW



Location	Result	Time	Cost	IP address
Australia, Sydney	Connection timed out			10.214.8.85
Austria, Vienna	Connection timed out			10.214.8.85
Brazil, Sao Paulo	Connection timed out			10.214.8.85
Bulgaria, Sofia	Connection timed out			10.214.8.85
Canada, S. Bayview	Connection timed out			10.214.8.85
Canada, Montreal	Connection timed out			10.214.8.85
France, Paris	Connection timed out			10.214.8.85
Germany, Frankfurt	Connection timed out			10.214.8.85
Germany, Nuremberg	Connection timed out			10.214.8.85
Hong Kong, Hong Kong	Connection timed out			10.214.8.85
India, Mumbai	Connection timed out			10.214.8.85
Iran, Tehran	Connection timed out			10.214.8.85
Iran, Tehran	Connection timed out			10.214.8.85
Israel, Tel Aviv	Connection timed out			10.214.8.85
Italy, Milan	Connection timed out			10.214.8.85
Japan, Tokyo	Connection timed out			10.214.8.85
Kazakhstan, Nur-Sultan	Connection timed out			10.214.8.85
Malaysia, Kuala Lumpur	Connection timed out			10.214.8.85
Netherlands, Amsterdam	Connection timed out			10.214.8.85
Poland, Warsaw	Connection timed out			10.214.8.85
Poland, Warsaw	Connection timed out			10.214.8.85
Portugal, Lisbon	Connection timed out			10.214.8.85
Russia, St. Petersburg	Connection timed out			10.214.8.85
Russia, Moscow	Connection timed out			10.214.8.85
Russia, Moscow	Connection timed out			10.214.8.85
Russia, Saint-Petersburg	Connection timed out			10.214.8.85
Serbia, Belgrade	Connection timed out			10.214.8.85
Switzerland, Zurich	Connection timed out			10.214.8.85
Thailand, Bangkok	Connection timed out			10.214.8.85
Turkey, Istanbul	Connection timed out			10.214.8.85
Turkey, Istanbul	Connection timed out			10.214.8.85
UK, London	Connection timed out			10.214.8.85
USA, New York	Connection timed out			10.214.8.85

Cambodia Angkor air flight website down By Host-Kill-Crew

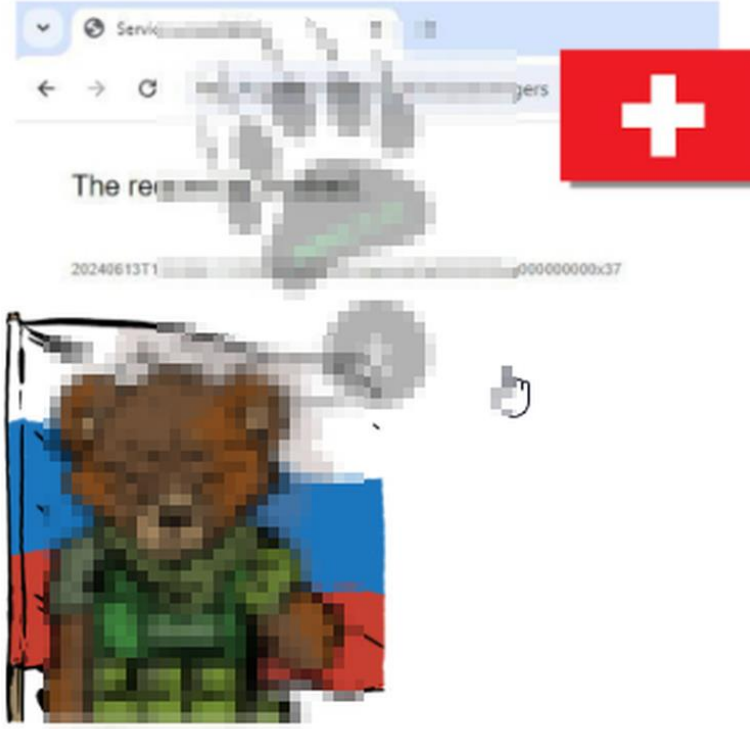
URL:<https://www.cambodiaangkorair.com>

CHECK-HOST*:<https://check-host.net/check-report/fd66ffb858>

Kendilerine Host Kill Crew adını veren ve diğer tehdit aktörlerine göre daha az bilinen bir hacker grubu Kamboçya Angkor Air siber saldırısının sorumluluğunu üstlendi. Grup, saldırının ayrıntılarını Telegram kanallarında DDOS (Distributed Denial of Service attack) iddialarıyla yayınlarak çevrimiçi hizmetleri bir süreliğine durdurdu.

DDoS Saldırıları

Tehdit Aktörü NoName057(16) Avrupa'daki Kritik Önemdeki Havalimanlarını Hedef Aldı

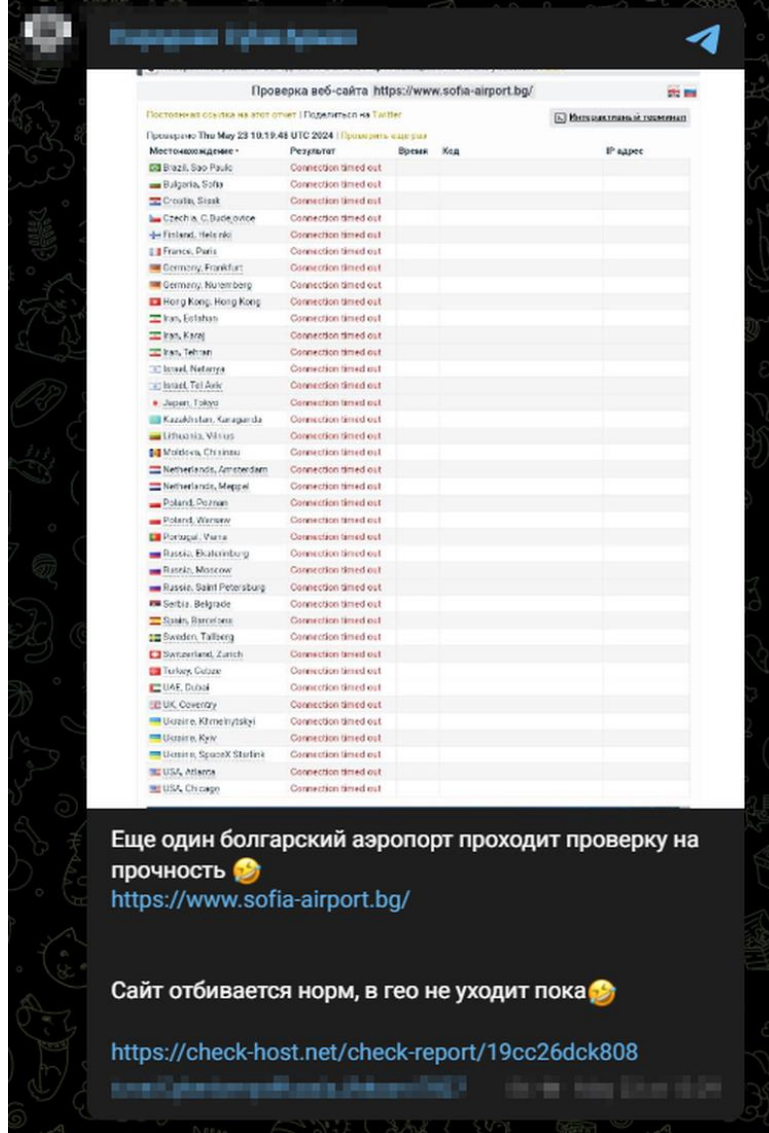


[Continuing](#) the attacks on Switzerland and hitting the local airport website with our DDoS missiles🐱

✗The largest international airport in Switzerland, located in Zurich. The main hub for Swiss International Air Lines. Serves most international flights (dead on ping)

İlgili saldırı paylaşımı **NoName057(16)** adlı hacktivist grup tarafından gizli Telegram kanallarından yapıldı. Rus menşeli tehdit aktörü **"NoName057(16)"**, Zürih'te bulunan İsviçre'nin en büyük uluslararası havalimanı olan ve çoğu uluslararası uçuşa hizmet veren **"Flughafen Zürich"** havalimanını hedef aldığını iddia ediyor. Saldırı yöntemi olarak ise tehdit aktörleri arasında oldukça yaygın bir teknik olan Distributed Denial-of-Service (DDoS) saldırısını kullandıklarını belirtiyor.

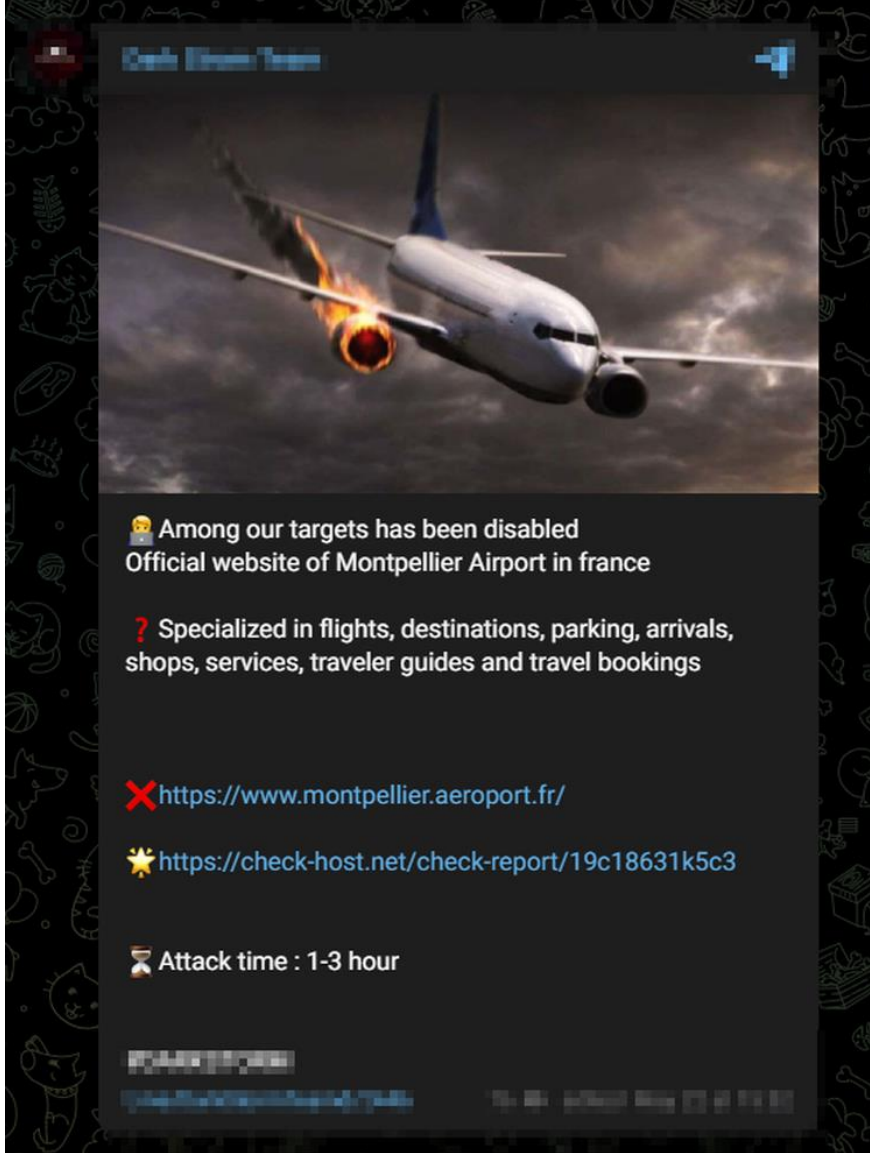
Tehdit Aktörü Народная CyberАрмия Bulgaristan Havacılık Sektörünü Hedef Aldıklarını İddia Etti



İlgili saldırı paylaşımı "**Народная CyberАрмия**" adlı hacktivist grup tarafından gizli Telegram kanallarından yapıldı.

Rus menşeli tehdit aktörü "**Народная CyberАрмия**", Bulgaristan havacılık sektöründe hizmet veren "Sofia Airport" hedef aldıklarını iddia ediyor. Tehdit aktörleri, saldırı yöntemi olarak da tehdit aktörleri arasında oldukça yaygın bir teknik olan Distributed Denial-of-Service (DDoS) saldırısını kullandıklarını belirttiler.

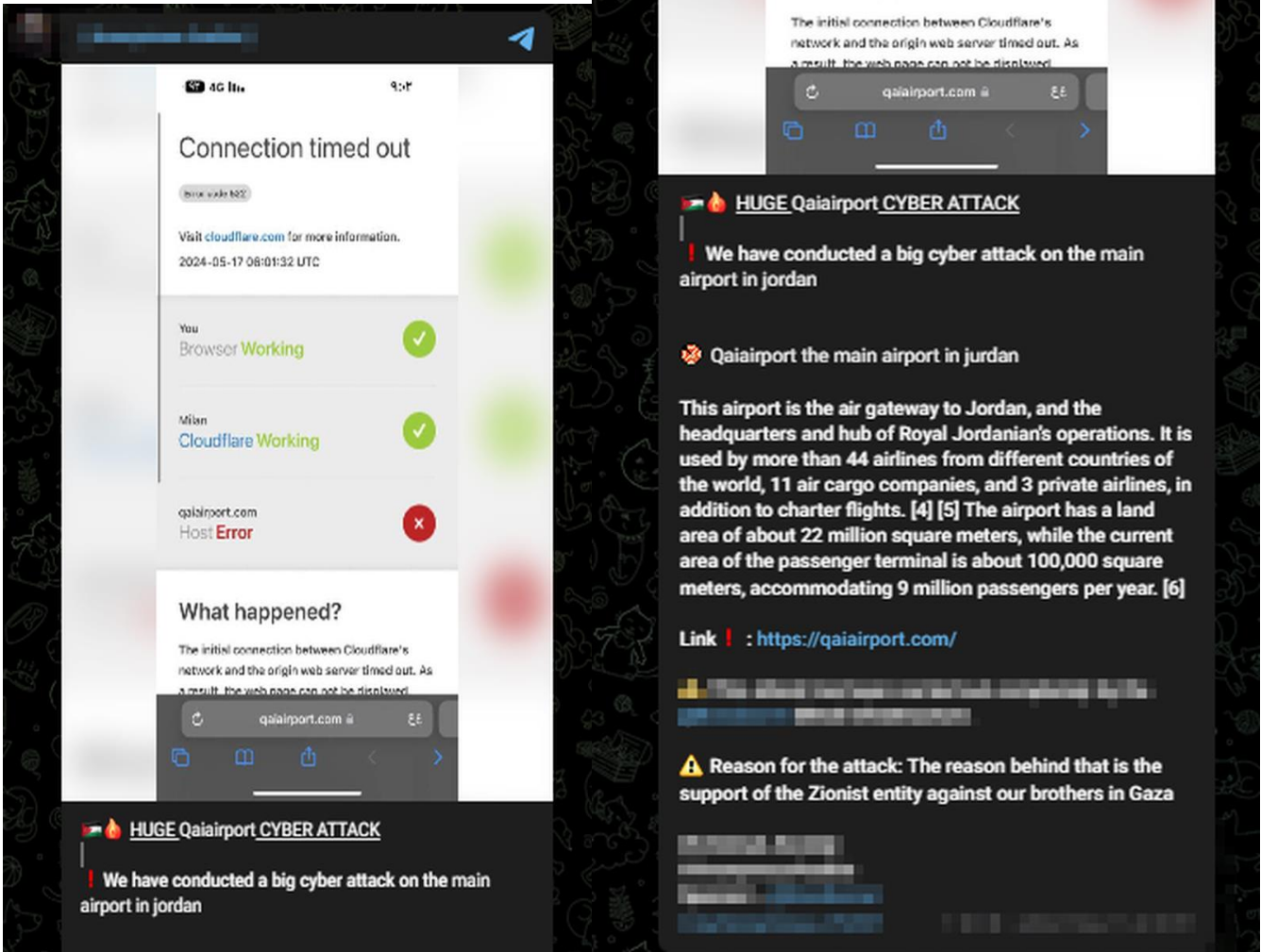
Tehdit Aktörü Dark Strom Team Fransa Havacılık Sektörünü Hedef Aldı



İlgili saldırı paylaşımı "**Dark Strom Team**" adlı hacktivist grup tarafından gizli Telegram kanallarından yapıldı.

Rus menşeli tehdit aktörü "**Dark Strom Team**", Fransa havacılık sektöründe hizmet veren "**Aéroport Montpellier Méditerranée**" hedef aldıklarını iddia ediyor. Tehdit aktörleri, saldırı yöntemi olarak da tehdit aktörleri arasında oldukça yaygın bir teknik olan Distributed Denial-of-Service (DDoS) saldırısını kullandıklarını belirttiler.

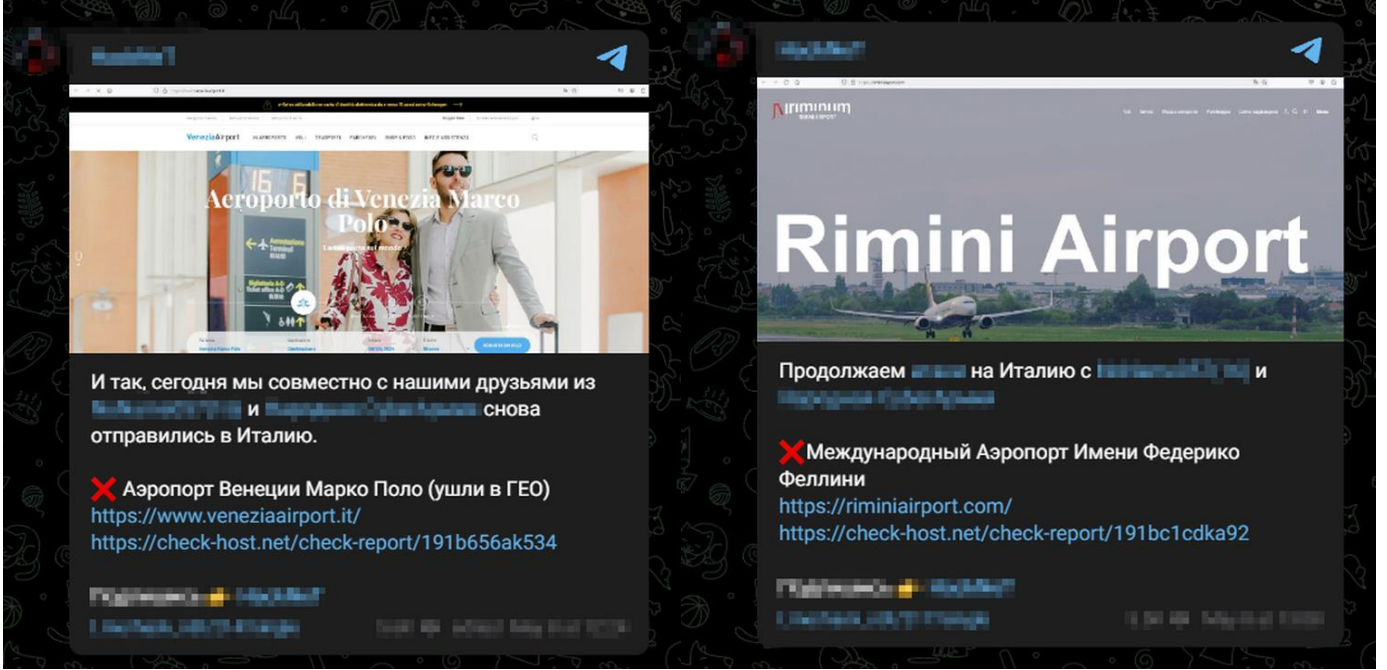
Tehdit Aktörü Anonymous Arabia Ürdün Havacılık Sektörünü Hedef Aldı



İlgili saldırı paylaşımı "**Anonymous Arabia**" adlı hacktivist grup tarafından gizli Telegram kanallarından yapıldı.

Tehdit aktörü "**Anonymous Arabia**" ve "**Criminal_Society**" ortaklığı ile Ürdün havacılık sektöründe hizmet veren "Qaiairport" havalimanını hedef aldıklarını iddia ediyor. Tehdit aktörleri, saldırı yöntemi olarak da tehdit aktörleri arasında oldukça yaygın bir teknik olan Distributed Denial-of-Service (DDoS) saldırısını kullandıklarını belirttiler.

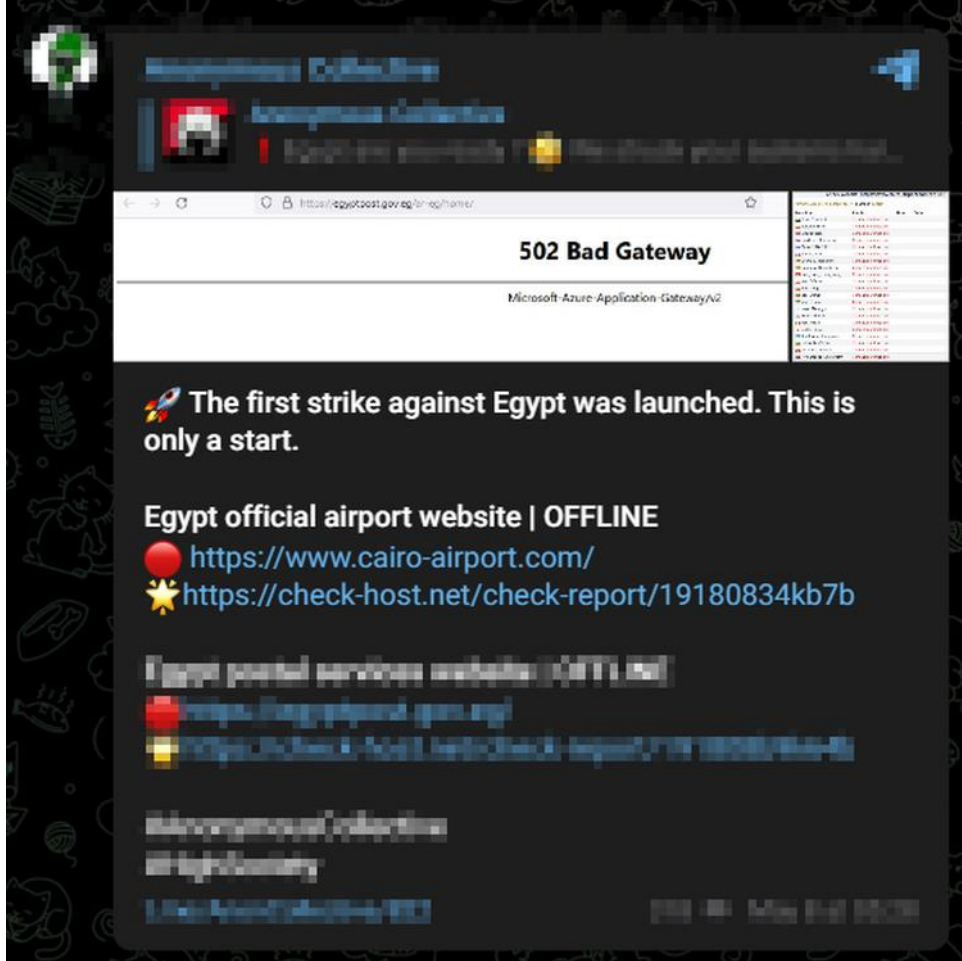
HackNeT İtalya Havacılık Sektörünü Hedef Aldı



İlgili saldırı paylaşımı HackNeT adlı hacktivist grup tarafından gizli Telegram kanallarından yapıldı.

Rus menşeli Tehdit aktörleri "**HackNeT**" "**NoName057(16)**" ve "**Народная CyberАрмия**" ortaklaşa yapılan siber saldırıda İtalya'daki en yoğun beşinci havalimanı olan "**Venice Marco Polo Airport**" ve İtalya'nın Rimini kentinde bulunan "**Federico Fellini International Airport'u**" hedef aldıklarını iddia etti. Tehdit aktörleri, saldırı yöntemi olarak da tehdit aktörleri arasında oldukça yaygın bir teknik olan Distributed Denial-of-Service (DDoS) saldırısını kullandıklarını belirttiler.

Anonymous Collective Siber Tehdit Grubu Mısır Havacılık Sektörünü Hedef Aldı



İlgili saldırı paylaşımı **Anonymous Collective** adlı hacktivist grup tarafından gizli Telegram kanallarından yapıldı.

Tehdit aktörü "**Anonymous Collective**" ve "HighSociety" ortaklığında Mısır havacılık sektöründe hizmet veren "Cairo International Airport" hedef aldıklarını iddia etti. Tehdit aktörleri, saldırı yöntemi olarak da tehdit aktörleri arasında oldukça yaygın bir teknik olan Distributed Denial-of-Service (DDoS) saldırısını kullandıklarını belirttiler.

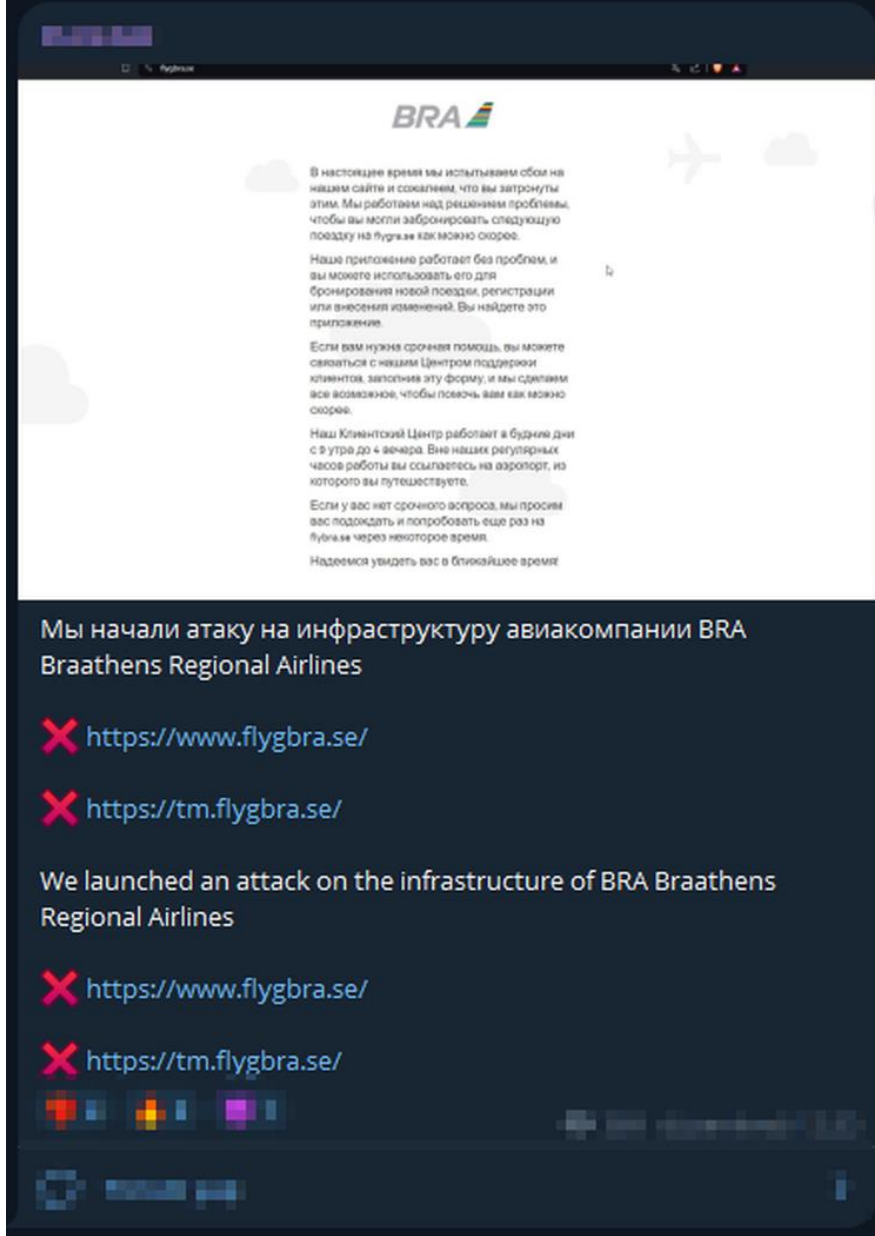
Siber Tehdit Grubu UserSec Almanya Havacılık Sektörünü Hedef Aldı



İlgili saldırı paylaşımı **UserSec** adlı hacktivist grup tarafından gizli Telegram kanallarından yapıldı.

Rus menşeli tehdit aktörlerinden **UserSec**, Almanya havacılık sektöründe hizmet veren "**Düsseldorf Havalimanı'nı**" hedef aldıklarını iddia etti. Tehdit aktörleri, saldırı yöntemi olarak da tehdit aktörleri arasında oldukça yaygın bir teknik olan Distributed Denial-of-Service (DDoS) saldırısını kullandıklarını belirttiler.

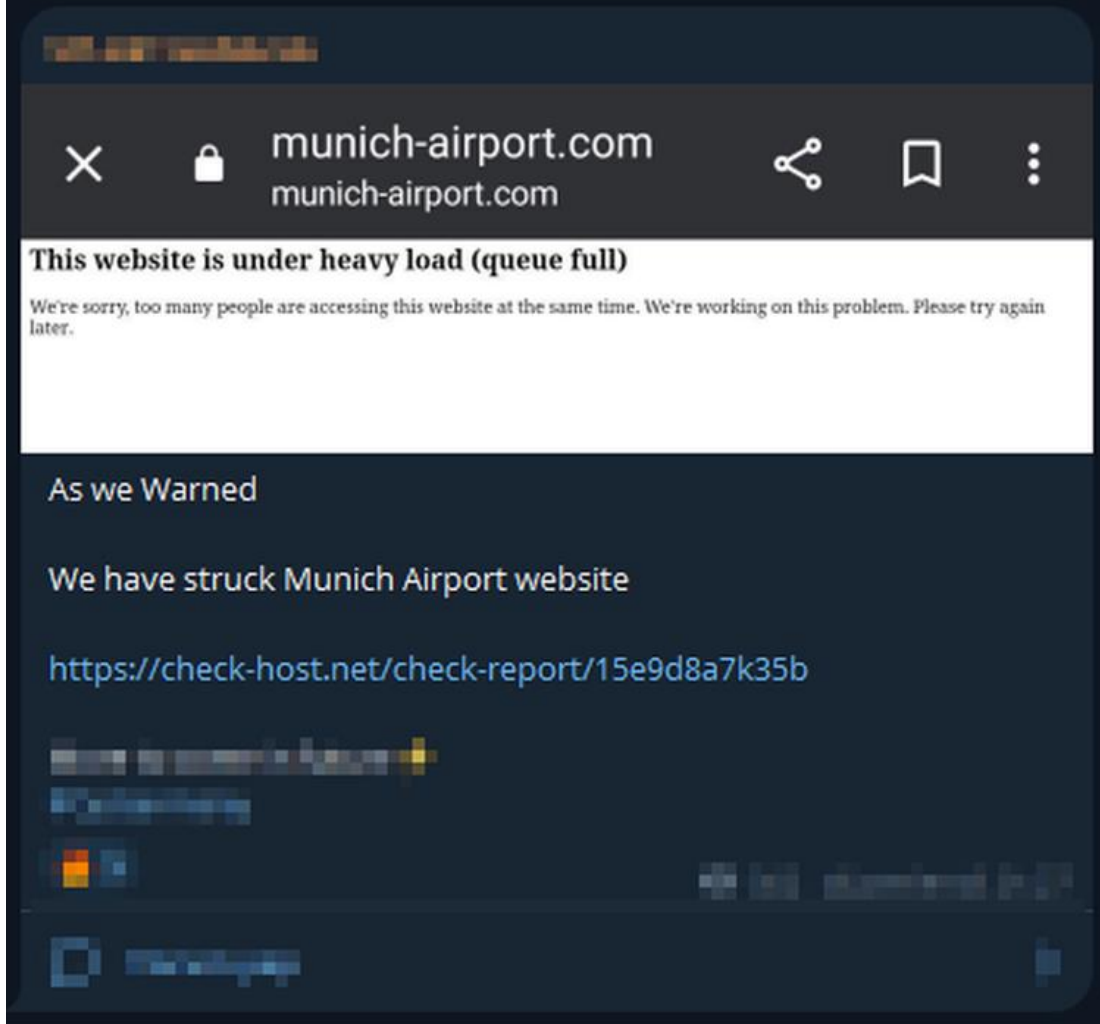
PHOENIX İsveç Havacılık Sektörünü Hedef Aldıklarını İddia Ediyor



İlgili saldırı paylaşımı PHOENIX adlı hacktivist grup tarafından gizli Telegram kanallarından yapıldı.

Tehdit aktörü "**PHOENIX**", Braathens Regional Airlines genellikle BRA olarak kısaltılır, merkezi Stockholm'de bulunan bir İsveç bölgesel havayolu şirketi olan "**BRA Braathens Regional Airlines**'i" hedef aldıklarını iddia etti. Tehdit aktörleri, saldırı yöntemi olarak da tehdit aktörleri arasında oldukça yaygın bir teknik olan Distributed Denial-of-Service (DDoS) saldırısını kullandıklarını belirttiler.

SYLHET GANG-SG Siber Tehdit Grubu Almanya Havacılık Sektörünü Hedef Aldı



İlgili saldırı paylaşımı **SYLHET GANG-SG** adlı hacktivist grup tarafından gizli Telegram kanallarından yapıldı.

Tehdit aktörü SYLHET GANG-SG, Münih Franz Josef Strauss Havalimanı, Almanya Bavyera eyaletinin merkezi Münih'e hizmet veren uluslararası havalimanı olan "**Munich Airport**" hedef aldıklarını iddia etti. Tehdit aktörleri, saldırı yöntemi olarak da tehdit aktörleri arasında oldukça yaygın bir teknik olan Distributed Denial-of-Service (DDoS) saldırısını kullandıklarını belirttiler.

CyberArmyofRussia_Reborn İtalya Havacılık Sektörünü Hedef Aldı

Местонахождение *	Результат	Время	Код	IP адрес
Brazil, Sao Paulo	Connection timed out			80.229.150.18
Bulgaria, Sofia	Connection timed out			92.123.103.83
Croatia, Sreak	Connection timed out			2.16.16.166
Czechia, C. Budajovice	Connection timed out			2.17.147.192
Finland, Helsinki	Connection timed out			80.229.150.51
France, Paris	Connection timed out			92.123.236.73
Germany, Frankfurt	Connection timed out			2.17.100.203
Germany, Nuremberg	Connection timed out			2.17.112.41
Hong Kong, Hong Kong	Connection timed out			104.115.38.208
India, Hyderabad	Connection timed out			184.51.165.169
Iran, Esfahan	Connection timed out			2.19.120.18
Iran, Karaj	Connection timed out			2.17.22.137
Iran, Shiraz	Connection timed out			92.123.103.81
Iran, Tehran	Connection timed out			2.20.143.59
Israel, Netanya	Connection timed out			92.123.181.92
Israel, Tel Aviv	Connection timed out			92.123.181.92
Italy, Milan	Connection timed out			173.222.105.42
Japan, Tokyo	Connection timed out			23.46.229.98
Kazakhstan, Karaganda	Connection timed out			80.229.150.18
Lithuania, Vilnius	Connection timed out			96.16.54.154
Moldova, Chisinau	Connection timed out			92.123.103.81
Netherlands, Amsterdam	Connection timed out			2.18.244.68
Netherlands, Middel	Connection timed out			23.73.0.40
Poland, Poznan	Connection timed out			2.16.204.74
Poland, Warsaw	Connection timed out			80.229.254.37
Portugal, Viana	Connection timed out			95.100.105.188
Russia, Ekaterinburg	Connection timed out			92.123.189.8
Russia, Moscow	Connection timed out			95.101.133.9
Russia, Moscow	Connection timed out			80.229.254.37
Russia, Saint Petersburg	Connection timed out			96.16.49.46
Serbia, Belgrade	Connection timed out			95.101.23.163
Spain, Barcelona	Connection timed out			95.101.110.6
Switzerland, Zurich	Connection timed out			92.123.27.89
Turkey, Gebze	Connection timed out			2.19.196.123
Turkey, Istanbul	Connection timed out			2.20.45.3
UAE, Dubai	Connection timed out			2.21.12.167
UK, Coventry	Connection timed out			23.48.165.145
Ukraine, Khmelnytskyi	Connection timed out			23.38.98.93

Netherlands, Amsterdam	Connection timed out	74.124.199.81
Netherlands, Amsterdam	Connection timed out	2.18.244.68
Netherlands, Middel	Connection timed out	23.73.0.40
Poland, Poznan	Connection timed out	2.16.204.74
Poland, Warsaw	Connection timed out	80.229.254.37
Portugal, Viana	Connection timed out	95.100.105.188
Russia, Ekaterinburg	Connection timed out	92.123.189.8
Russia, Moscow	Connection timed out	95.101.133.9
Russia, Moscow	Connection timed out	80.229.254.37
Russia, Saint Petersburg	Connection timed out	96.16.49.46
Serbia, Belgrade	Connection timed out	95.101.23.163
Spain, Barcelona	Connection timed out	95.101.110.6
Switzerland, Zurich	Connection timed out	92.123.27.89
Turkey, Gebze	Connection timed out	2.19.196.123
Turkey, Istanbul	Connection timed out	2.20.45.3
UAE, Dubai	Connection timed out	2.21.12.167
UK, Coventry	Connection timed out	23.48.165.145
Ukraine, Khmelnytskyi	Connection timed out	23.38.98.93

bologna-airport.it/voli/vola-da-bologna/voli-in-tempo-reale/

red while processing your request.

7c524350.1707989613.198e72e8

<https://check-host.net/check-report/15902805k5f9>

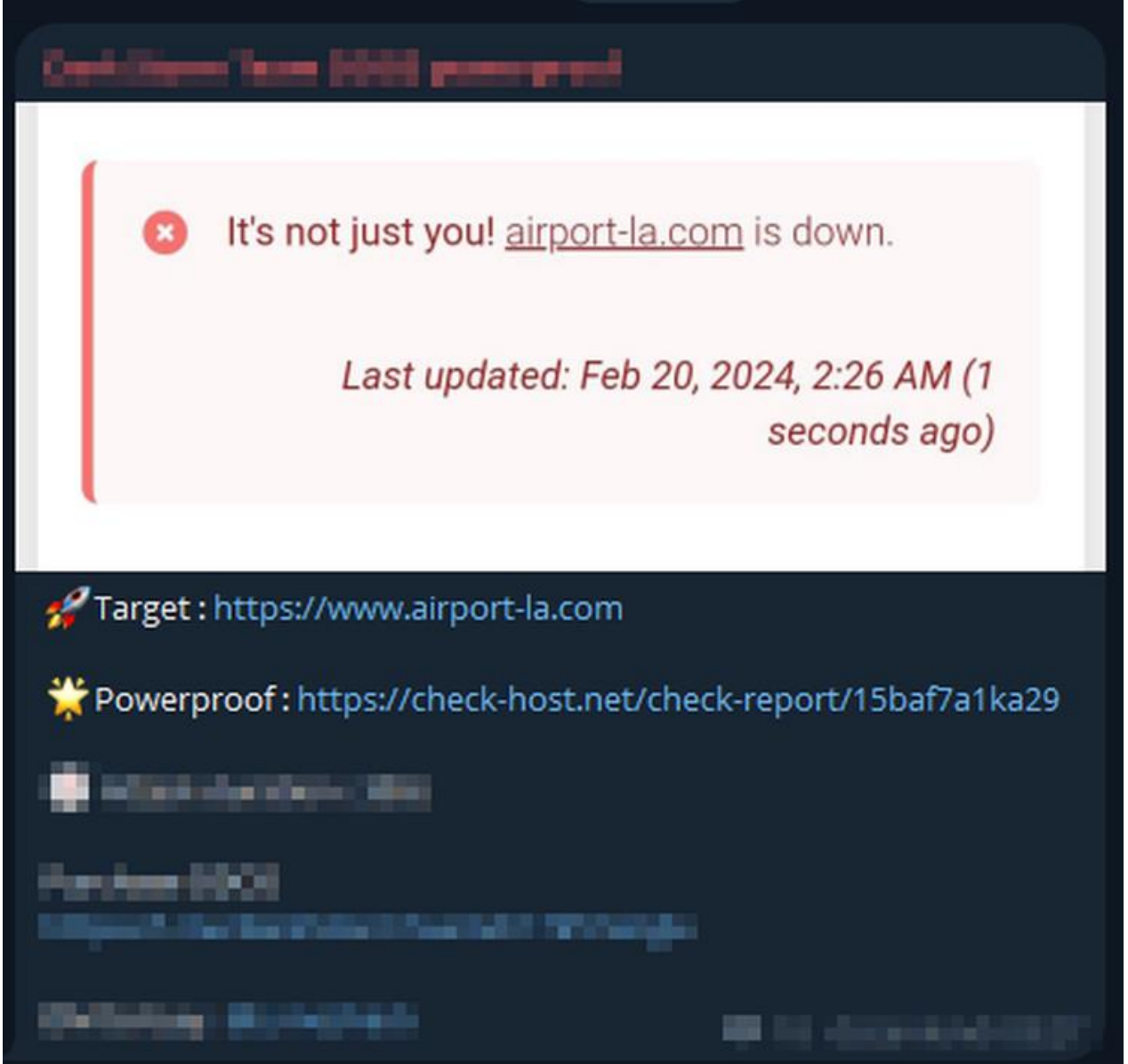
Международный аэропорт Болоньи все-таки пал под нашими DDoS ракетами!!!

Слава России 🇷🇺🇷🇺🇷🇺

İlgili saldırı paylaşımı **CyberArmyofRussia_Reborn** diğer adıyla **Народная CyberАрмия** olarak bilinen hacktivist grup tarafından gizli Telegram kanallarından yapıldı.

Rus menşeli tehdit aktörü "**CyberArmyofRussia_Reborn**" İtalya'nın Bologna kentinde yer alan uluslararası havalimanı olan "**Bologna Guglielmo Marconi Havalimanı**" hedef aldıklarını iddia etti. Tehdit aktörleri, saldırı yöntemi olarak da tehdit aktörleri arasında oldukça yaygın bir teknik olan Distributed Denial-of-Service (DDoS) saldırısını kullandıklarını belirttiler.

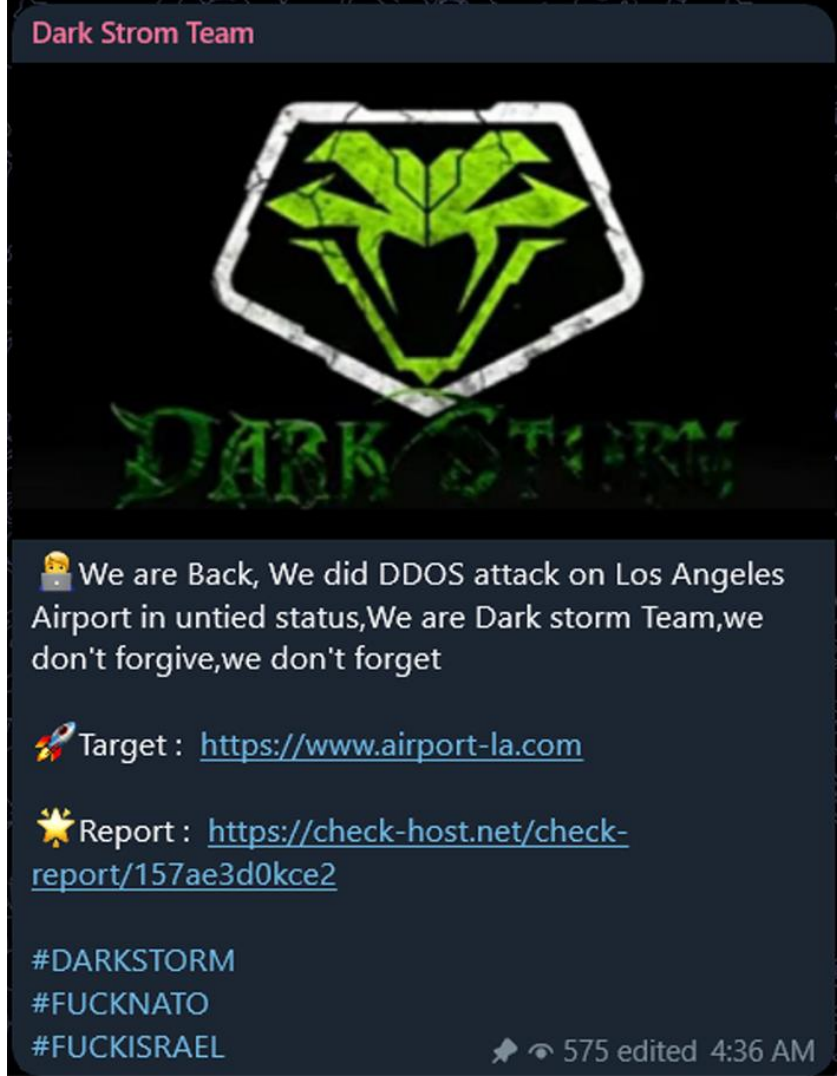
Dark Storm Team ABD Havacılık Sektörünü Hedef Aldı



İlgili saldırı paylaşımı **Dark Storm Team** adlı hacktivist grup tarafından gizli Telegram kanallarından yapıldı.

Tehdit aktörü **Dark Storm Team**, ABD'nin Kaliforniya eyaletinin Los Angeles şehrinde yer alan uluslararası havalimanı olan "**airport-la.com**" hedef aldıklarını iddia etti. Tehdit aktörleri, saldırı yöntemi olarak da tehdit aktörleri arasında oldukça yaygın bir teknik olan Distributed Denial-of-Service (DDoS) saldırısını kullandıklarını belirttiler.

Dark Strom Ekibinin Los Angeles Havalimanı'na DDOS Saldırısı Gerçekleştirildi



12 Şubat 2024'te Dark Strom Team tarafından gerçekleştirilen bir DDoS saldırısı sonucunda Los Angeles Uluslararası Havalimanı (LAX) etkilendi. Bu saldırı, havacılık altyapısının siber saldırılara karşı savunmasızlığını gösterdi. Dark Strom Team, kötü şöhretli bir bilgisayar korsanlığı grubudur ve DDoS saldırılarıyla tanınmıştır. LAX'e yapılan saldırıda, çevrimiçi platformlara gelen ağ trafiği arttı. Bu artış, havalimanı web sitesinin geçici olarak kapanmasına ve yolcuların ve personelin çevrimiçi hizmetlerden yararlanamamasına neden oldu. Saldırının motivasyonu hala spekülasyon konusudur, ancak etkisi büyük oldu. Havalimanı yetkilileri, siber saldırının neden olduğu rahatsızlığı daha da kötüleştiren güncellemelerde zorluklar yaşadılar. Havalimanının siber güvenlik ekibi saldırıya hızla yanıt vererek önlemler aldı. Bu olay, havalimanının siber güvenlik altyapısının gözden geçirilmesine yol açtı. Saldırının kaynağını tespit etmek için bir soruşturma başlatıldı ve LAX'in kolluk kuvvetleri ve siber güvenlik firmalarıyla iş birliği yapıyor. Bu saldırı, havalimanlarında siber güvenlik önlemlerinin uygulanmasının önemini vurgulamakta ve kesintisiz hizmet sağlamak için olay müdahale planlamasının geliştirilmesi gerektiğini ortaya koymaktadır.

Gulf Air Siber Saldırıya Maruz Kaldı



Posted Tuesday at 08:04 PM

Report post

As you may see it in the news, GulfAir database including Passengers Personal Information and their trips are stolen. And we were the group that hacked into it.

<https://www.reuters.com/business/aerospace-defense/gulf-air-exposed-data-breach-vital-operations-not-affected-2023-11-25/>

The Database includes:

- Emails
- Passport numbers
- Personal Information
- Mobile number
- Passengers flights
- etc.

They are in several databases some with +200M records!!

The data time is from GulfAir establishment until nearly one month ago.

For 7 Days, We sell it exclusively and the price is \$70K, which means first buyer will be the last.

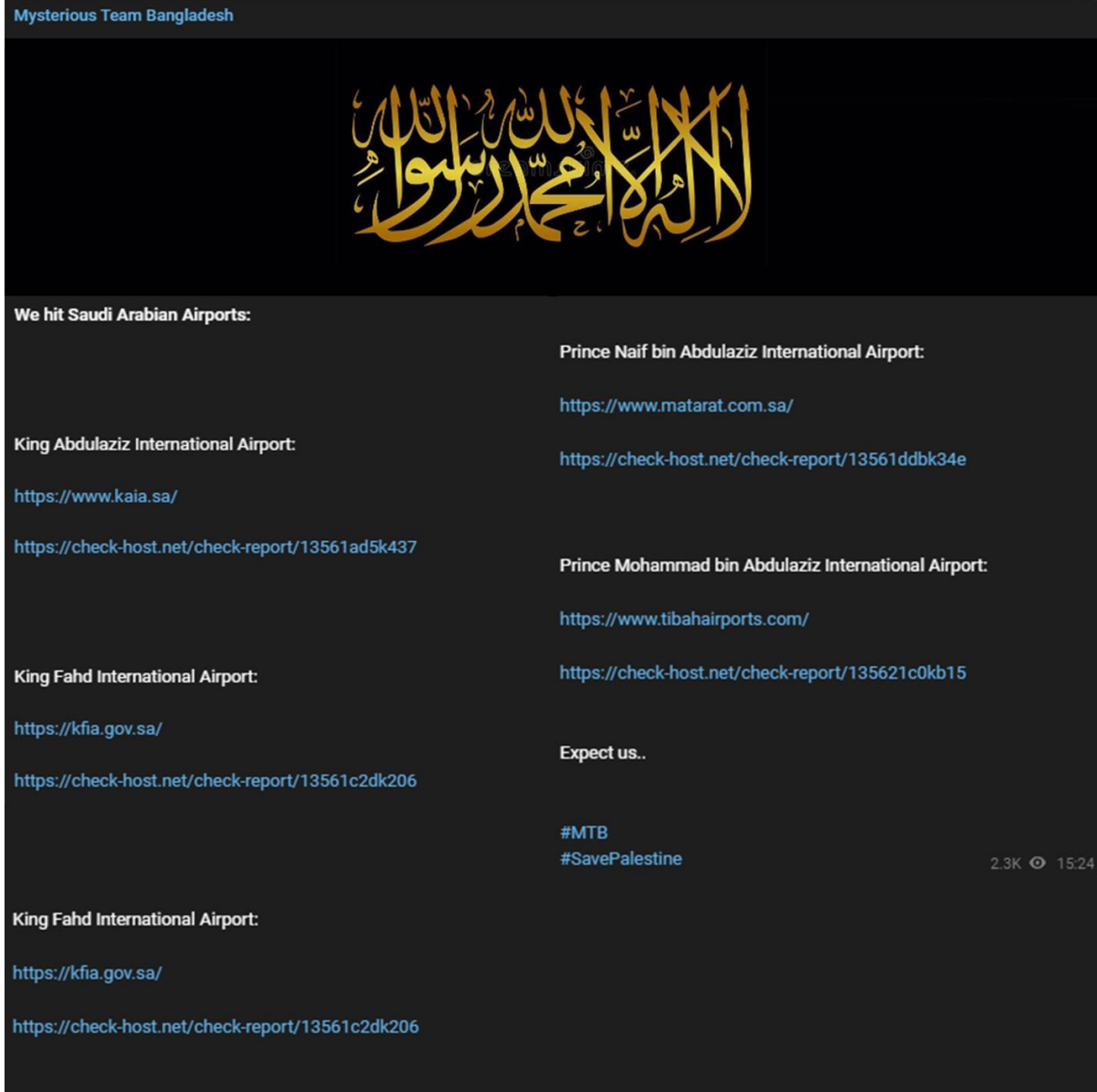
After 7 days if no one want the data exclusively, then the price will drop to \$20K and we will sell it to anybody with no limits.

First contacts in PM.

POC images are attached

Bir tehdit-aktör grubu olan ALTOUFAN TEAM, Bahreyn'in ulusal havayolu şirketi Gulf Air'e Dağıtık Hizmet Engelleme (DDoS) saldırısı gerçekleştirme niyetinde olduklarını duyurdu. Grup, eylemlerini Filistin davasına verilen destekle ilişkilendiriyor. ALTOUFAN TEAM, ayrıca Gulf Air ve Bahreyn Uluslararası Havalimanı'na karşı başarılı bir DDoS saldırısı gerçekleştirdiğini duyurdu. Bu saldırılar, Gulf Air'in çevrimiçi hizmetlerinde kesintilere ve operasyonel sıkıntılara neden oldu. Aynı gün Bahreyn Havalimanı'nın çevrimiçi portalı da bir DDoS saldırısı nedeniyle geçici olarak erişilemez hale geldi. Gulf Air, verilerinin ihlal edildiğini duyurdu, ancak Bahreyn haber ajansı havayolunun operasyonlarının etkilenmediğini belirtti. ALTOUFAN TEAM'in saldırısı sonucunda şirketin e-posta sistemi ve müşteri veri tabanı bazı bilgilerin tehlikeye girmiş olabileceği rapor edildi. Saldırılı kontrol altına almak için acil durum planları devreye sokuldu.

Mysterious Team Bangladesh Suudi Arabistan Havalimanı Web Sitesini Hedef Aldı



19 Kasım 2023 tarihinde " Mysterious Team Bangladesh" (MTB) adını takan bir grup, Suudi Arabistan'ın bazı önemli havalimanlarına Dağıtık Hizmet Engelleme (DDoS) saldırısı gerçekleştirdi. Saldırıdan etkilenen havalimanları arasında Kral Abdülaziz Uluslararası Havalimanı, Kral Fahd Uluslararası Havalimanı, Prens Naif bin Abdülaziz Uluslararası Havalimanı ve Prens Muhammed bin Abdülaziz Uluslararası Havalimanı yer aldı.

MTB'nin neden saldırı düzenlediği ve gerçek niyeti konusunda henüz net bir bilgi bulunmamaktadır. MTB'nin #SavePalestine etiketini kullanması, Gazze çatışmasıyla ilgili ideolojik ya da siyasi motivasyonlarının olabileceğini düşündürmektedir. Ancak, saldırının arkasındaki gerçek niyete ve daha geniş jeopolitik bağlantılara ulaşabilmek için daha fazla araştırma yapılması gerekmektedir. Son mesajları "Bizi bekleyin..." ifadesiyle sona ermiştir ve #MTB ve #SavePalestine hashtag'lerini içermektedir.

A red hexagonal grid pattern, resembling a honeycomb or isometric cube structure, covers the top and bottom portions of the image. The pattern is composed of thin red lines on a dark blue-grey background.

ECHO

CYBER THREAT INTELLIGENCE