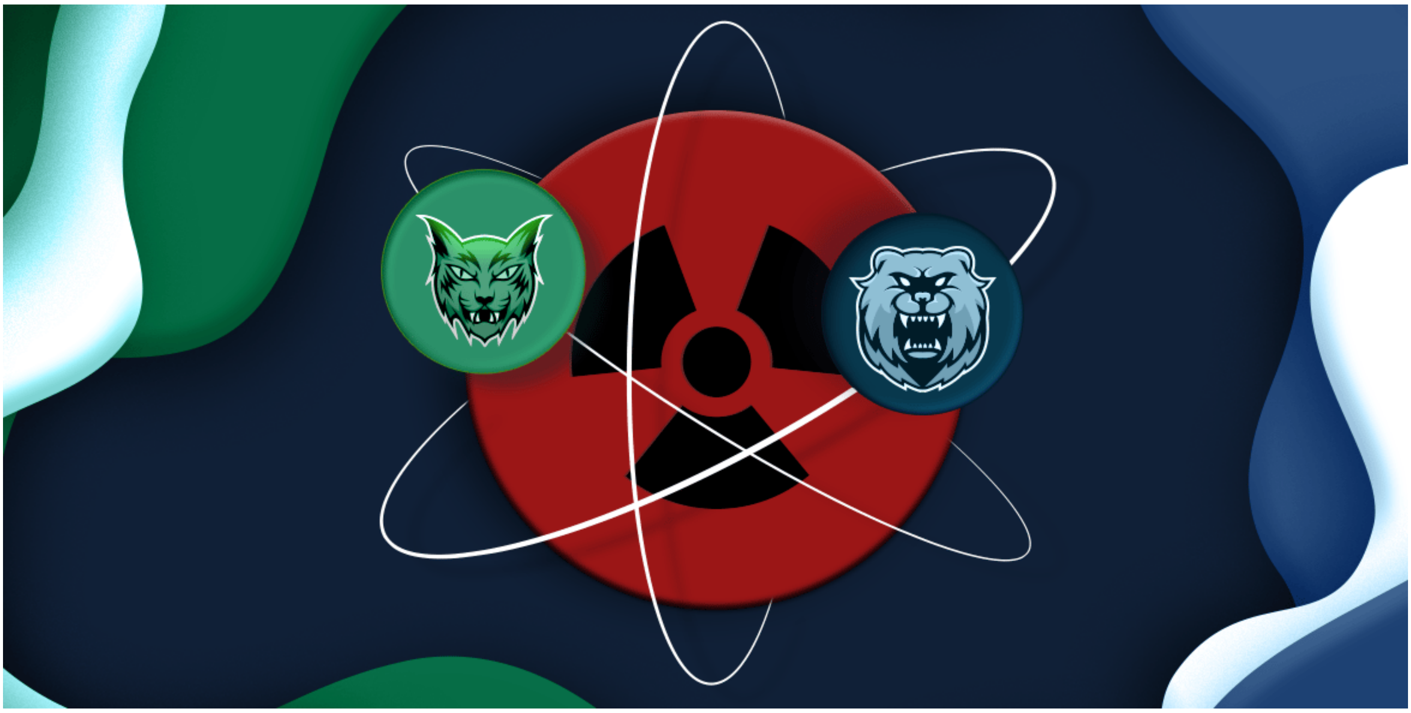
Sanctioned deals: the Irano-Russian connection under Ankara's supervision. Analysis of the NPPD leak

Cluster25 Threat Intel Team ⁝⁝ 11/7/2022



On October 22nd, during the usual OSInt monitoring, Cluster25 detected the Farsi speaking hacktivist TA known as **Black Reward** claiming to have hacked into an email account belonging to employees of the Iranian Nuclear Power Production and Development (NPPD), exfiltrating and then leaking confidential data related as the group stated ”Contracts of Iran Atomic Energy Production and Development Company (NPPD) with domestic and foreign partners, management and operational schedules of Bushehr power plant, identity details and paystub of engineers and employees of the company as well as passports and visas of Iranian and Russian specialists of Bushehr power plant”.

Before talking about the leak, let’s outline the geopolitical background on the energy deals that are being signed around the world, between Moscow, Teheran, and Ankara.

Recently as the energetic crisis is getting worse and the tension around the Ukrainian conflict is rising, during the period between the 12nd and the 23rd of October 2022, Turkish President Tayyip Erdogan has been quite active in strengthening economic ties and partnerships with both countries, Iran, and Russia, which will likely get to Turkey more accountability and power among the Arab Countries, and the Caucasus area.

On October 19th, 2022, President Putin and President Erdogan reached an agreement on the creation of a gas hub, permitting Europe to use Russian gas passing through the natural gas pipeline **TurkStream**. In the following days, Ankara proposed to President Putin the creation of an oil hub, managing to purchase and transport oil from Russia without the need for Western financing or insurance, as declared by Turkish Finance Minister Nureddin Nebati. As for the gas hub, also the creation of a Turkish oil hub will likely be useable by European countries, offering tools and a platform for trade, which will likely at the same time ease the energetic pressure among Europe and increase Erdogan’s influence in the international scenario.

Along with the Russian-Turkish gas hub accord, President Erdogan has reached several agreements with Iran in the fields of gas exports, in addition to the already 10 billion cubic meters of gas per year (circa) Iranian supply, through the Tengiz-Ankara gas pipeline. As reported by the National Gas Company of Iran Mohammad Reza Jolayi "In accordance with these agreements, various activities related to the export of Iranian gas to Turkey will be carried out over the next six months with the coordination of the parties."

Another commercial way that these countries are exploiting in the recent years is the International North–South Transport Corridor (INSTC). On May 16th, 2002, Russia, Iran, and India signed the agreement for the INSTC, a 7,200-km-long multi-mode network of ship, rail, and road route for moving freight between India, Iran, Azerbaijan, Russia, Central Asia, and Europe. The objective of the study was to identify and address key bottlenecks, such as the Suez Canal, saving both time and money. Opening a huge highway for goods and services, mimicking the ancient glories of the Silk Road, interconnecting these countries, and saving a lot of money in the meantime.

Both Russia and Iran are under international sanctions, while Turkey has gained that amount of power on the geopolitical arena that can bend the international law on its favor. Stating so, it's natural that the three would cooperate in different sectors, from the import/export of goods to the military and weapon sector, and of course the energy sector, given the double ended ties between Tehran, Moscow and Ankara.

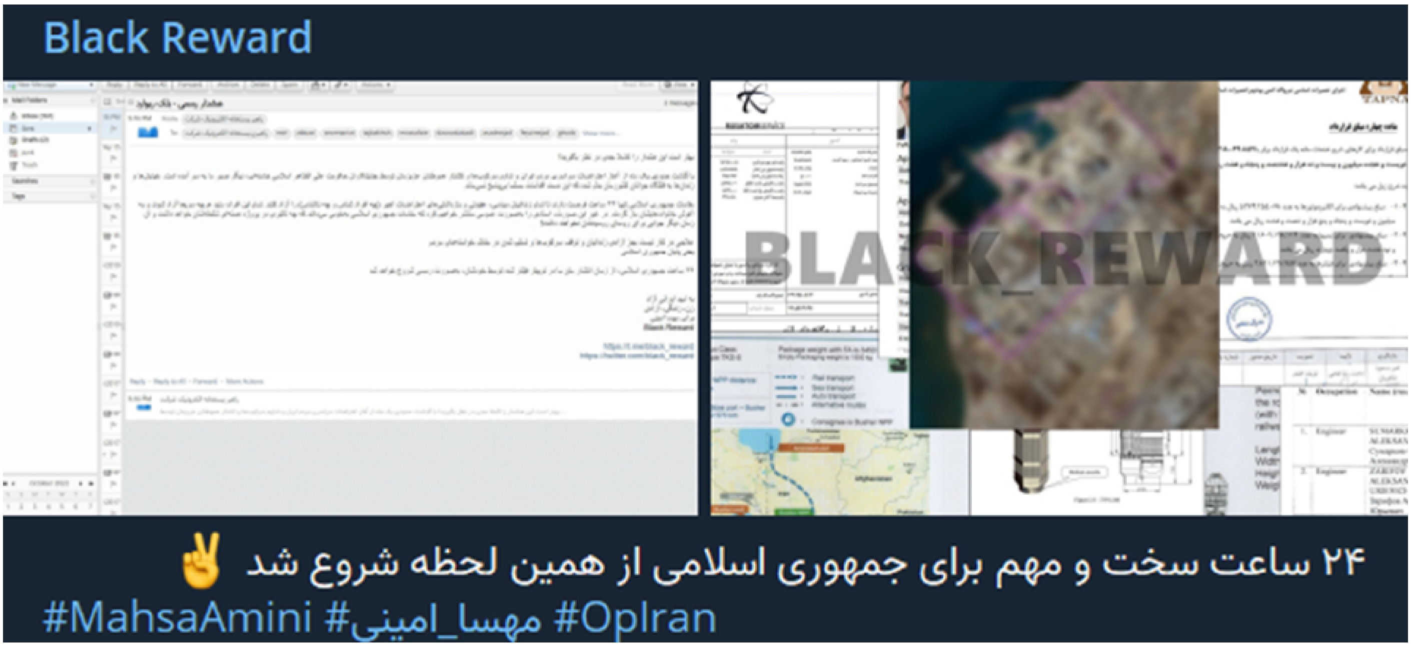
Talking about the energy sector, following the information found in the data-leak shared by Black Reward it's now clear how the Kremlin has a really in deep collaboration within the atomic energy sector and how Rosatom and the Iranian nuclear program are connected. Analyzing the documents, Cluster25 found several maps underlining the uranium logistics from Russia to Iran and vice versa that will follow the INSTC routes.

Summarizing what happened, on October 22nd, the Iranian hacktivist group **Black Reward** exposed several confidential documents related to the Iranian government's nuclear project with the Russian Federation. This was an act of hacktivism linked to the ongoing demonstrations and riots shaking up the Iranian soil, where people are protesting the behaviors towards the civilians of the Government and the Islamic Revolutionary Guard Corps (IRGC).

This whole wave of manifestations started on September 18th in response to Mahsa Amini's death on September 16th.

As reported through its social profile and channels, the Iranian hacktivist group exposed 75.18 GB of data after the 24 hours threat deadline given to NPPD in exchange for the liberation of the political prisoners detained after the riots.

The leak contains images, visas requests for Russian engineers to go to Iran, their passports, WhatsApp chats between Iranian and Russian engineers about technical drawings, Assessments, emails, and others.



Black Reward

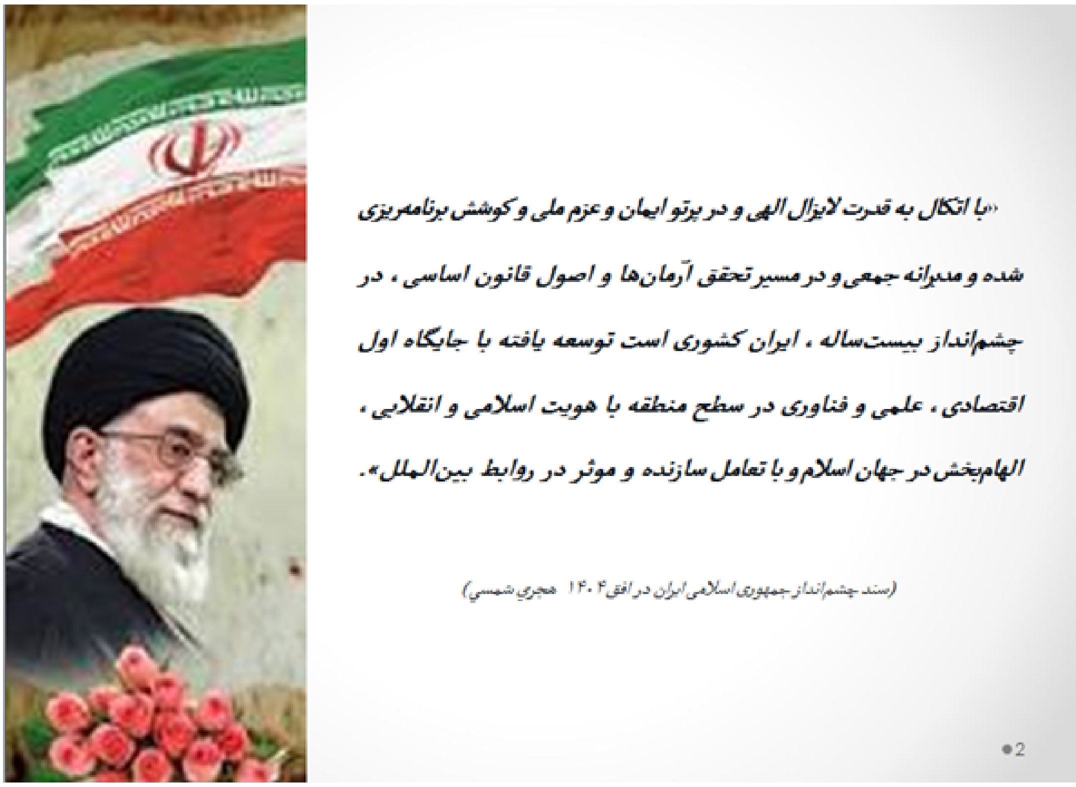
۲۴ ساعت سخت و مهم برای جمهوری اسلامی از همین لحظه شروع شد ✌️
#MahsaAmini #مهسا_امینی #OpIran

The revindication of the leak by the group.

INSIGHTS

C25 analyzed most of the data leak consisting in email attachments, around 42k files. The majority of the files are technical drawings, internal documents, curricula and chats. Interesting to note how a lot of these documents are both in Russian and English, linked to Russian experts in the atomic sphere.

Following some screenshots taken from the leaked files.



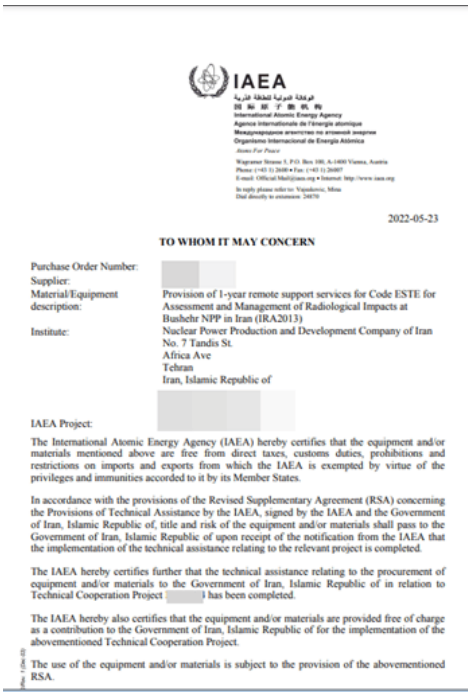
«با اتکال به قدرت لایزال الهی و در پرتو ایمان و عزم ملی و کوشش برنامه‌ریزی
شده و مدبرانه جمعی و در مسیر تحقق آرمان‌ها و اصول قانون اساسی ، در
چشم‌انداز بیست‌ساله ، ایران کشوری است توسعه یافته با جایگاه اول
اقتصادی ، علمی و فناوری در سطح منطقه با هویت اسلامی و انقلابی ،
الهام‌بخش در جهان اسلام و با تعامل سازنده و موثر در روابط بین‌الملل».

(سند چشم‌انداز جمهوری اسلامی ایران در افق ۱۴۰۴ هجری شمسی)

•2

Relying on the eternal power of God and in the light of faith and national determination and planned and deliberate collective effort and on the path to realizing the ideals and principles of the constitution, in the twenty-year perspective, Iran is a developed country with the first economic, scientific and technological position at the level The region with Islamic and revolutionary identity, inspiring in the Islamic world and with constructive and effective interaction in international relations. (Document on the vision of the Islamic Republic of Iran in the horizon of 1404 AH)”

Iran Nuclear program is monitored by the International Atomic Energy Agency (IAEA) and the World Association of Nuclear Operators (WANO). And this is no news for the scope of this report. In fact, on April 13th the WANO declared the successful pass of their assessments of the Bushehr Nuclear Plant.



IAEA
الوكالة الدولية للطاقة الذرية
国际原子能机构
International Atomic Energy Agency
Agence internationale de l'énergie atomique
Международное агентство по атомной энергии
Organismo Internacional de Energía Atómica
Atoms For Peace

Wagramer Strasse 5, P.O. Box 100, A-1400 Vienna, Austria
Phone: (+43 1) 2600 • Fax: (+43 1) 26007
E-mail: Official.Mail@iaea.org • Internet: http://www.iaea.org

In reply please refer to: Vujaskovic, Mina
Dial directly to extension: 24870

2022-05-23

TO WHOM IT MAY CONCERN

Purchase Order Number:	[redacted]
Supplier:	
Material/Equipment description:	Provision of 1-year remote support services for Code ESTE for Assessment and Management of Radiological Impacts at Bushehr NPP in Iran (IRA2013)
Institute:	Nuclear Power Production and Development Company of Iran No. 7 Tandis St. Africa Ave Tehran Iran, Islamic Republic of
IAEA Project:	[redacted]

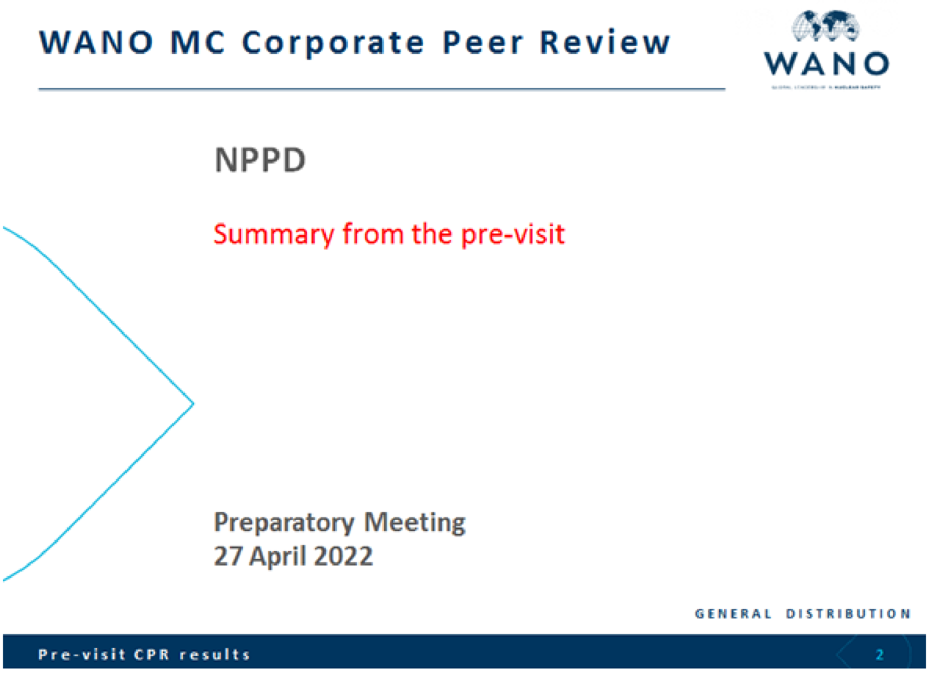
The International Atomic Energy Agency (IAEA) hereby certifies that the equipment and/or materials mentioned above are free from direct taxes, customs duties, prohibitions and restrictions on imports and exports from which the IAEA is exempted by virtue of the privileges and immunities accorded to it by its Member States.

In accordance with the provisions of the Revised Supplementary Agreement (RSA) concerning the Provisions of Technical Assistance by the IAEA, signed by the IAEA and the Government of Iran, Islamic Republic of, title and risk of the equipment and/or materials shall pass to the Government of Iran, Islamic Republic of upon receipt of the notification from the IAEA that the implementation of the technical assistance relating to the relevant project is completed.

The IAEA hereby certifies further that the technical assistance relating to the procurement of equipment and/or materials to the Government of Iran, Islamic Republic of in relation to Technical Cooperation Project [redacted] has been completed.

The IAEA hereby also certifies that the equipment and/or materials are provided free of charge as a contribution to the Government of Iran, Islamic Republic of for the implementation of the abovementioned Technical Cooperation Project.

The use of the equipment and/or materials is subject to the provision of the abovementioned RSA.



WANO MC Corporate Peer Review

WANO

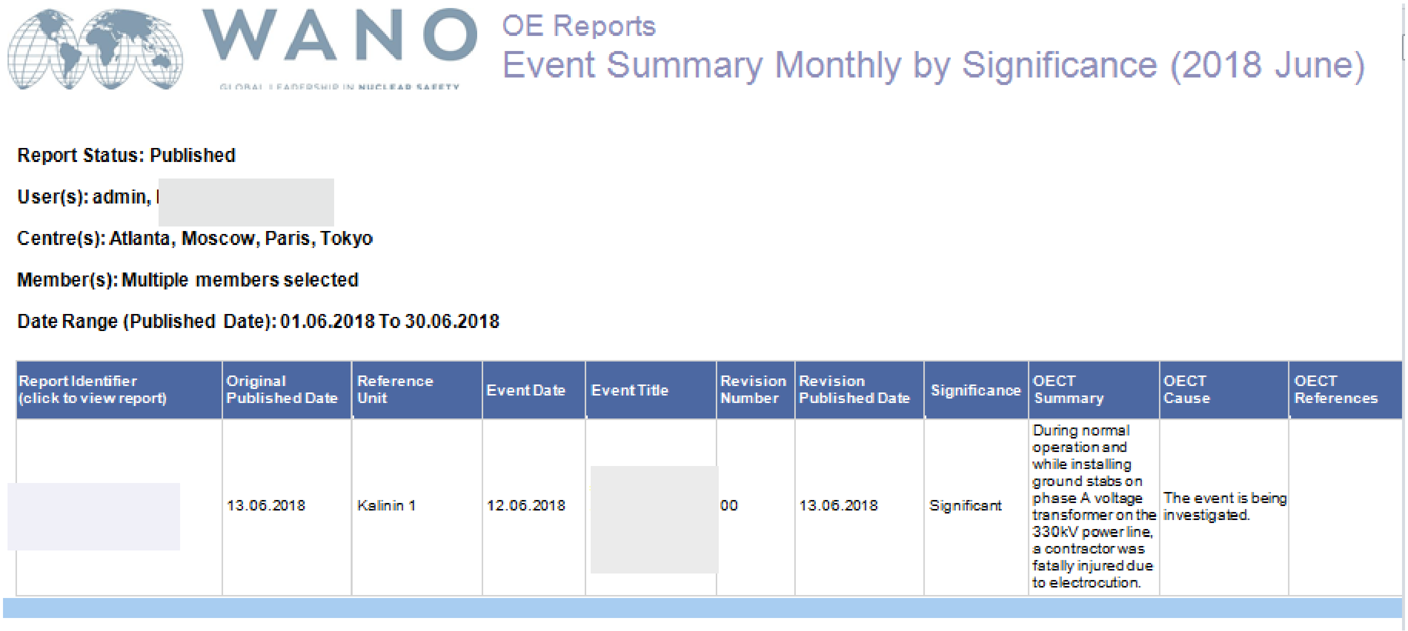
NPPD

Summary from the pre-visit

Preparatory Meeting
27 April 2022

GENERAL DISTRIBUTION

Pre-visit CPR results 2



WANO
GLOBAL LEADERSHIP IN NUCLEAR SAFETY

OE Reports
Event Summary Monthly by Significance (2018 June)

Report Status: Published

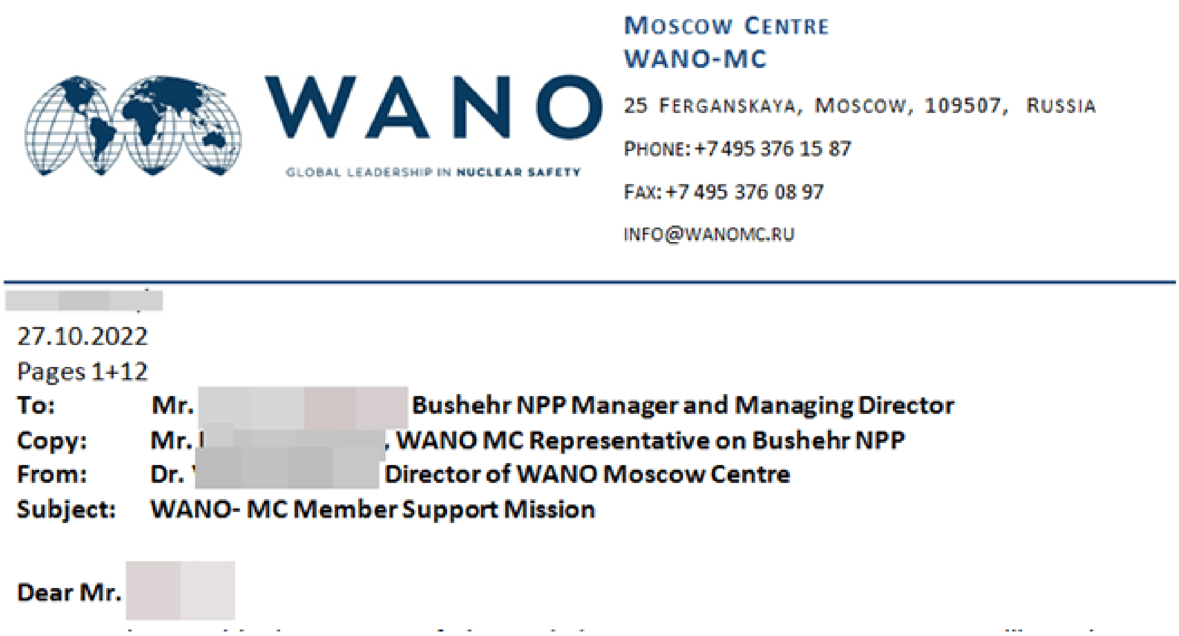
User(s): admin, [redacted]

Centre(s): Atlanta, Moscow, Paris, Tokyo

Member(s): Multiple members selected

Date Range (Published Date): 01.06.2018 To 30.06.2018

Report Identifier (click to view report)	Original Published Date	Reference Unit	Event Date	Event Title	Revision Number	Revision Published Date	Significance	OECT Summary	OECT Cause	OECT References
[redacted]	13.06.2018	Kalinin 1	12.06.2018	[redacted]	00	13.06.2018	Significant	During normal operation and while installing ground stabs on phase A voltage transformer on the 330kV power line, a contractor was fatally injured due to electrocution.	The event is being investigated.	



WANO
GLOBAL LEADERSHIP IN NUCLEAR SAFETY

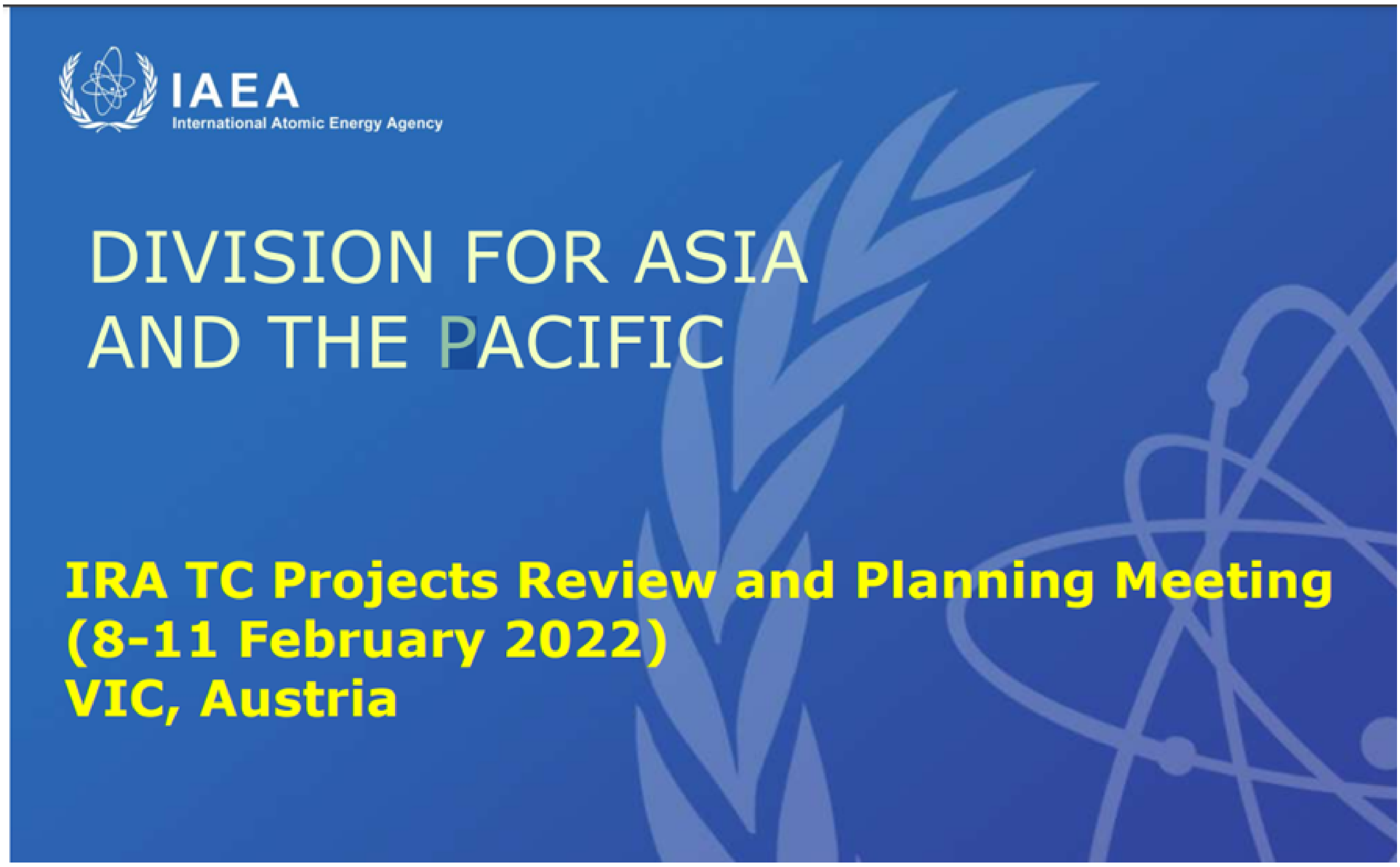
Moscow Centre
WANO-MC

25 Ferganskaya, Moscow, 109507, Russia
Phone: +7 495 376 15 87
Fax: +7 495 376 08 97
INFO@WANOMC.RU

[redacted]
27.10.2022
Pages 1+12

To:	Mr. [redacted] Bushehr NPP Manager and Managing Director
Copy:	Mr. [redacted], WANO MC Representative on Bushehr NPP
From:	Dr. [redacted] Director of WANO Moscow Centre
Subject:	WANO- MC Member Support Mission

Dear Mr. [redacted]

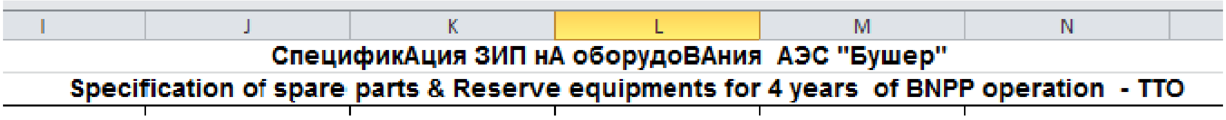


IAEA
International Atomic Energy Agency

DIVISION FOR ASIA AND THE PACIFIC

IRA TC Projects Review and Planning Meeting (8-11 February 2022) VIC, Austria

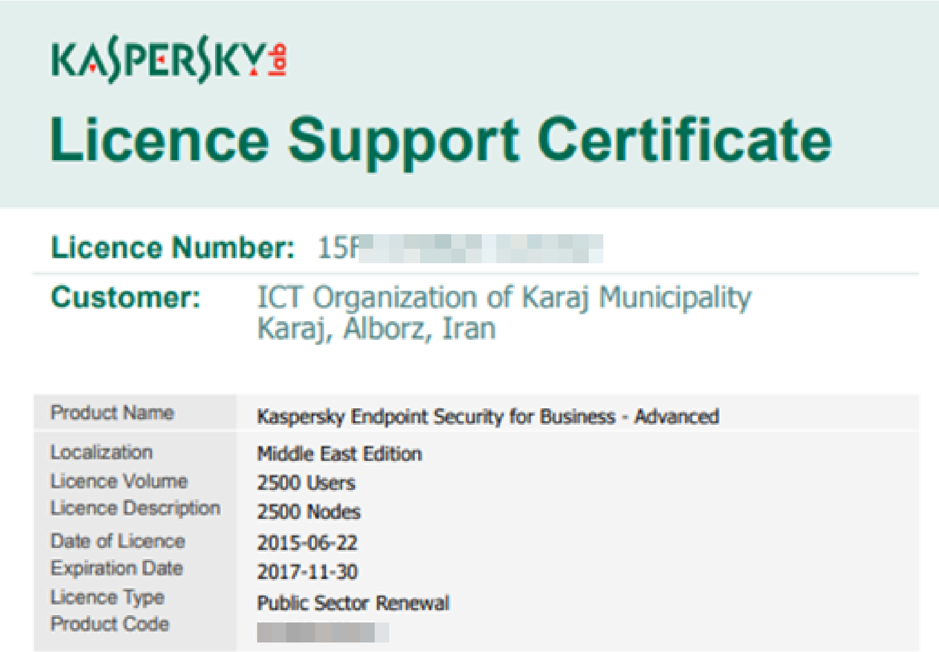
Some of the files are showing a clear link with Russia, starting from antivirus licenses to Russian experts' passports, Irani visas for Russian citizens to lists of spare parts and other Russian language documents.



I	J	K	L	M	N

СпецификАция ЗИП нА оборудоВАния АЭС "Бушер"

Specification of spare parts & Reserve equipments for 4 years of BNPP operation - TTO



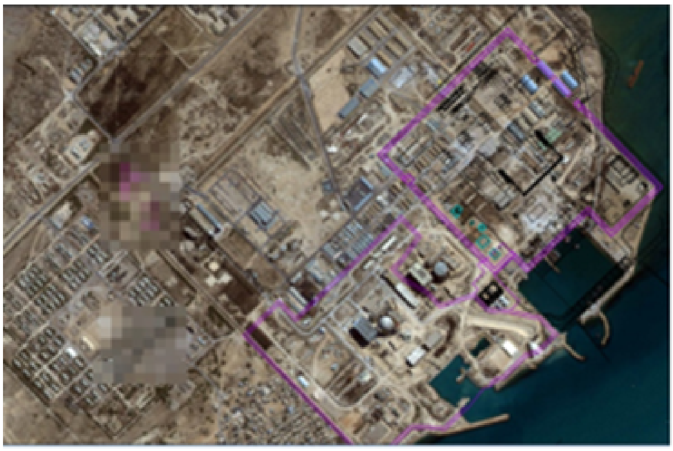
KASPERSKY lab

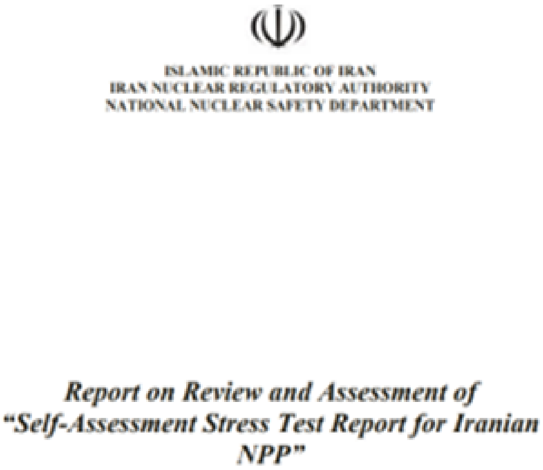
Licence Support Certificate

Licence Number: 15F[redacted]

Customer: ICT Organization of Karaj Municipality
Karaj, Alborz, Iran

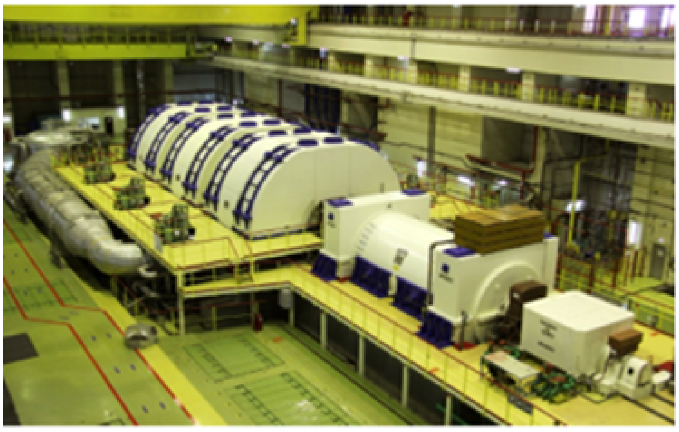
Product Name	Kaspersky Endpoint Security for Business - Advanced
Localization	Middle East Edition
Licence Volume	2500 Users
Licence Description	2500 Nodes
Date of Licence	2015-06-22
Expiration Date	2017-11-30
Licence Type	Public Sector Renewal
Product Code	[redacted]

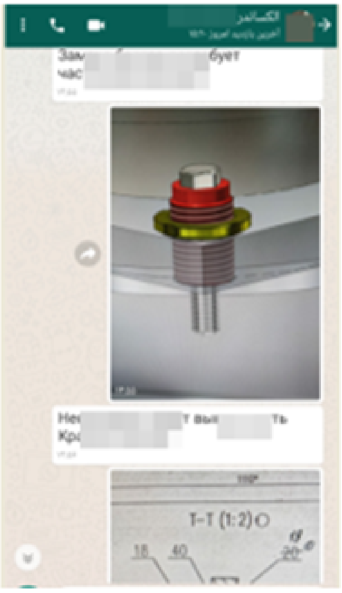




ISLAMIC REPUBLIC OF IRAN
IRAN NUCLEAR REGULATORY AUTHORITY
NATIONAL NUCLEAR SAFETY DEPARTMENT

Report on Review and Assessment of "Self-Assessment Stress Test Report for Iranian NPP"

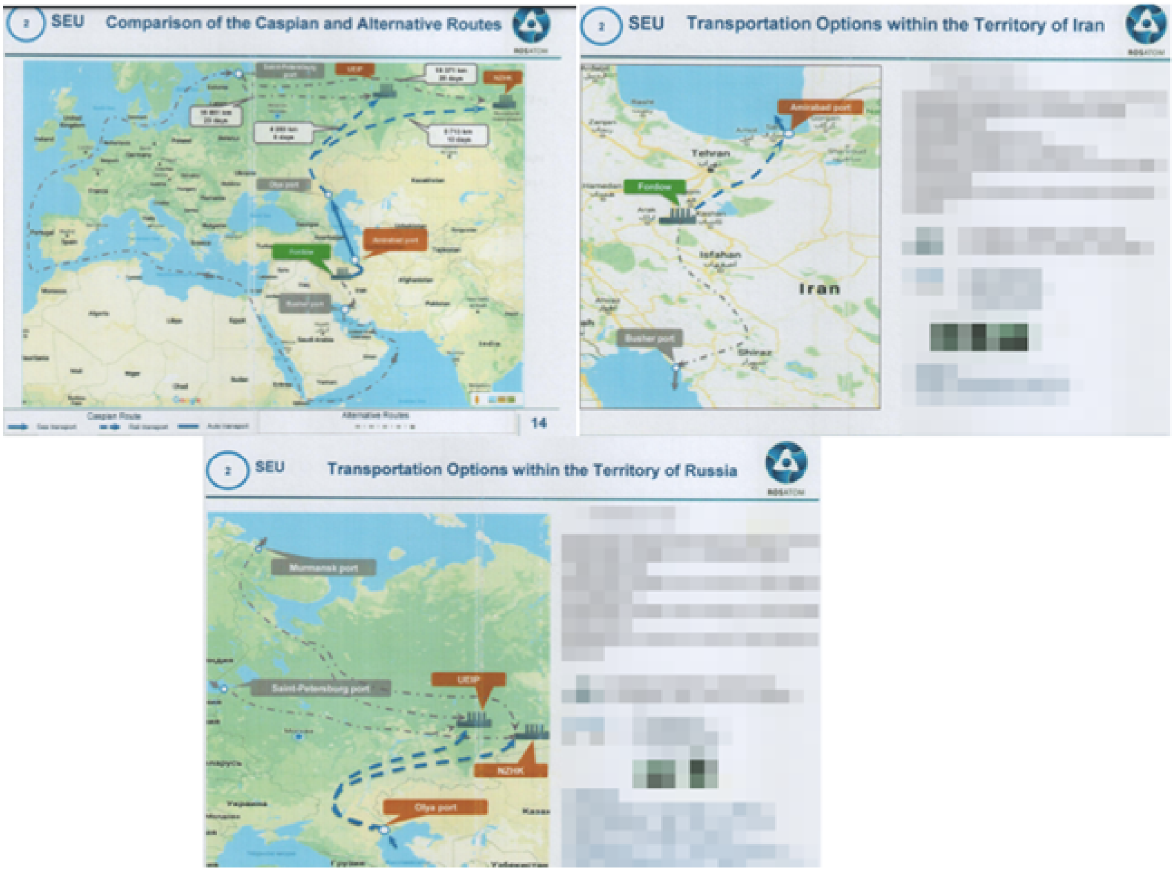




[redacted]

[redacted]

Bushehr Nuclear Power Plant map and internal photos, technical drawings, internal documents as shared by the group to Russian speaking individuals



2 SEU Comparison of the Caspian and Alternative Routes

14

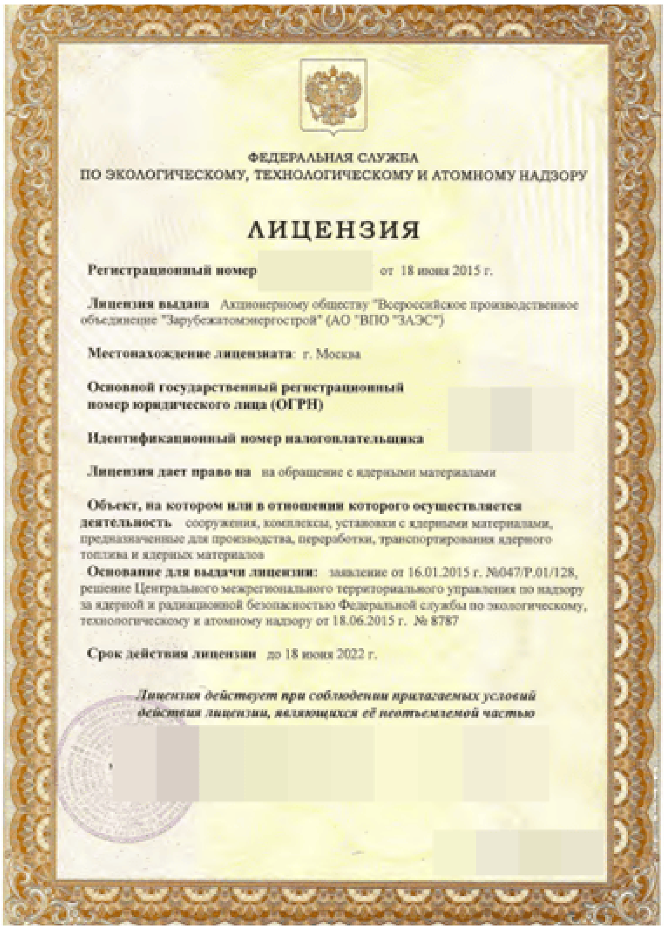
2 SEU Transportation Options within the Territory of Iran

[redacted]

2 SEU Transportation Options within the Territory of Russia

[redacted]

Transportation options for Uranium along the INSTC from Russia to Iran and vice versa



ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ЭКОЛОГИЧЕСКОМУ, ТЕХНОЛОГИЧЕСКОМУ И АТОМНОМУ НАДЗОРУ

ЛИЦЕНЗИЯ

Регистрационный номер [redacted] от 18 июня 2015 г.

Лицензия выдана Акционерному обществу "Всероссийское производственное объединение "Зарубежатомэнергострой" (АО "ВПО "ЗАЭС")

Местонахождение лицензиата: г. Москва

Основной государственный регистрационный номер юридического лица (ОГРН) [redacted]

Идентификационный номер налогоплательщика [redacted]

Лицензия дает право на на обращение с ядерными материалами

Объект, на котором или в отношении которого осуществляется деятельность сооружения, комплексы, установки с ядерными материалами, предназначенные для производства, переработки, транспортирования ядерного топлива и ядерных материалов

Основание для выдачи лицензии: заявление от 16.01.2015 г. №047/Р.01/128, решение Центрального межрегионального территориального управления по надзору за ядерной и радиационной безопасностью Федеральной службы по экологическому, технологическому и атомному надзору от 18.06.2015 г. № 8787

Срок действия лицензии до 18 июня 2022 г.

Лицензия действует при соблюдении прилагаемых условий действия лицензии, являющихся её неотъемлемой частью

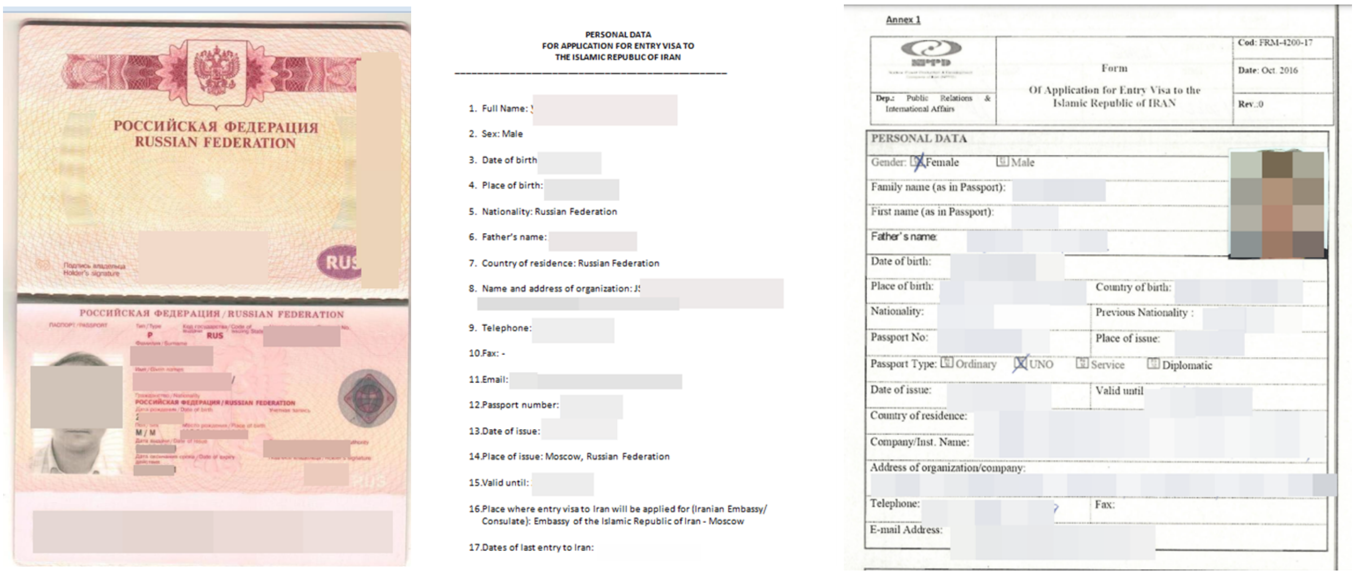
[redacted]

[redacted]

A license gave to the Russian company JSC "All-Russian Production Association "Zarubezhatomenergostroy" sent to the Iranian plant

JSC "All-Russian Production Association "Zarubezhatomenergostroy" performs services in the field of quality assurance of manufacturing and supply of equipment for nuclear facilities in Russia and abroad. JSC "VPO "ZaES" has been carrying out technical acceptance of nuclear fuel, conformity assessment of manufactured equipment, instruments and materials for nuclear power plants, examination of design documentation and quality assurance audits of enterprises since 1973. Geography of the organization - 4 branches, 46 representative offices throughout the Russian Federation.

As stated before, in the leaked files are present a large number of Russian passports, visa requests and other travel document, all linking to a really deep collaboration between Moscow and Teheran.



РОССИЙСКАЯ ФЕДЕРАЦИЯ
RUSSIAN FEDERATION

Подпись владельца
Holder's signature [redacted]

RUS [redacted]

РОССИЙСКАЯ ФЕДЕРАЦИЯ / RUSSIAN FEDERATION

ПАСПОРТ / PASSPORT

Тип / Type: P

Код государства / Code of issuing State: RUS

No. [redacted]

Фамилия / Surname: [redacted]

Имя / Given names: [redacted]

Гражданство / Nationality: РОССИЙСКАЯ ФЕДЕРАЦИЯ / RUSSIAN FEDERATION

Дата рождения / Date of birth: [redacted]

Пол / Sex: M / M

Место рождения / Place of birth: [redacted]

Дата выдачи / Date of issue: [redacted]

Authority: [redacted]

Дата окончания срока действия / Date of expiry: [redacted]

Подпись владельца / Holder's signature: [redacted]

[redacted]

PERSONAL DATA
FOR APPLICATION FOR ENTRY VISA TO
THE ISLAMIC REPUBLIC OF IRAN

1. Full Name: [redacted]
2. Sex: Male
3. Date of birth [redacted]
4. Place of birth: [redacted]
5. Nationality: Russian Federation
6. Father's name: [redacted]
7. Country of residence: Russian Federation
8. Name and address of organization: J[redacted]
9. Telephone: [redacted]
10. Fax: -
11. Email: [redacted]
12. Passport number: [redacted]
13. Date of issue: [redacted]
14. Place of issue: Moscow, Russian Federation
15. Valid until: [redacted]
16. Place where entry visa to Iran will be applied for (Iranian Embassy/ Consulate): Embassy of the Islamic Republic of Iran - Moscow
17. Dates of last entry to Iran:

Annex 1

NPPD Dep.: Public Relations & International Affairs	Form Of Application for Entry Visa to the Islamic Republic of IRAN	Cod: FRM-4200-17 Date: Oct. 2016 Rev.:0

PERSONAL DATA

Gender: ☒ Female ☐ Male

Family name (as in Passport): [redacted]

First name (as in Passport): [redacted]

Father's name: [redacted]

Date of birth: [redacted]

Place of birth: [redacted] Country of birth: [redacted]

Nationality: [redacted] Previous Nationality : [redacted]

Passport No: [redacted] Place of issue: [redacted]

Passport Type: ☐ Ordinary ☒ UNO ☐ Service ☐ Diplomatic

Date of issue: [redacted] Valid until [redacted]

Country of residence: [redacted]

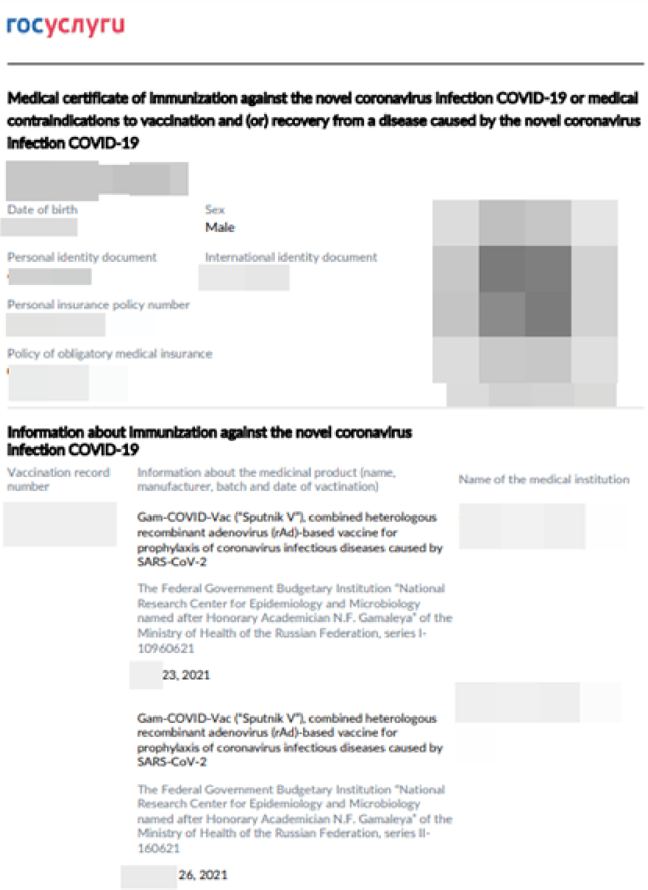
Company/Inst. Name: [redacted]

Address of organization/company: [redacted]

Telephone: [redacted] Fax:

E-mail Address: [redacted]

Russian Passports and visas requests



госуслуги

Medical certificate of immunization against the novel coronavirus infection COVID-19 or medical contraindications to vaccination and (or) recovery from a disease caused by the novel coronavirus infection COVID-19

[redacted]

Date of birth: [redacted]

Sex: Male

Personal identity document: [redacted]

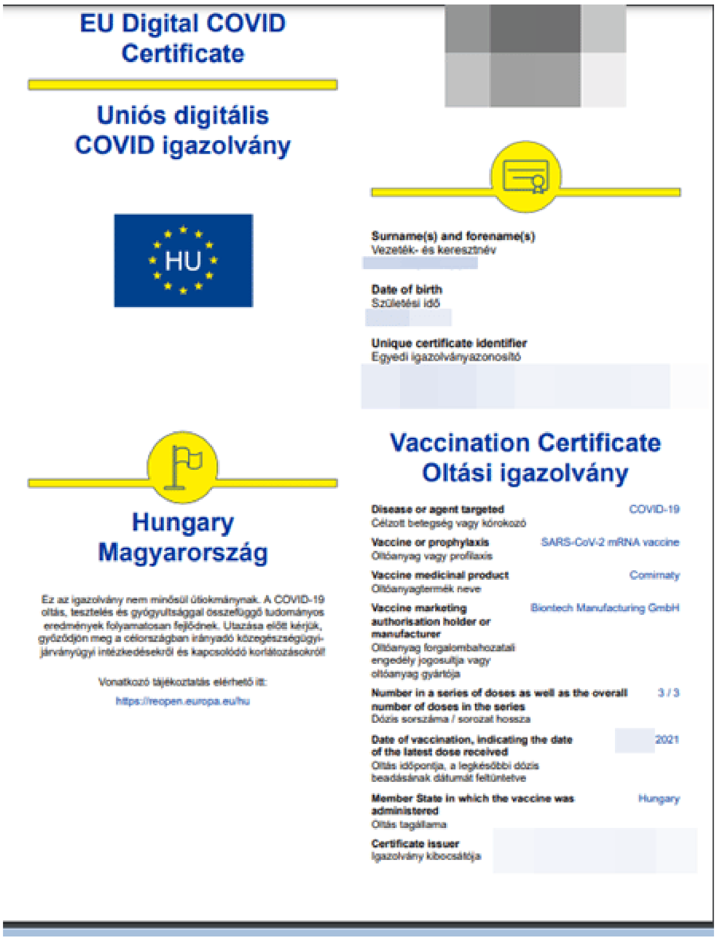
International identity document: [redacted]

Personal insurance policy number: [redacted]

Policy of obligatory medical insurance: [redacted]

Information about immunization against the novel coronavirus infection COVID-19

Vaccination record number	Information about the medicinal product (name, manufacturer, batch and date of vactination)	Name of the medical institution
[redacted]	Gam-COVID-Vac ("Sputnik V"), combined heterologous recombinant adenovirus (rAd)-based vaccine for prophylaxis of coronavirus infectious diseases caused by SARS-CoV-2 The Federal Government Budgetary Institution "National Research Center for Epidemiology and Microbiology named after Honorary Academician N.F. Gamaleya" of the Ministry of Health of the Russian Federation, series I-10960621 [redacted] 23, 2021	[redacted]
	Gam-COVID-Vac ("Sputnik V"), combined heterologous recombinant adenovirus (rAd)-based vaccine for prophylaxis of coronavirus infectious diseases caused by SARS-CoV-2 The Federal Government Budgetary Institution "National Research Center for Epidemiology and Microbiology named after Honorary Academician N.F. Gamaleya" of the Ministry of Health of the Russian Federation, series II-160621 [redacted] 26, 2021	[redacted]



EU Digital COVID Certificate

Uniós digitális COVID igazolvány

HU

Hungary
Magyarország

Ez az igazolvány nem minősül útiokmánynak. A COVID-19 oltás, tesztelés és gyógyultsággal összefüggő tudományos eredmények folyamatosan fejlődnek. Utazása előtt kérjük, győződjön meg a célországban irányadó közegészségügyi-járványügyi intézkedésekről és kapcsolódó korlátozásokról!

Vonatkozó tájékoztatás elérhető itt:
https://reopen.europa.eu/hu

[redacted]

Surname(s) and forename(s)
Vezeték- és keresztnév
[redacted]

Date of birth
Születési idő
[redacted]

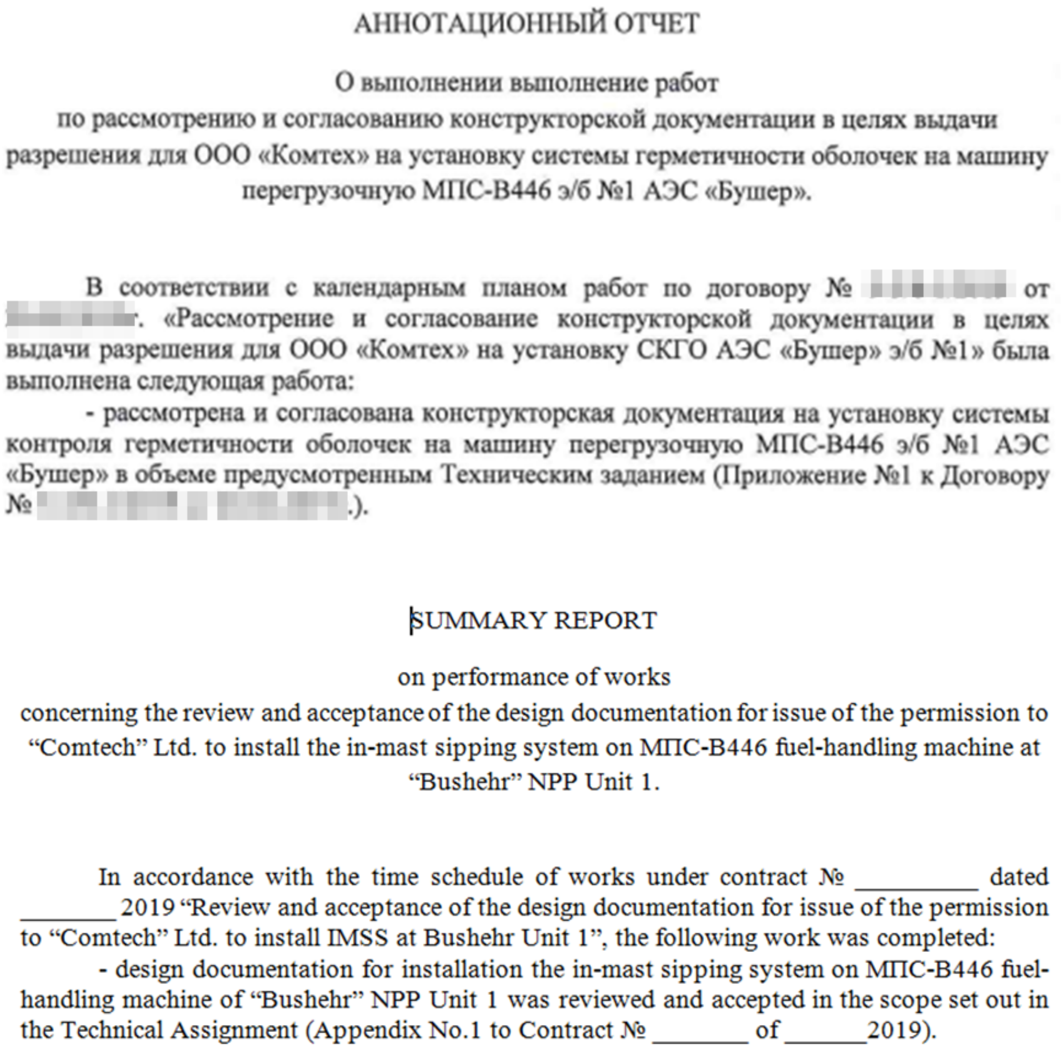
Unique certificate identifier
Egyedi igazolványazonosító
[redacted]

Vaccination Certificate
Oltási igazolvány

Disease or agent targeted Célzott betegség vagy kórokozó	COVID-19
Vaccine or prophylaxis Oltóanyag vagy profilaxis	SARS-CoV-2 mRNA vaccine
Vaccine medicinal product Oltóanyagtermék neve	Comirnaty
Vaccine marketing authorisation holder or manufacturer Oltóanyag forgalombahozatali engedély jogosultja vagy oltóanyag gyártója	Biontech Manufacturing GmbH
Number in a series of doses as well as the overall number of doses in the series Dózis sorszáma / sorozat hossza	3 / 3
Date of vaccination, indicating the date of the latest dose received Oltás időpontja, a legkésőbbi dózis beadásának dátumát feltüntetve	[redacted] 2021
Member State in which the vaccine was administered Oltás tagállama	Hungary
Certificate issuer Igazolvány kibocsátója	[redacted]

Two PCR tests given to Russian citizens, probably asked to the Islamic republic to enter the country during the covid-19 pandemic.

Most of the documents found in the leak are official documents referring to the nuclear sector (see image below) and they are redacted both in Russian and in English, showing a close link between the two countries in this field.



АННОТАЦИОННЫЙ ОТЧЕТ

О выполнении выполнение работ
по рассмотрению и согласованию конструкторской документации в целях выдачи разрешения для ООО «Комтех» на установку системы герметичности оболочек на машину перегрузочную МПС-В446 э/б №1 АЭС «Бушер».

В соответствии с календарным планом работ по договору № [redacted] от [redacted]г. «Рассмотрение и согласование конструкторской документации в целях выдачи разрешения для ООО «Комтех» на установку СКГО АЭС «Бушер» э/б №1» была выполнена следующая работа:

- рассмотрена и согласована конструкторская документация на установку системы контроля герметичности оболочек на машину перегрузочную МПС-В446 э/б №1 АЭС «Бушер» в объеме предусмотренным Техническим заданием (Приложение №1 к Договору № [redacted].).

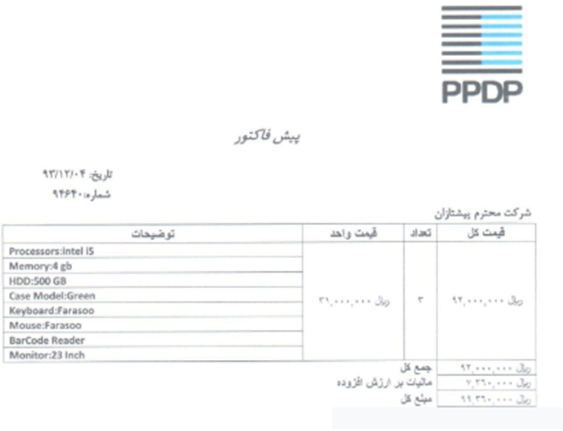
SUMMARY REPORT

on performance of works
concerning the review and acceptance of the design documentation for issue of the permission to "Comtech" Ltd. to install the in-mast sipping system on МПС-B446 fuel-handling machine at "Bushehr" NPP Unit 1.

In accordance with the time schedule of works under contract № _________ dated ________2019 "Review and acceptance of the design documentation for issue of the permission to "Comtech" Ltd. to install IMSS at Bushehr Unit 1", the following work was completed:

- design documentation for installation the in-mast sipping system on МПС-B446 fuel-handling machine of "Bushehr" NPP Unit 1 was reviewed and accepted in the scope set out in the Technical Assignment (Appendix No.1 to Contract № _______ of ______2019).

Another set of files that was found in the leak is material requests, given the fact that Iran is under sanctions, these files could suggest that there are other ways for Teheran to get the equipment needed, especially because most of them are in English.



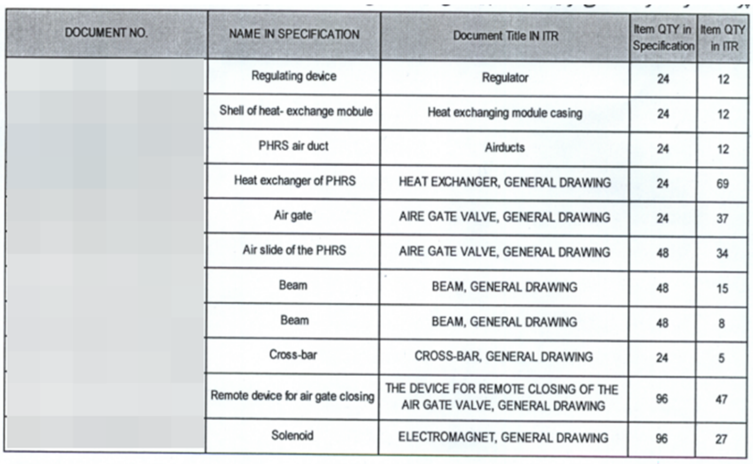
PPDP

پیش فاکتور

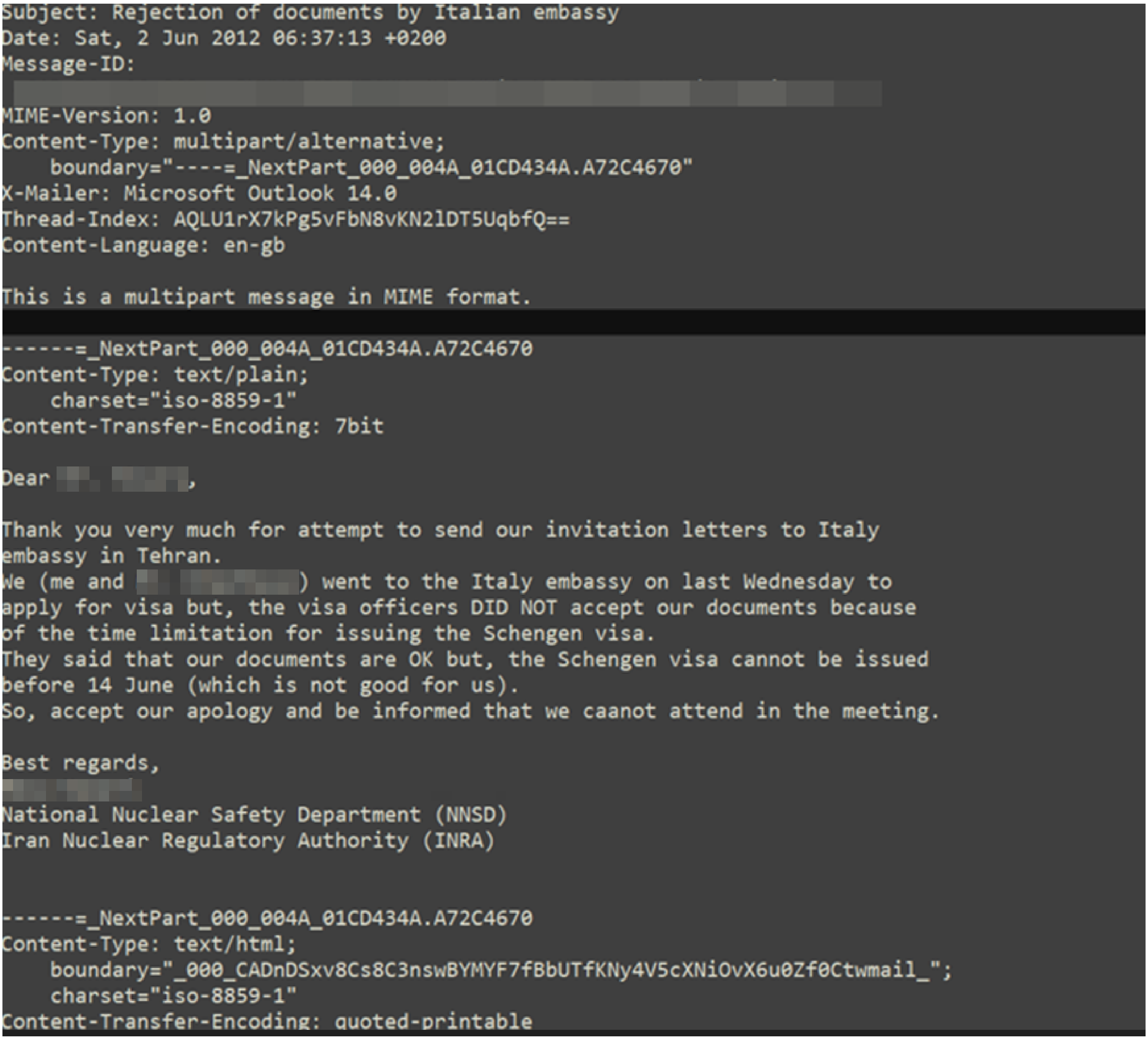
تاریخ: ۹۳/۱۲/۰۴
شماره: ۹۴۶۴۰

شرکت محترم پیشتازان

قیمت کل	تعداد	قیمت واحد	توضیحات
۹۲,۰۰۰,۰۰۰ ریال	۳	۳۱,۰۰۰,۰۰۰ ریال	Processors:Intel I5 Memory:4 gb HDD:500 GB Case Model:Green Keyboard:Farasoo Mouse:Farasoo BarCode Reader Monitor:23 Inch
۹۲,۰۰۰,۰۰۰ ریال	جمع کل		
۷,۳۶۰,۰۰۰ ریال	مالیات بر ارزش افزوده		
۹۹,۳۶۰,۰۰۰ ریال	مبلغ کل		



DOCUMENT NO.	NAME IN SPECIFICATION	Document Title IN ITR	Item QTY in Specification	Item QTY in ITR
[redacted]	Regulating device	Regulator	24	12
[redacted]	Shell of heat- exchange mobule	Heat exchanging module casing	24	12
[redacted]	PHRS air duct	Airducts	24	12
[redacted]	Heat exchanger of PHRS	HEAT EXCHANGER, GENERAL DRAWING	24	69
[redacted]	Air gate	AIRE GATE VALVE, GENERAL DRAWING	24	37
[redacted]	Air slide of the PHRS	AIRE GATE VALVE, GENERAL DRAWING	48	34
[redacted]	Beam	BEAM, GENERAL DRAWING	48	15
[redacted]	Beam	BEAM, GENERAL DRAWING	48	8
[redacted]	Cross-bar	CROSS-BAR, GENERAL DRAWING	24	5
[redacted]	Remote device for air gate closing	THE DEVICE FOR REMOTE CLOSING OF THE AIR GATE VALVE, GENERAL DRAWING	96	47
[redacted]	Solenoid	ELECTROMAGNET, GENERAL DRAWING	96	27



```
Subject: Rejection of documents by Italian embassy
Date: Sat, 2 Jun 2012 06:37:13 +0200
Message-ID:
 [redacted]
MIME-Version: 1.0
Content-Type: multipart/alternative;
	boundary="----=_NextPart_000_004A_01CD434A.A72C4670"
X-Mailer: Microsoft Outlook 14.0
Thread-Index: AQLU1rX7kPg5vFbN8vKN2lDT5UqbfQ==
Content-Language: en-gb

This is a multipart message in MIME format.

------=_NextPart_000_004A_01CD434A.A72C4670
Content-Type: text/plain;
	charset="iso-8859-1"
Content-Transfer-Encoding: 7bit

Dear [redacted],

Thank you very much for attempt to send our invitation letters to Italy
embassy in Tehran.
We (me and [redacted]) went to the Italy embassy on last Wednesday to
apply for visa but, the visa officers DID NOT accept our documents because
of the time limitation for issuing the Schengen visa.
They said that our documents are OK but, the Schengen visa cannot be issued
before 14 June (which is not good for us).
So, accept our apology and be informed that we caanot attend in the meeting.

Best regards,
[redacted]
National Nuclear Safety Department (NNSD)
Iran Nuclear Regulatory Authority (INRA)


------=_NextPart_000_004A_01CD434A.A72C4670
Content-Type: text/html;
	boundary="_000_CADnDSxv8Cs8C3nswBYMYF7fBbUTfKNy4V5cXNiOvX6u0Zf0Ctwmail_";
	charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable
```

An interesting mail found in the leak

MALICIOUS FILES FOUND

An Iranian mailbox in theory, considering the country's past in the field of cyber intrusion and malware infections, needs to be checked very carefully. Indeed, among the leaked files, very interesting files from a cyber point of view were found. Below there is an introduction of the groups behind these files, and in the next paragraph a list of IoCs linked to the found files.

Anunak/Carbanak

Anunak/Carbanak is the main malware of the APT group FIN7. Used along other tools, such as Mimikatz and MBR Eraser, this trojan is used only for targeted attacks on bank and payment systems. Among the primary features there are: keylogging, form-grabbing and functions to interact with the bank system iFOBS.

Phorpiex/Trik

Phorpiex/Trik is a botnet known since 2016 that initially operated using IRC protocol. It has been used to distribute different range of malware, including sextortion campaigns, ransomware and crypto-currency clipping. In 2019, an intelligence company estimated that over 1,000,000 computers were infected and controlled by this botnet.

AutoIT Worm

Malware of this family consists of an AutoIt script that runs various destructive tasks. The malware spreads via network resources or removable media by trying to copy itself to other folders.

AdWind

Backdoor:Java/Adwind is a Java archive that drops a malicious component onto the machines and runs as a backdoor, typically spread as an email attachment. While running as a background service, this backdoor can install other programs, stealing user information and updating its own configuration by communicating with a remote server.

Formbook

Formbook is a family of data-stealing and form-grabbing malware active since 2016. Available as a Malware-as-a-Service, the combination of its low price and advanced modules makes it one the most trending threat nowdays.

Nivdort

Nivdort is a trojan that was distributed in social-themed campaign, like WhatsApp and Facebook. The malicious file is contained within the email attachment and usually disguised within a button to lure the victim. Once executed, Nivdort will automatically replicate itself into C:\ directory and add a Windows Registry entry, while modifying the Windows Hosts file to prevent users from accessing AV websites.

Kuluoz

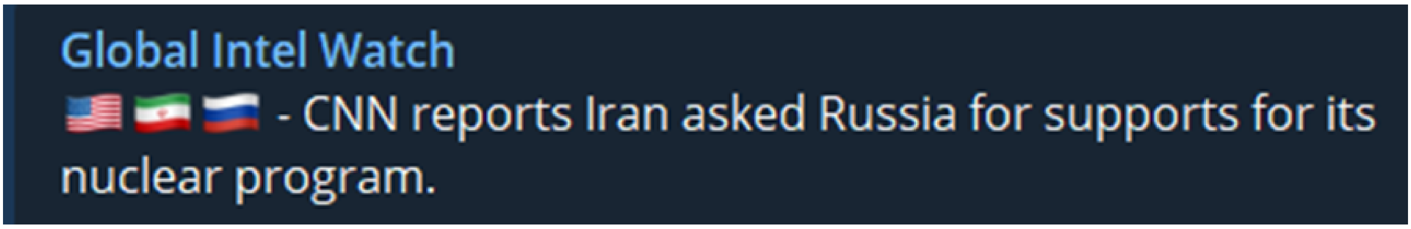
This trojan arrives on a system as a file dropped by other malware or as a file downloaded unknowingly by users when visiting malicious sites. Interestingly, this executable is masqueraded as a Fedex PDF document to lure the victim into opening it.

Narilam

Narilam is the name of the trojan used to target the MS SQL Server DB of three Iranian financial software application by TarrahSystem. Several variants exist, all of them written in Borland C++ (most probably in the late 2009 and beginning of 2010) and appears to be designed mainly to corrupt these databases.

CONCLUSIONS

Cluster25 after having thoroughly analyzed most of the documents, can confirm the fact that ties in the nuclear and atomic fields are strong, intense and frequent between Moscow and Tehran. A long list of experts, Russian citizens, nuclear engineers, frequently go to Iran to advise the Islamic Republic and check on the plants. This is just the confirmation of what is publicly said by the political leaders, thus going to underline the effective help that comes from the Kremlin in the Middle East.



Global Intel Watch

🇺🇸 🇮🇷 🇷🇺 - CNN reports Iran asked Russia for supports for its nuclear program.

News dated 04/11/2022

INDICATORS OF COMPROMISE

MALWARE	TYPE	VALUE
Anunak/ Carbanak	SHA256	0b68025a249bd04720540f688c58ba4bd3f6782de8119524eccfb57fcac36d13
	SHA256	dc2ade64db04b2da7bd825d842025deae7ebb43419a727435962cb093d4299b6
	SHA256	479921ba5eeee4ab662cdcf7f1ba376091f797a80fec4fdf04278288c6f1d0da
	SHA256	581d9b05126624b4522346593af4e48f97e860640c0989fe49357b7a3ed76286
	SHA256	f485a812460b674456ff6392aaf963323998f1d5d8c7e70959b76efb127b7725
	SHA256	603dd2d103cfb7b7e0a61479a0a5c6d33cb819819a80c32bac980b7c82f465e9
	URL	dns22dns22.ru/and/gate.php
	DOMAIN	dnsservicekl2.ru
Phorpiex/Trik	SHA256	0d966c5d04f2569ca957977ad6e9df6e6ab30553b070271be3f4c6b930e73b67

	SHA256	4638b936d235455fb2e79583b206dba30f4f3276e14e11c1fa17c03876bdaab6
	SHA256	a1b54c54cd9b7c321a77727a3367abaf37cbebd476242aa7366d3a1da5ac17c1
	DOMAIN	trkhaus.ru
AutoIT Worm	SHA256	fff661c6cf84d7aa1039287983ed21b91911fbc5887cfa35afc914fcedb9a068
	SHA256	a313235f969b73de1dff3f3e4428ce9c29b278b21d410aa6a51f118c32b743e7
AdWind	SHA256	0b288003b9a2efa470cd72c3a9aa6b2eb4e8cbdc34853a6d73431ae016a67ae3
Formbook	SHA256	fd4c27ac7a6f21ad241388b7bd44e7a287abd2cfa92fe494c27d91b88172eeb4
	SHA256	8ce629f720939b40acc1e571be11a81967e80dd4deb2a2b2a140623d64ea008b
Nivdort	SHA256	5dfca7afcd7ab84a6d98d9d0b64cb4aabf13c8f8b0a85b33848dc7c12b285358
	SHA256	7ffc8690352ed0e9dce46b4a11eb7d1b02ece0b7e1ed910a8912b439cda3b1e1
Kuluoz	SHA256	4f90c2bc0facb2212a70338673870b8f0893f51093216af16ca1f618340821e6
Narilam	SHA256	225d6fa43b4128be67fba2f0a8d1419f72ed9fa3ff92cf98bcceed3448bbef1e
Custom Trojan	SHA256	57fe038248a91847a6e592b68f9e17d190499f97a46eeb80b12e19ff47461386