



contact us

about us

Our revelations

suggestions

Our revelations



Invoice 4690494

Igor Sorokopud
Third Secretary
Embassy of Russian Fed
Neauphle-le-Chateau Street 39
Tehran
Iran

Account 3000487
Sales order 4677701

Delivery address
Igor Sorokopud
Embassy of Russian Fed
Neauphle-le-Chateau Street
39
Tehran
Iran

Page 1 / 3
Invoice date 2020-01-17
Due date 2020-01-24
Your tax exempt number
Mode of delivery Airfreight
Sales responsible
Customer reference Confirmed 10/1
Contact

Item no.	Qty	Description	Freight	Unit price	Discount	Discount %	Amount
032526	3	Johnnie Walker Black Label, 100 cl. - Alc. 40% Vol. In gift box.	8.90	31.09			93.27
032523	3	Ballantine's 100 cl. - Alc. 40% Vol.	9.17	14.75			44.25
032525	3	Johnnie Walker Red Label, 100 cl. - Alc. 40% Vol. In gift box.	8.90	14.13			42.39
085512	1	Budweiser Budvar 24x33 cl. cans. - Alc. 5.00% Vol.	16.61	20.06			20.06
032521	2	Beefeater London Dry Gin 100 cl. - Alc. 47% Vol.	6.55	12.49			24.98
032277	1	Schweppes Tonic 24x33 cl. cans.	16.65	15.88			15.88
032354	5	Torres 10 YO Brandy 100 cl. - Alc. 38% Vol.	14.83	11.87			59.35
084675	4	Kilbeggan Blended Irish Whiskey, 100 cl. - Alc. 40% Vol.	12.33	19.78			79.12
032719	1	ERDINGER Weissbier with fine yeast 24x50 cl. cans. - Alc. 5.3% Vol.	25.12	32.78			32.78
032544	4	Tullamore D.E.W. 100 cl. - Alc. 40% Vol. Irish.	11.87	19.78			79.12

</files/Sample1.pdf>

An example of the hacking of the Russian Embassy in Tehran by the IRGC Intelligence Organization

(1)

176 | DME | 62570981



176-62570981

Shipper's Name and Address RUSSKIY MIR FOUNDATION MOSFILMOVSKAYA STR 40A 119285, RUSSIAN FEDERATION		Shipper's Account Number		Not Negotiable Air Waybill Issued by EMIRATES NEW EMIRATES GROUP HQ AIRPORT ROAD, DEIRA UNITED ARAB EMIRATES								
Consignee's Name and Address FARASOOBAR INT'L FORWARDERS AND SHIPPING AGENCY CO. SUITE NO.603, 5TH FLOOR, SADAF BUILDING NO.132, KESHAVARZ BOULVARD P.O BOX 14155-3635, TEHRAN-14 I.R OF IRAN, TEHRAN, TEL:+982188979737		Consignee's Account Number		Copies 1, 2 and 3 of this Air Waybill are originals and have the same validity.								
Issuing Carrier's Agent Name and City ASTRA CARGO, MOSCOW		Agent's IATA Code		Accounting Information CGR HAWB 20210901		Account No.						
Airport of Departure (Addr. of First Carrier) and Requested Routing DME/DOMODEDOVO				Reference Number		Optional Shipping Information						
To	By First Carrier	Routing and Destination	to	by	to	by	Currency	CHG Code	WT/VAL	Other	Declared Value for Carriage	Declared Value for Customs
DXB	EK		THR	EK			RUB	PP	X	X	NVD	NCV
Airport of Destination TEHRAN		Requested Flight/Date EKXXXX/01SEP21		Requested Flight/Date EKXXXX/03SEP21		Amount of Insurance NIL		INSURANCE - If carrier offers insurance, and such insurance is requested in accordance with the conditions thereof, indicate amount to be insured in figures in box marked "Amount of Insurance".				
Handling Information HAWB 20210901 NOTIFY FARASOOBAR INT'L FORWARDERS AND SHIPPING AGENCY CO. TEL+9821 88979737-9											SCI	

</files/Sample2.pdf>

An example of the hacking of the Russian Embassy in Tehran by the IRGC Intelligence Organization

(2)



Islamic Republic of Iran
Ministry of Economic Affairs and Finance
Organization for Investment
Economic and technical Assistance of Iran

Ref: 1839-1-21
Date: 2/20/2021

Confidential

**Mr. Timur Maksimov
Deputy Minister of Finance,
Russian Federation**

Subject: "Protocol on Electrification of Garmsar-Inche Burun Railway Line" project

Dear Deputy Minister,

This is to acknowledge the receipt of your letter attached with the draft Protocol of Amendment to the Intergovernmental Loan Agreement for the above-mentioned project, through Russian Federation Embassy to Tehran, Note No. 83 dated January 17, 2021.

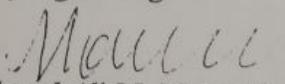
While appreciating prolongation of the credit utilization period for the project, till the end of 2026, I would like to draw your attention to the following issues mentioned in the draft protocol:

1. A large amount of utilization of the loan will be made in the period of 2023-2026, which makes it difficult and even impossible to repay the loan within two years (in the years 2027-2028) due to internal procedures and budget constraints.
2. The part of the loan that will be used until the end of 2022, should be repaid before the start of operation of the project.

In light of the above, it would be prudent to postpone the start of repayment of the credit, after the end of the utilization period (2026), with a format similar to what already agreed in the Loan Agreement, (within 5 years).

Therefore, it is requested to kindly confirm the above issues and provide us with the revised draft of the Protocol at the earliest convenience.

Please accept, Excellency, the assurances of my highest regard.

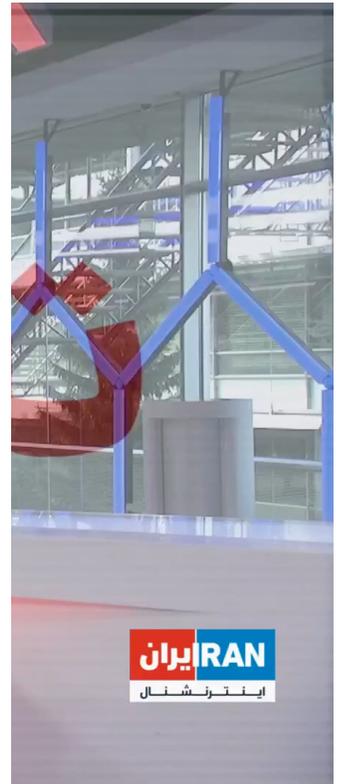

Seyed Ali M. Mousavi

**Vice Minister
and President of OIETAI**

An example of the hacking of the Russian Embassy in Tehran by the IRGC Intelligence Organization (3)



0:00 / 4:24



گروه هکری لبدوختگان، هویت برخی از کارمندان سایبری سپاه پاسداران را افشا کرد

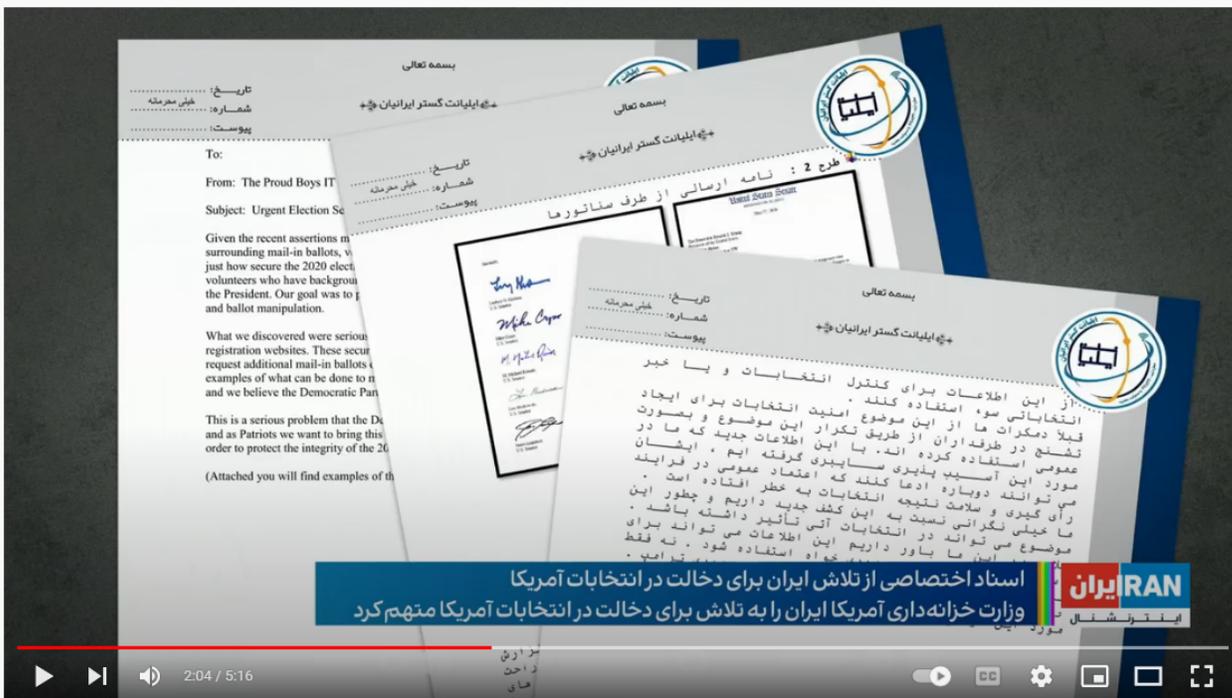


۱۴۰۱/۴/۲۵

ایران

<https://www.iranintl.com/202207168711>

Disclosure of the identity of the cyber employees of Naji Technology Company and the thoughts of the system affiliated to the Cyber Corps



اسناد اختصاصی از تلاش برای دخالت در انتخابات آمریکا
وزارت خزانه داری آمریکا ایران را به تلاش برای دخالت در انتخابات آمریکا متهم کرد

اسناد اختصاصی ایران اینترنشنال از تلاش سپاه پاسداران برای دخالت در انتخابات آمریکا

3,013 views • Nov 21, 2021

44 DISLIKE SHARE DOWNLOAD SAVE

<https://youtu.be/JKsL4fJfdwI>

Sending the exclusive documents of Lab Dokhtegan to Iran International: Exposing the attempt of the terrorists of the Iliant Gostar unit headed by Shirinkar affiliated with the Cyber Corps under the command of Amir Lashgarian to interfere in the American elections



تحریم فعالان سایبری ایران به دلیل تلاش جهت نفوذ در انتخابات ریاست جمهوری ۲۰۲۰ ایالات متحده آمریکا

ترجمه
English

فیلتر بلاگ

واژه (های) کلیدی

دسته بندی ها

- دستورها
- سخنرانی ها
- بیانیه های مطبوعاتی
- رویدادها
- ویدئو

بر اساس تاریخ/سال



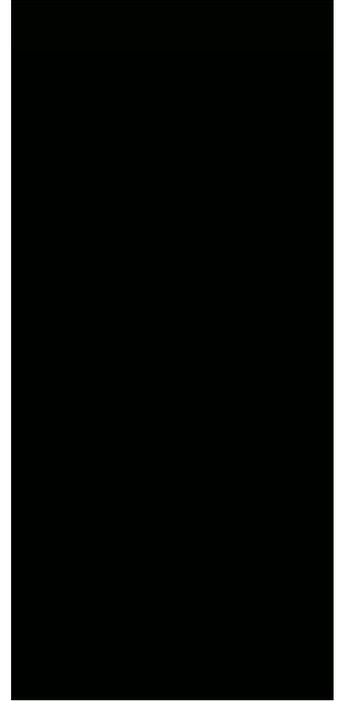
<https://ir.usembassy.gov/fa/statement-by-secretary-4/>

Following the revelation of the sewn lips: the sanctioning of terrorists active in the Iliant Gostar unit affiliated with the Cyber Corps for allegedly trying to interfere in the American elections

0:00 / 1:01



بدنبال افشاگری لب دوختگان: صدور کیفرخواست توسط وزارت دادگستری آمریکا بر علیه دو تروریست سپاه سایبری متهم دخالت در انتخابات آمریکا



0:00 / 1:23



ما گروه لب دوختگان تمام

se
n the US elections.
an.

18/01/2021 ما گروه لب دوختگان

وابسته به سپاه سایبری به

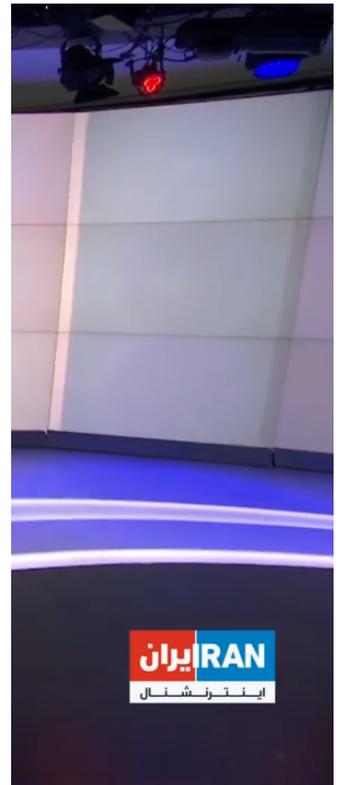
undermined
ar / Emen Net Pasargad).

تیزر | افشاگری قرن توسط لب دوختگان: تلاش واحد تروریستی ایلینت گستر به ریاست شیرینکار وابسته به سپاه سایبری به فرماندهی امیر لشگریان برای دخالت در انتخابات آمریکا

Double tap left or right to skip 10s



0:13 / 2:51



افشای تروریست شیرین محمد علی کارمند شرکت افکار سیستم در آژانس خبری ایران اینترنشنال

← → ↻ old.iranintl.com/ پاسداران-سپاه-سایبری-تیم-یک-رییس-هویت-افشای-اینترنشنال-ایران-ارسالی-به-ایران-اینترنشنال-افشای-هویت-رییس-یک-تیم-سایبری-سپاه-پاسداران/

ایران اینترنشنال | خبر و گزارش | صفحات ویژه | برنامه‌ها | جدول پخش | فرکانس‌ها | پخش زنده

شما صفحه ای از سایت قدیمی ایران اینترنشنال را مشاهده می کنید که دیگر به روز نمی شود. برای مشاهده سایت جدید به iranintl.com مراجعه کنید.

مرتبط

سپاه پاسداران برای دومین روز پیاپی ارتفاعات اقلیم کردستان عراق را گلوله باران کرد
۱۹ شهریور ۱۴۰۰

سپاه پاسداران مواضع احزاب کرد در اقلیم کردستان عراق را بمباران کرد
۱۸ شهریور ۱۴۰۰

فرمانده نیروی قدس سپاه: در افغانستان مهم این است که امنیت جمهوری اسلامی مخدوش نشود
۱۶ شهریور ۱۴۰۰

سپرمدن «وزارت سرکوب» به فرمانده ارتش سپاه
۲۶ مرداد ۱۴۰۰

اسناد افشا شده جدید از برنامه‌های جمهوری اسلامی برای حمله سایبری به نقاط مختلف جهان خبر می‌دهد
۵ مرداد ۱۴۰۰

تازه چه خبر؟



ایران | دوشنبه ۱ شهریور ۱۴۰۰

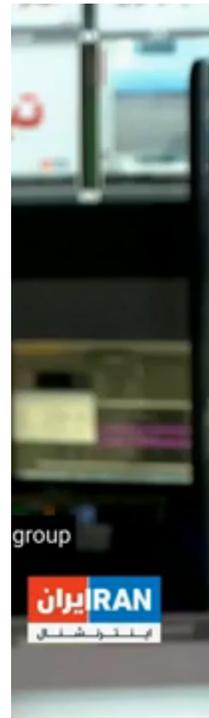
سند ارسالی به ایران اینترنشنال؛ افشای هویت رییس یک تیم سایبری سپاه پاسداران

گروه هکری **لب دوختگان** که درباره فعالیت‌های سایبری سپاه پاسداران افشاگری می‌کند، از طریق سامانه سوت بزن ایران اینترنشنال هویت رییس یک تیم سایبری سپاه را افشا کرده است.

<https://old.iranintl.com/%D8%A7%D9%8A%D8%B1%D8%A7%D9%86/%D8%B3%D9%86%D8%AF-%...>

ارسال اسناد اختصاصی لب دوختگان به ایران اینترنشنال | افشای هویت رییس یکی از تیمهای تروریستی سایبری گروه شهید کاوه: رضا سالاروند

0:00 / 2:51



افشای فعالیتها و هویتهای کارمندان دو شرکت تروریستی افکار سیستم و ناجی تکنولوژی وابسته به سپاه سایبری در آژانس خبری ایران اینترنشنال

iranintl • Following

گروه هکری لب دوختگان که درباره فعالیت های سایبری سپاه پاسداران افشاگری می کند، از طریق سامانه سوت بزین ایران اینترنشنال هویت رییس یک تیم سایبری سپاه را افشا کرده است. اسناد ارسالی، هویت رضا سالاروند را به عنوان رییس یک تیم هکری به نام «تیم اطلاعاتی ۱۳» را افشا می کند که زیر مجموعه «گروه شهید کاوه» قرار دارد و وابسته به فرماندهی سایبری سپاه پاسداران است.

هدف این گروه تهیه بانک اطلاعاتی از اهدافی مانند کشتی های باری، پمپ بنزین ها و مراکز کنترل تبادلات دریایی در آمریکا و سایر نقاط بنا هدف حمله سایبری به آنهاست.

سند ارسالی گروه لب دوختگان به ایران اینترنشنال نشان می دهد که سالاروند رییس «تیم اطلاعاتی ۱۳» متولد ۱۳ اسفند ۱۳۶۹ و

سند ارسالی به ایران اینترنشنال؛
افشای هویت رییس یک تیم
سایبری سپاه پاسداران

Liked by narimangharib and 138,862 others

AUGUST 23, 2021

Add a comment... Post

<https://www.instagram.com/p/CS6QzKmCI5T/>

ارسال اسناد اختصاصی لب دوختگان به ایران اینترنشنال | افشای هویت رییس یکی از تیمهای تروریستی سایبری گروه شهید کاوه: رضا سالاروند

← Tweet

Amin Sabeti | امین تابتی @AminSabeti

لب دوختگان برداشته برای یکی که به عنوان اطلاعات سپاه کار می‌کنه دسته گل در خونه @LabDookhtegan2

Following

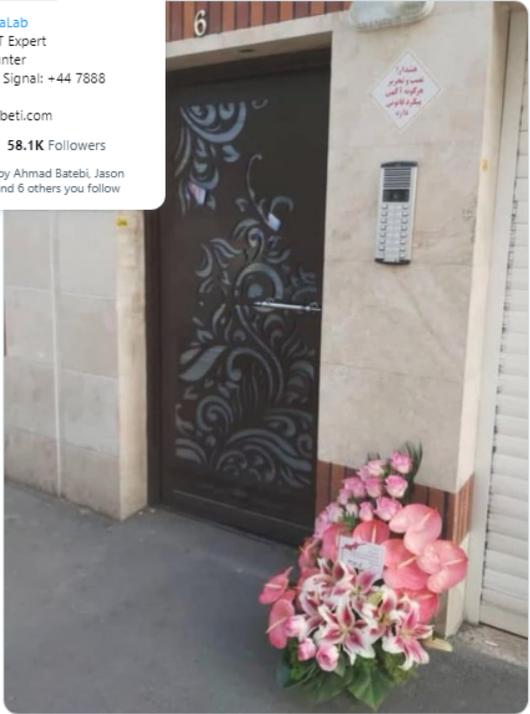
Amin Sabeti | امین تابتی @AminSabeti Follows you

Founder @CertfaLab
#Iran's OSINT Expert
#Iran APT Hunter
WhatsApp & Signal: +44 7888 865050
me@aminsabeti.com

743 Following 58.1K Followers

Followed by Ahmad Batebi, Jason Brodsky, and 6 others you follow

Tweet



Lab_Dookhtegan @LabDookhtegan2

<https://twitter.com/AminSabeti/status/1413392347698769921>

فعالیت میدانی لب دوختگان: تماس با همسر محمی علی میثمی، یکی از تروریستهای واحد شهید کاوه وابسته به سپاه سایبری

- Home
- Explore
- Notifications
- Messages
- Bookmarks
- Lists
- Profile
- More

Tweet

Tweet

me@narimangharib.com @NarimanGharib

Following

me@narimangharib.com @NarimanGharib

Britain-based Iranian Activist
Cyber Espionage Investigator
#KeptlON

نریمان غریب
Signal/WhatsApp/Telegram: +1 (628) 3000015

3,238 Following 85.3K Followers

Followed by PS752Justice, Azadah #براندازم, and 10 others you follow

اختصاصی @LabDookhtegan2 : سند مر
 عملیات " هک @IranIntl . سال گذشته
 شرکت ایلینت گستر درخواست کرد سیس
 خبری را به هدف اخلاص در پخش زنده این
 محتوای دروغین و تغییر و حذف فیلم‌های
 نماید.
drive.google.com/file/d/1HDjVR-...

شیکه معاند ایران اینترنشنال (ational)
 بزرگترین شبکه های سازمان دهی شده
 این شبکه متعلق به شرکت "Volant Media"
 العبدالکریم" و تمامی سرمایه گذاران آن اهل عربستان
 سعودی میباشد. این شبکه معاند نقش مهمی در بر هم
 ریختن نظم کشور، دامن زدن به جریان‌های انحرافی،
 تحریک مخاطبان و بزرگنمایی بحران در مناطق مختلف
 ایران و شایعه پراکنی در منطقه و ایران را دارد.
 این رسانه معاند قابلیت انشار اخبار در ماهواره،
 سایت(به صورت زنده)، رادیو، شبکه های اجتماعی
 Twitter و Instagram دارد.
 لازم به ذکر است که شبکه ایران اینترنشنال نقش مهمی
 در شورش های اخیر آذر ماه در ایران داشت.

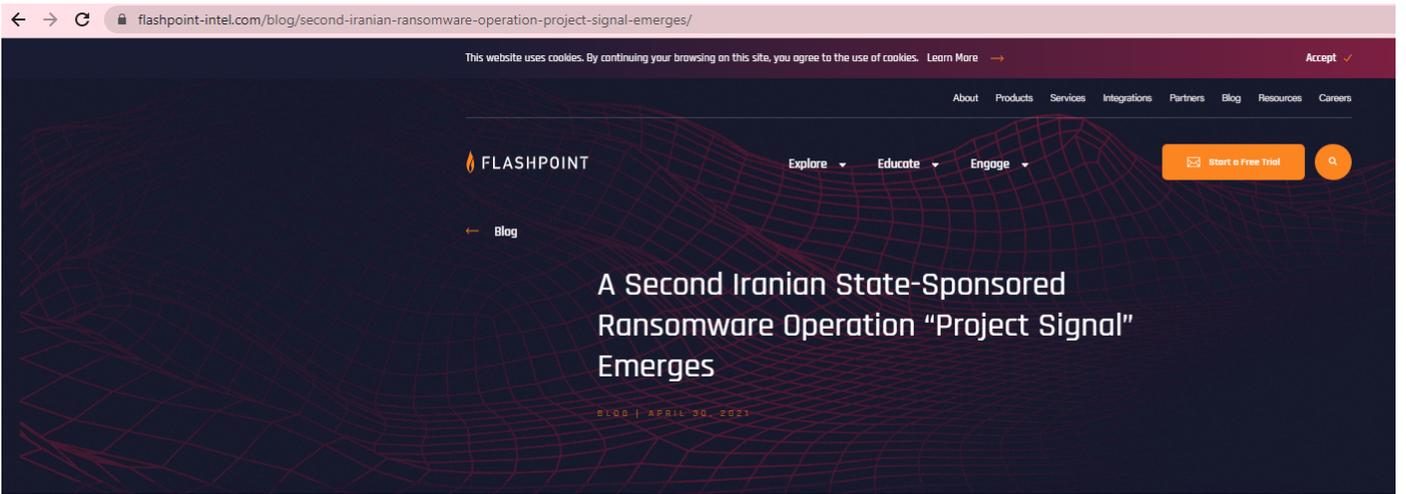
معرفی سایت



Lab_Dookhtegan @LabDookhtegan2

<https://twitter.com/NarimanGharib/status/1410227759905902597>

افشای برنامه ریزی تزوریستهای واحد ایلینت گستر به هدف هک آژانس خبری ایران اینترنشنال



Leaked Documents Confirm Second Iranian State-Sponsored Ransomware Operation

Flashpoint has validated recently leaked documents that indicate Iran's Islamic Revolutionary Guard Corps (IRGC) was operating a state-sponsored ransomware campaign through an Iranian contracting company called "Emen Net Pasargard" (ENP) (aka "Imannet Pasargard," "Iliant Gostar Iranian," "Eeleyenat Gostar Iranian"). These three documents were originally leaked between March 19 and April 1, 2021, by the Iranian dissident group **Lab Dookhtegan** famous for providing highly reputable intelligence on Iranian state-sponsored cyber programs.

<https://www.flashpoint-intel.com/blog/second-iranian-ransomware-operation-project-signal-emer...>

افشای پروژه سیگنال توسط لب دوختگان: پروژه مربوط به واحد تروریستی ایلینت گستر



0:00 / 2:30



گروه لب دوختگان در آژانس خبری منوتو

ifmat.org/01/25/lab-dookhtegan-exposed-irgc-terrorist-who-is-responsible-for-the-shutdown-of-the-ukrainian-plane/

Wednesday, Feb 9, 2022 Breaking News: Iran 'on the verge of an explosion,' says lawmaker

Home Press Releases Black List Gray List Banking Provocation Dark Network Research News Join Us



Lab Dookhtegan Exposed IRGC Terrorist Who Is Responsible For The Shutdown Of The Ukrainian Plane

January 25, 2022 | Iran Regime Threats | News / Threats /

Select Language: 

One of the central perpetrators of this terrorist activity (the destruction of a Ukrainian plane) is a person who is responsible for the bereavement of 176 families and whose hands are stained with the blood of 176 innocent passengers:

Brigadier General Fereydoun Mohammadi Saghaei, Deputy Coordinator of the IRGC Aerospace Command

Father's name: Lutfullah
National Code: 1861060386

INVOLVED IN THIS ARTICLE:



FEREYDOUN MOHAMMADI SAGHAEI



IRGC - AEROSPACE FORCE

<https://www.ifmat.org/01/25/lab-dookhtegan-exposed-irgc-terrorist-who-is-responsible-for-the-s...>

افشای فریدون سقایی توسط لب دوختگان در ifmat: فریدون سقایی معاون هماهنگ کننده هوا فضای سپاه پاسداران، قاتل اصلی انهدام عمدی هواپیمای اوکراینی

marcoramilli.com/2021/05/01/muddywater-binder-project-part-1/

MR

Home About Books Contact Press and Media

MuddyWater: Binder Project (Part 1)

ADWIND, APT, CYBER CRIME, CYBERSECURITY MAY 1, 2021

According to **Lab Dookhtegan**, which you might remember him/their from **HERE**, **HERE** and **HERE**, Binder is a project related to IRGC cyber espionage group build for trojanize google apps (APK). The application "trojanization" is a well-known process which takes as input a good APK and a code to inject (a RAT, for example). The system is able to unbuild the original APK and to inject the RAT into the "good application". The result is a Trojan which could compromise an unaware target. Indeed unaware users by opening up the trojanized APK will run the desired application as well as the RAT in a background process by starting up the infection chain. MuddyWater is notoriously alleged linked to IRGC (**HERE**) as main contractors so what this blog post. According with ClearSky (Report **HERE**) Iranian cyber espionage forces are increasing their mobile abilities by meaning they are investing in Mobile (RAT and Trojan) development on either iOS and Android operative systems. All these information are rolling on the same direction and they are building up a concrete base to start to analyze what **Lab Dookhtegan** released over the past weeks.



<https://marcoramilli.com/2021/05/01/muddywater-binder-project-part-1/>

افشای پروژه بایندر توسط لب دوختگان: پروژه مربوط به واحد ایلینت گستر به ریاست شیرینکار

Researchers Uncover Iranian State-Sponsored Ransomware Operation

May 03, 2021 Ravie Lakshmanan



Iran has been linked to yet another state-sponsored ransomware operation through a contracting company based in the country, according to new analysis.

"Iran's Islamic Revolutionary Guard Corps (IRGC) was operating a state-sponsored ransomware campaign through an Iranian contracting company called 'Emen Net Pasargard' (ENP)," cybersecurity firm Flashpoint said in its findings summarizing three documents leaked by an anonymous entity named Read My Lips or Lab Dookhtegan between March 19 and April 1 via its Telegram channel.

Security for a suddenly remote workforce

Learn more AT&T Business

Netsurion

IDC Tech Spotlight: It's Time to Consolidate Security Technology

Learn why IT Security leaders are consolidation their tech stacks, and how it benefits their security maturity.

Download Now

Popular This Week

New 0-Day Attack Targeting



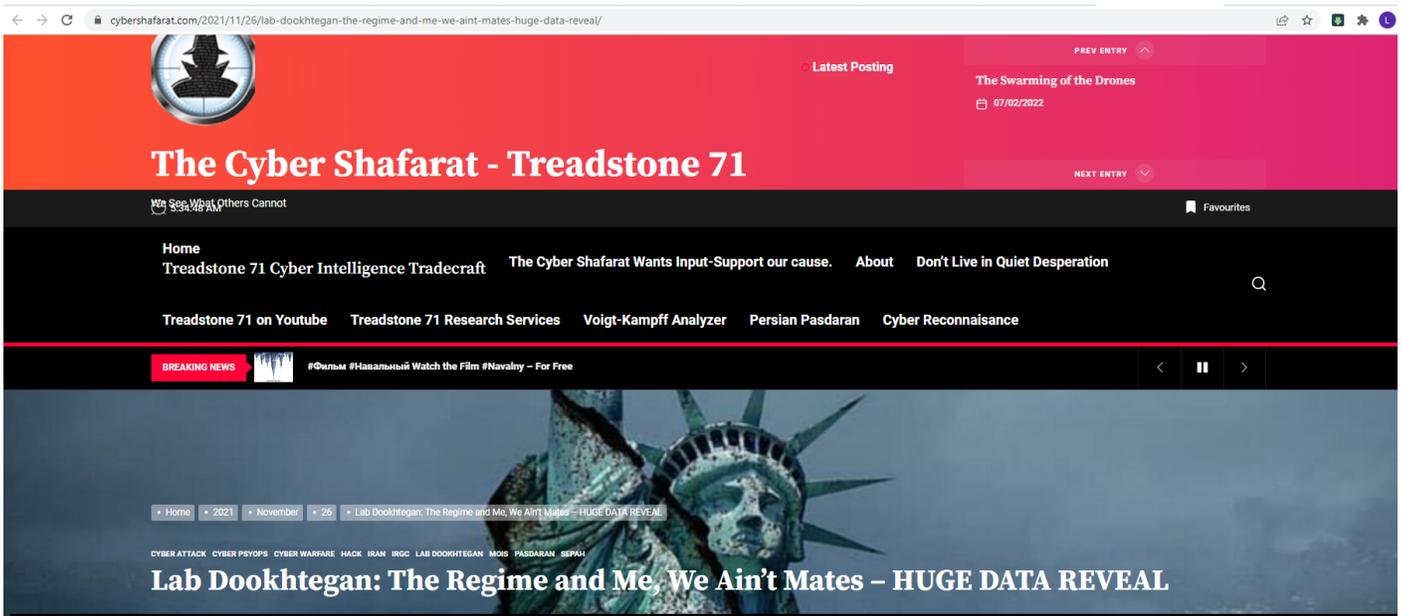
https://go.thn.li/crowdsec-728

<https://thehackernews.com/2021/05/researchers-uncover-iranian-state.html>

افشاگری فعالیت‌های تروریستی سپاه سایبری توسط لب دوختگان در سایت هکر نیوز

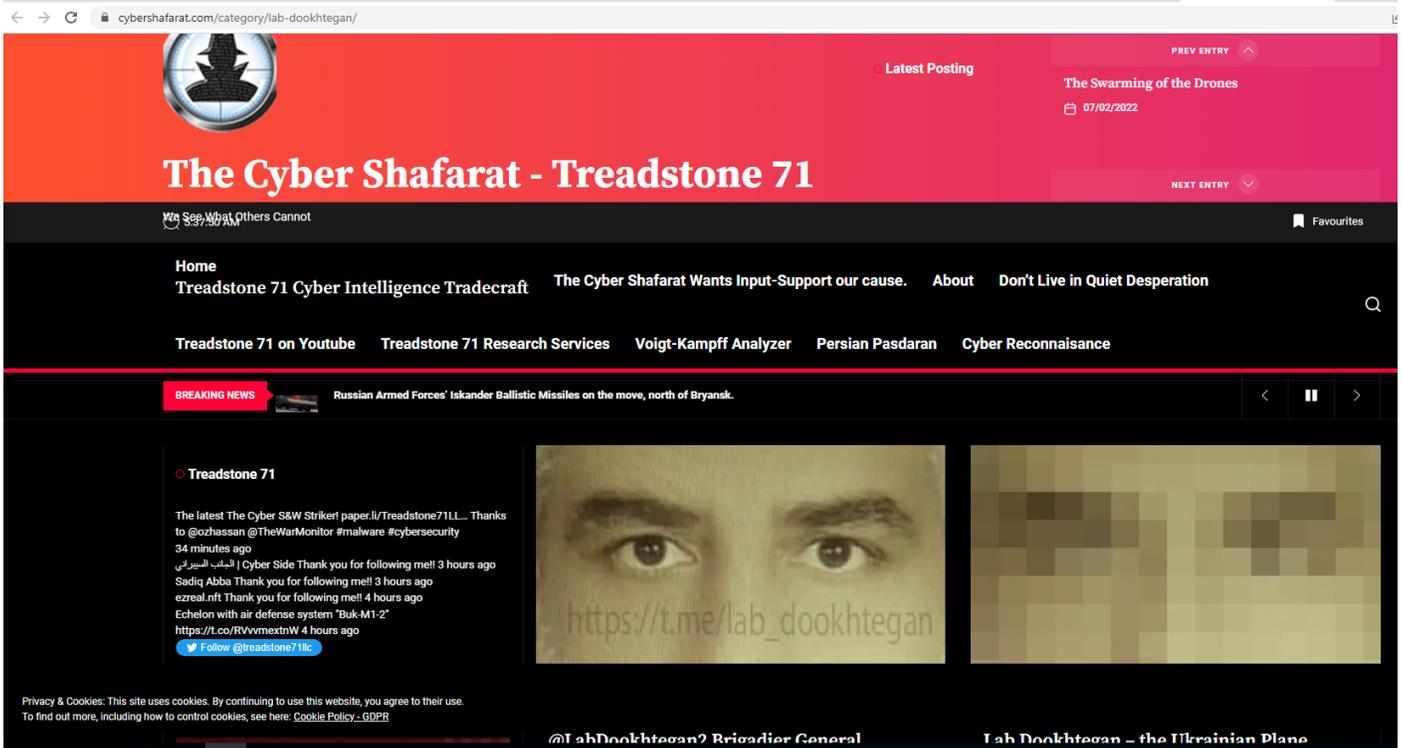
<https://www.bankinfosecurity.com/irans-military-reportedly-backs-ransomware-campaign-a-16517>

افشاگری فعالیت‌های تروریستی سپاه سایبری توسط لب دوختگان در سایت Bank Info Security



<https://cybershafarat.com/2021/11/26/lab-dookhtegan-the-regime-and-me-we-aint-mates-huge-...>

Exposing the terrorist activities of the Cyber Corps by Lab Dokhtegan on the Cyber Shafarat website



<https://cybershafarat.com/category/lab-dookhtegan/>

The exposure of Fereydoun Saqqaei by Lab Dokhtegan in Cyber Shafarat: Fereydon Soghaei, the deputy air space coordinator of the IRGC, the main killer of the deliberate destruction of the

The image shows a screenshot of a Twitter post from the account 'Thread Reader App' (@threadreaderapp). The post is titled 'Tweet' and contains the text: 'I'm a 🤖 to help you read threads more easily. Reply to any tweet of a thread and mention me with the "unroll" keyword and I'll give you a link back 😊'. The account has 1,276 following and 538.5K followers. A pop-up overlay is visible over the tweet, showing the account's profile picture, name, and a 'Following' button. Below the tweet, there is a promotional banner for 'Thread Reader App' with the text 'Twitter threads easily!' and a list of features: 'Save great threads to read later!' and 'To unroll, tweet "@threadreaderapp unroll"'. The banner also features a blue robot icon and a red heart icon with the word 'unroll' next to it. At the bottom of the banner, it says 'threadreaderapp.com Read and Share Twitter Threads easily! Thread Reader helps you read and share the best of Twitter Threads'. The user's profile picture and name 'Lab_Dookhtegan @LabDookhtegan2' are visible at the bottom left of the tweet.

<https://twitter.com/threadreaderapp/status/1464958550720061440>

Thread Reader App on Twitter

