Iranian Nation-State APT Groups 'Black Box' Leak

Overview and Analysis of Exposed Documents: Targets, Plans, and Attack Vectors

May 2019

Table of Contents

Overview of Targets, Plans, and Attack Vectors 3

Israeli companies mentioned in the documents 3

Outline of the preliminary data gathering operation and attacks on Ethiopian Airlines and Malaysia Airlines 3

A strategic document regarding the creation of Rana 5

Targeted entities 6

Targeted countries 6

Analysis of Targets, Plans, and Attack Vectors 7

Summary of the Event 7

Documents from the Iranian Ministry of Intelligence 8

IRGC Documents 13

Israeli companies mentioned in the documents

- Israir
- Teletus
- Various Israeli hotels
- Most of the Israeli insurance companies

Outline of the preliminary data gathering operation and attacks on Ethiopian Airlines and Malaysia Airlines

1. Preparation sessions – learning about Iranian airlines operating from Iranian airports. This included learning about Operational Technologies (OT) used by the airlines and airports.
2. Identifying the Database (DB) admins for the targeted airlines.
3. Identifying the admins of various systems exposed to the internet.
4. Breaching the targeted airlines network and attempting to compromise additional systems.
5. Once within the network, obtaining admins' passwords.
6. Identifying the DC.
7. Exfiltrating the DC's logs.
8. Exfiltrating the Events Security logs.
9. Identifying various systems' IP addresses.
10. Breaching critical servers via brute force techniques.
11. Assessing if and how it is possible to breach the DB by analyzing the files (note – it is unclear what files the document is referring to).
12. Accessing the DB.

A specific clause to Malaysian Airlines – receiving the dump

13. Exfiltrating the data.
14. Compromising or creating Web servers to receive the data.
15. Collaborating with other teams in order to analyze the data.

Attack on AirAsia

First stage – breaching their network.

1. Obtaining the company's IP addresses.
2. Conducting penetration tests on their network.
3. Gathering a list of the all of the company's website as well as any other website linked to the company, and then conducting on them penetration tests.
4. Breaching any vulnerable asset.

Second stage – obtaining sensitive data.

1. Obtaining usernames and passwords of employees.
2. Levering compromised employee accounts to evaluate the systems admins.

Attack on Philippine Airlines

1. Using a VPN to access the company's internal network.
2. Obtaining usernames and passwords for the company's work stations, servers, and email accounts.
3. Evaluating the system admins and assets to determine whether it is possible and how to execute the attack.
4. Leveraging the compromised data from the breached systems and DBs.

Problems the attackers encountered

1. Robust anti-virus installed on critical systems.
2. Strong firewalls that prevented access to various ports.
3. The use of a local Microsoft Office365 email server. As a result, even after the attackers obtained usernames and passwords they were unable to remotely login to them.
4. Network segmentation – the internal network was not connected to the external network.

Attack on Thai Airways

1. The attackers used a compromised email of a Fly Dubai employee to send phishing emails to other employees. The email contained an attachment of a malicious Excel file with various flight lists.
2. This file was created by penetration team (likely Muddy Water). Out of the 40 recipiences 5 individuals opened the email and infected their computers.
3. After they obtained these employees' usernames and passwords the attackers accessed two databases. The first was an Oracle DB, while the other was an IBM DB2 database.

Attack on the Azerbaijani Department of Health

1. Locating vulnerable websites hosted on the governmental network.
2. Searching on Google for absolute address within the vulnerable websites.
3. Attempting to execute SQL injections on these sites. This appear to have been unsuccessful.
4. Creating shells on the databases.
5. Using a shell to send remote commands to compromised computers. This method was conducted via Desktop Protocol (RDP).

Attack on the website – roshan.af

First stage – attempting to breach the network via a social engineering attack. This attack was unsuccessful as the nobody opened the malicious file. Concurrently, breaching the Linux system used by the website and injecting a shell. Note however that the Linux system had limited capabilities (it is unclear what the attackers meant by this). After considerable efforts the attackers eventually were able to install a hydra system. Afterwards the attackers executed a successful brute force attack on the SMB systems.

The attackers detail the most valuable type of data they were trying to obtain from the DB:

1. Email addresses of directors and other key individuals in the organization.
2. Types and version of the system used by the organization.
3. Network layouts.

4. List of open ports.
5. List of active internal ports used by employees for purchases.
6. List of port used for communication. It is unclear what the attackers mean by this. Possibly ports used by various chat programs.

Attack on Etihad Airways

The attack on the UAE airline was executed via RDP – CITRIX account. Once in the attackers gathered intelligence, notably usernames and passwords.

A strategic document regarding the creation of Rana

First stage – the need for Rana

According to the document the leader of Iran it is vital to develop and expand the country's intelligence gathering and cyber capabilities (developing malware and viruses, various systems, etc.). Accordingly, they created a specialized cyber espionage unite that also had the objective of protected the regime if need be.

Second stage – Rana's objectives

- Propagating the Islamic culture and its ideas.
- Obtaining and providing the leader with strategic intelligence.
- Develop technological knowledge and capabilities.
- Conducting a cyber and intelligence warfare with the rest of the world.
- Utilizing Iranian experts, particularity members of universities in Tehran, as consultants on matters of info-security.
- Using these new skills and capabilities to promote and achieve the government's objective.
- Obtaining intelligence of value to various governmental departments and industrial sectors (note that the Department of Defense oversees the Iranian industrial-defense complex rather than the military).
- These objectives are then followed by more specific goals related to the Iranian population, including expanding the intelligence gathering operation within the country by hacking Iranian universities, mobile companies, airports, etc. (note – it is unclear however the document possibly also refers to Iranian individuals who have contacts to people outside of the country).

Rana sub-group – trojan and malware teams

The objective of this sub-group is hacking, developing malware and attack tools, establishing and maintaining foothold on compromised networks, etc. One other objective is using malwares to identify anyone who poses a threat to the regime such as riot leaders.

The members of the group are experts in IT, encryptions algorithms, firmware, malware and virus development. Further, they are fluent in various foreign languages.

The group can be categorized to several teams:

- Linux.
- Viruses (likely Microsoft based however this is unclear).
- MAC OS.
- Mobile.

- Networks and web development.

From the documents it appears that the Networks and web development are knowledgeable in the following systems and languages:

1. HTML, HTML5, CSS.
2. PHP, Python, SCALA, RUBY AND RAILS, SPT, .NET.
3. Javascript.
4. SQL server, Mysql, Oracle, Nosql.

From the documents it appears that other than IT skills, the mobile team is knowledgeable and has development skills in the following mobile operating systems:

- Android OS.
- IOS.
- Windows Mobile.

Targeted entities

The main targets of the group are

- Governmental departments, agencies and offices.
- Airlines.
- Telecom companies.
- IT companies.

Targeted countries

Asia		Africa	Other
Sri Lanka	Oman	Egypt	Fiji
India	Israel	Morocco	New Zealand
UAE	Turkey	Ethiopia	Australia
Dubai	Iraq	Kenia	Colombia
Thailand	Qatar	South Africa	
Philippines	Lebanon	Mauritius	
Syria	Malaysia		
Azerbaijan	Indonesia		
Afghanistan	Kyrgyzstan		
Pakistan	Kuwait		
Hong Kong	Bahrain		

Iranian Nation-State APT Groups - Confidential Documents Leak
Analysis of Targets, Plans, and Attack Vectors

Summary of the Event

Over the last few weeks, several significant leaks regarding a number of Iranian APTs took place. After analyzing and investigating the documents we conclude that they are authentic. Consequently, this causes considerable harm to the groups and their operation.

The identity of the actor behind the leak is currently unknown, however based on the scope and the quality of the exposed documents and information, it appears that they are professional and highly capable. This leak will likely hamstring the groups' operation in the near future. Accordingly, in our assessment this will minimize the risk of potential attacks in the next few months and possibly even year.

Note - most of the leaks are posted on Telegram channels that were created specifically for this purpose.

Below are the three main Telegram groups on which the leaks were posted:

Lab Dookhtegam pseudonym ("The people whose lips are stitched and sealed" – translation from Persian) – In this channel attack tools attributed to the group 'OilRig' were leaked; including a webshell that was inserted into the Technion, various tools that were used for DNS attacks, and more.

Green Leakers – In this channel attack tools attributed to the group 'MuddyWatter' were leaked. The group's name and its symbol are identified with the "green movement", which led the protests in Iran after the Presidential elections in 2009. These protests were heavily repressed by the revolutionary guards (IRGC)

Black Box – Unlike the previous two channels this has been around for a long time. On Friday May 5th, dozens of confidential documents labeled as "secret" (a high confidentiality level in Iran, one before the highest - top secret) were posted on this channel. The documents were related to Iranian attack groups' activity.

The documents leaked on Friday include:

Documents by the Iranian Ministry of Intelligence (comparable to the FBI and CIA) with information about a group known as "Rana". At this stage, we cannot attribute the group to other known Iranian actors.

The documents shed light on some aspects of the group's activity, notably:

- Tracking Iranians
- Tracking Iranians citizens outside of Iran
- The group's members

These documents contain lists of victims, cyber-attack strategies, alleged areas of access, a list of employees, and screenshots from internal websites relevant to espionage systems.

Further, a one of the document appears to be from the center for IT security incidents Kavesh". Note however that the it was adapted from the original document by the Islamic Revolutionary Guard Corps, and now also contains their symbol. This document was partly leaked and contained details regarding a development program of a malware for attacking SCADA systems (similar Stuxnet).

In this item we review the documents relevant to Israel and to attack capabilities. We translated the documents independently and did not use Google. Note that there are some ambiguous sentences.

Documents from the Iranian Ministry of Intelligence

Rana team

In this leak there are numerous confidential documents with a level of "secret", which detail Rana's goals. They appear to have been written by a hacking and penetration team within the Iranian Ministry of Intelligence's cyber operations department.

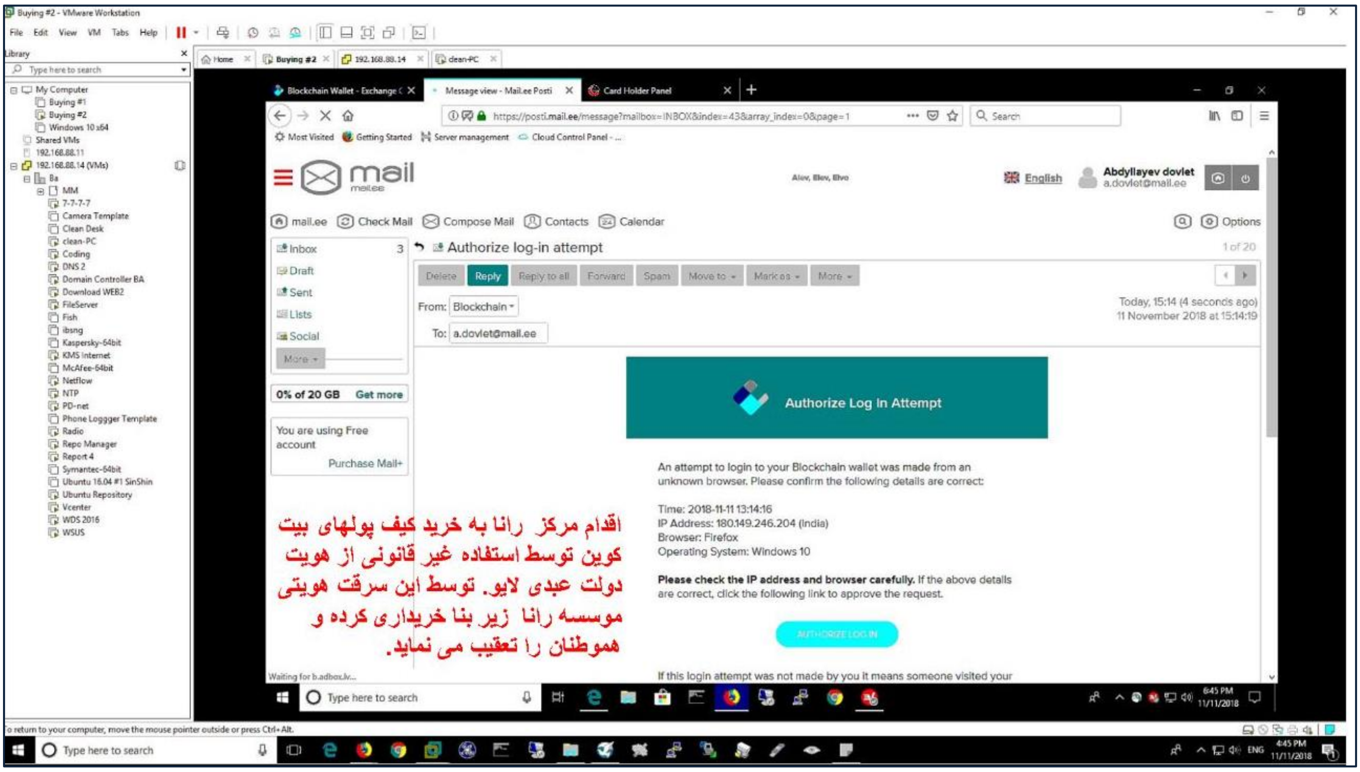
Infrastructure used by the team

Name	IP Address	نام مسئول یا یوزر و پس	Column1	State	Guest OS	Status	Provisioned Space	Used Space	Host	Host CPU	Host Mem	VM Storage Policies Compliance	Managed By	Host Type	Guest Mem - %	Compatibi
Asiacell-ID	192.168.30.17	حسن (پس)		Powered On	Microsoft Windows Server 2012 (64-bit)	Normal	14.67 TB	14.67 TB	192.168.88.95	0	1490	--		ESXi	0	ESXi 6.0 an later (VM version 11
CentOS-Web-4GB		حذف!		Powered Off	CentOS 4/5/6/7 (64-bit)	Normal	64.17 GB	60 GB	host01.mgmt.dc	0	0	--		ESXi	0	ESXi 5.0 an later (VM version 8)
Database Server		حذف!		Powered On	CentOS 4/5/6/7 (64-bit)	Normal	136.17 GB	53.62 GB	192.168.88.95	0	1096	--		ESXi	0	ESXi 5.0 an later (VM version 8)
DomainController	10.10.10.254	حذف!		Powered Off	Microsoft Windows Server 2012 (64-bit)	Normal	156.17 GB	150 GB	host01.mgmt.dc	0	0	--		ESXi	0	ESXi 6.0 an later (VM version 11
Download	192.168.25.26	حسن و سایرین		Powered On	Microsoft Windows Server 2008 R2 (64-bit)	Normal	10.2 TB	6.73 TB	192.168.88.90	25	6221	--		ESXi	0	ESXi 6.0 an later (VM version 11

We are continuing to examine these servers and will update on our findings.

Proof that VMware is used to enter and trade with cryptocurrency wallets

Amongst the documents there was also an image which, according to the leakers, proves an attempt to conceal currency procurement (perhaps due to the sanctions on Iran). This was done using a virtual environment – VMware server.



https://posti.mail.ee/message?mailbox=INBOX&index=43&array_index=0&page=1

Abdyllayev dovlet
a.dovlet@mail.ee

Authorize log-in attempt

From: Blockchain
To: a.dovlet@mail.ee

Today, 15:14 (4 seconds ago)
11 November 2018 at 15:14:19

Authorize Log In Attempt

An attempt to login to your Blockchain wallet was made from an unknown browser. Please confirm the following details are correct:

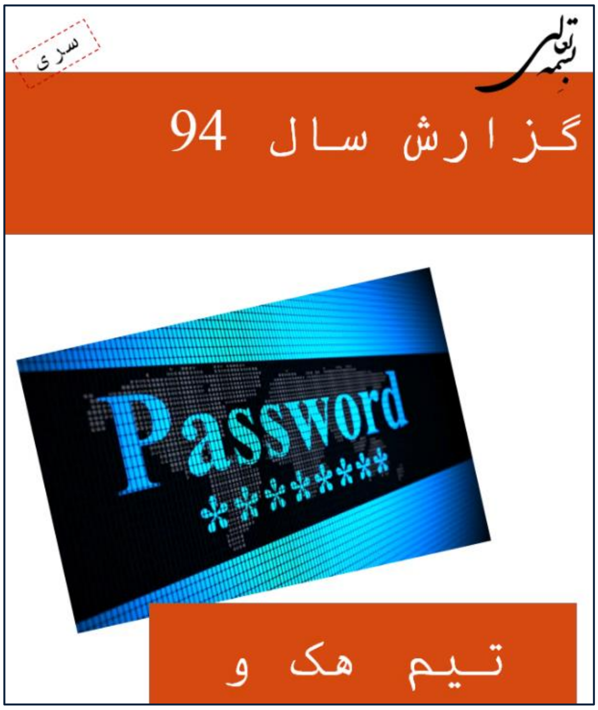
Time: 2018-11-11 13:14:16
IP Address: 180.149.246.204 (India)
Browser: Firefox
Operating System: Windows 10

Please check the IP address and browser carefully. If the above details are correct, click the following link to approve the request.

If this login attempt was not made by you it means someone visited your

اقدام مرکز رانا به خرید کیف پولهای بیت
کوین توسط استفاده غیر قانونی از هویت
دولت عبدی لایو. توسط این سرقت هویتی
موسسه رانا زیر بنا خریداری کرده و
هموطنان را تعقیب می نماید.

End of year Report 2015 (1394 according to Persian calendar).



سری

گزارش سال 94

Password

****

تیم هک و

The first pages from the 1394 end of year report (March 2015 – March 2016) were leaked. They contain a strategic plan to hack airline companies and collect information about them. Based on this report we believe that hacking attempts on airline companies were carried out. The writers of the document stated that some important people in the country use international airlines, and therefore the following information should be gathered:

1. Information about flights.
   a. Flights routes that could be under foreign surveillance.
   b. Comprehensive information on identification scenarios of passengers and identifying important people on the plane.
   c. Certain individuals that could board a flight in disguise (for example, a scenario where with Iranians citizens departs from Iran, and then fly to Israel via another country such as Dubai).
   d. Information on suspicious people that boarded specific flights, for example "the man" who was on the flight from Tehran to Moscow on January 1st, 2014, and flew on April 7th, 2016 from London to Tel Aviv.
2. Information about passengers in specific airlines (the airlines were not mentioned). Specifically - first name, last name, passport number, visa number, ethnicity, communication details, how the tickets were sold and bought.
3. Information about the flight crew. For example, number of pilots on a flight from Dubai to London.
4. Information about airline employees, with an emphasis on executives, managers, network admins, airport managers, and booking operators.
5. Information about the airlines' finacial status.
6. Information on equipment used by the company. This includes planes (e.g. number and type of planes, their condition, when they were used last, etc.) as well as computer equipment (number and type of servers and computers, etc.)

   Note - at the end of the page it is stated that in the next pages there will be a specific list of targets, but this page is missing from this leak.

Report on the first half of 1395

In another report on regarding 1395 (specifically March 2016 – August 2016), several tracking projects are detailed. A documentation regarding attacks that were carried out on airlines' databases, including the Israeli airline 'Israir'. Below is a full translation of relevant parts of the document:

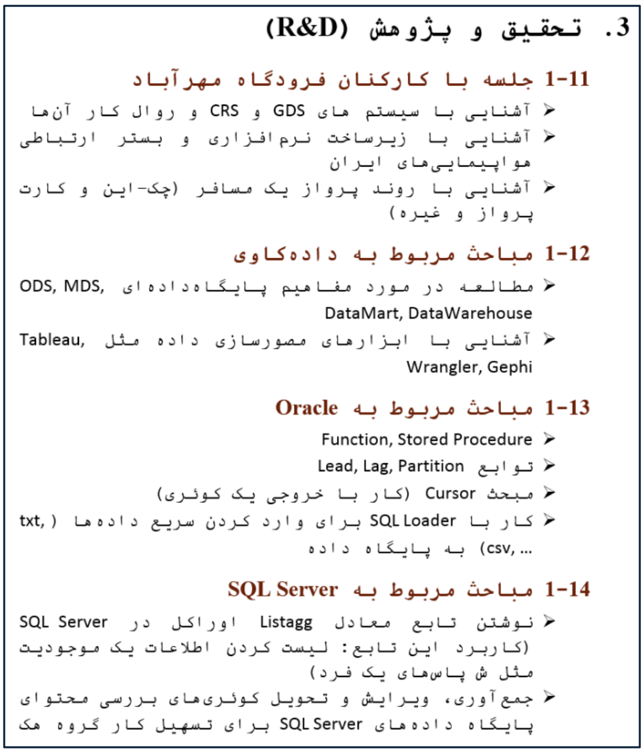
- The airline's database
  - Entering Qatar's database, and queries on flights.
  - Entering Israir's database.
  - Query on Dubai activity.
  - Query on Skyward's activity
- The Turkish police database
- Cooperation with these targets' attack groups.

- Examine Israir's databases.
- Examining an insurance company's databases in Saudi Arabia
- Examining RTA's databases from the UAE

The next page contains an R&D clause, with details on measures taken before attacks, preliminary research, and possible attack vectors. Some of the measures include:

- A meeting with employees from the international airport in Tehran to learn about the airport's systems.
- Research on various databases.
- Research on using ORACLE and SQL server. In this regard, the attackers worked with SQL Loader and Bulk insert in order to quickly enter databases, and with BCP utility to copy the information from the servers.

Moreover, the document also mentions gathering information on flights – mapping of assets that can be used to check-in, security procedures on the plane, and data collection via the real-time flight tracking website FlightRadar24.



.3 تحقیق و پژوهش (R&D)

1-11 جلسه با کارکنان فرودگاه مهرآباد

- آشنایی با سیستم های GDS و CRS و روال کار آن‌ها
- آشنایی با زیرساخت نرم‌افزاری و بستر ارتباطی هواپیمایی‌های ایران
- آشنایی با روند پرواز یک مسافر (چک-این و کارت پرواز و غیره)

1-12 مباحث مربوط به داده‌کاوی

- مطالعه در مورد مفاهیم پایگاه‌داده‌ای ODS, MDS, DataMart, DataWarehouse
- آشنایی با ابزارهای مصورسازی داده مثل Tableau, Wrangler, Gephi

1-13 مباحث مربوط به Oracle

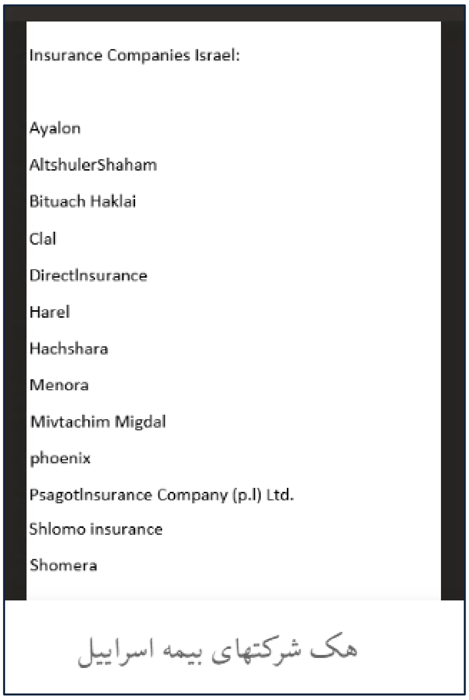
- Function, Stored Procedure
- توابع Lead, Lag, Partition
- مبحث Cursor (کار با خروجی یک کوئری)
- کار با SQL Loader برای وارد کردن سریع داده‌ها (txt, csv, ...) به پایگاه داده

1-14 مباحث مربوط به SQL Server

- نوشتن تابع معادل Listagg اوراکل در SQL Server (کاربرد این تابع: لیست کردن اطلاعات یک موجودیت مثل ش پاس‌های یک فرد)
- جمع‌آوری، ویرایش و تحویل کوئری‌های بررسی محتوای پایگاه داده‌های SQL Server برای تسهیل کار گروه هک

Attacks on Israel

Attacks on insurance companies – A document with the title "Hacking Israel's insurance companies". It contains a list of Israeli insurance companies (see image below). Note that the title in Persian does not enable us to discern if it is an attack that already took place, or a list of future targets.



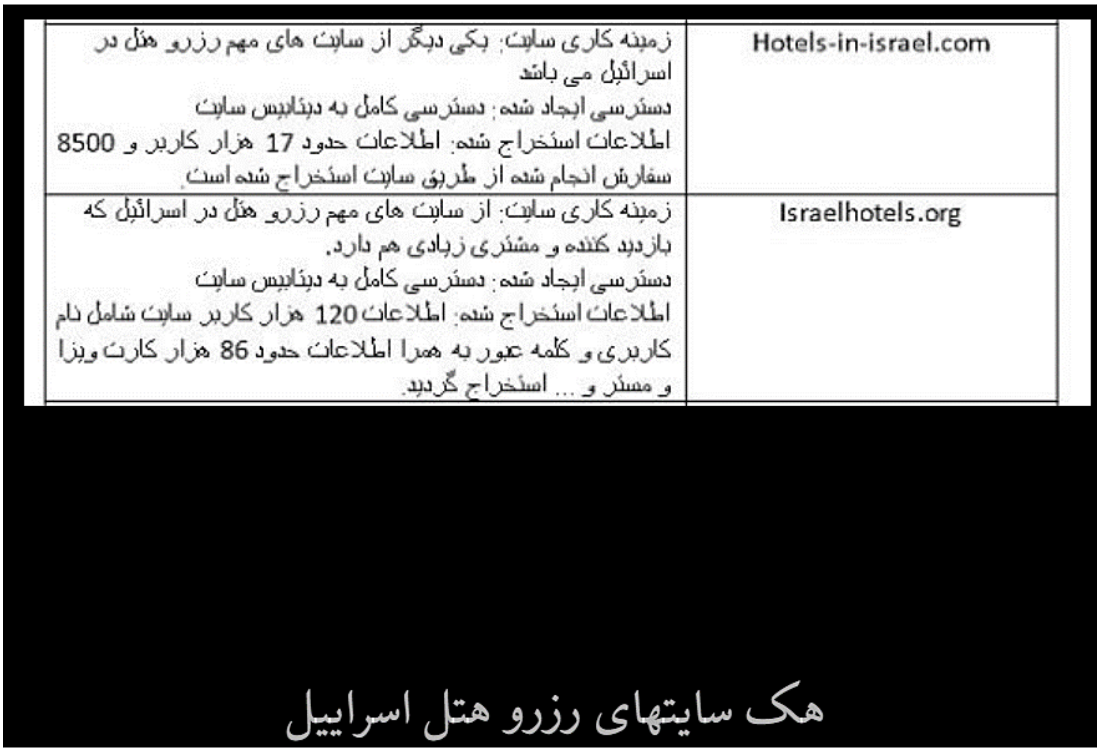
Insurance Companies Israel:

Ayalon
AltshulerShaham
Bituach Haklai
Clal
DirectInsurance
Harel
Hachshara
Menora
Mivtachim Migdal
phoenix
PsagotInsurance Company (p.l) Ltd.
Shlomo insurance
Shomera

هک شرکتهای بیمه اسراییل

Attacks on hotel booking websites in Israel – Below is a screenshot from a document with information about two hotel booking websites. It lays out the website's main activity, the access obtained, and the intelligence gathered.

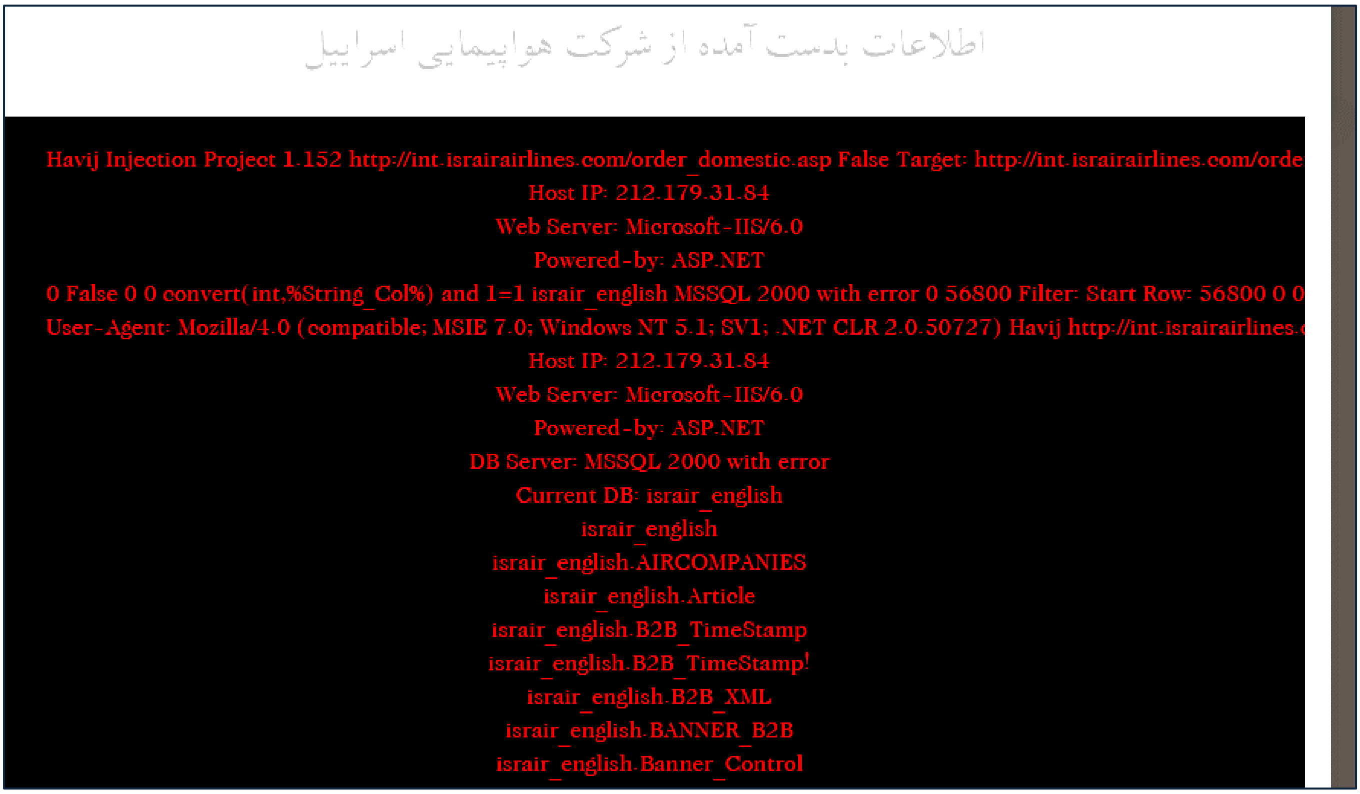
According to the document, Israelhotels.org is one of the most important hotel booking websites. Further, it alleges that they gained full access to the website's database. The documents contain information on 120 thousand of the website's users, including name, password, and around 86 thousand credit cards.



Hotels-in-israel.com	زمینه کاری سایت: یکی دیگر از سایت های مهم رزرو هتل در اسرائیل می باشد دسترسی ایجاد شده: دسترسی کامل به دیتابیس سایت اطلاعات استخراج شده: اطلاعات حدود 17 هزار کاربر و 8500 سفارش انجام شده از طریق سایت استخراج شده است.
Israelhotels.org	زمینه کاری سایت: از سایت های مهم رزرو هتل در اسرائیل که بازدید کننده و مشتری زیادی هم دارد. دسترسی ایجاد شده: دسترسی کامل به دیتابیس سایت اطلاعات استخراج شده: اطلاعات 120 هزار کاربر سایت شامل نام کاربری و کلمه عبور به همرا اطلاعات حدود 86 هزار کارت ویزا و مستر و ... استخراج گردید.

هک سایتهای رزرو هتل اسراییل

Israeli airlines' databases – Like the strategic documents, this document also mentions an attack against Israir. The attack includes attempts to gather information from Israir's booking system's database, which mainly include information about bookings and credit cards. Due to the many error messages in the document, we cannot determine whether this attack succeeded or failed.



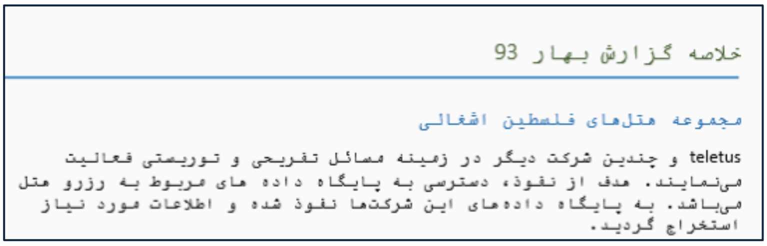
اطلاعات بدست آمده از شرکت هواپیمایی اسراییل

```
Havij Injection Project 1.152 http://int.israirairlines.com/order_domestic.asp False Target: http://int.israirairlines.com/orde
Host IP: 212.179.31.84
Web Server: Microsoft-IIS/6.0
Powered-by: ASP.NET
0 False 0 0 convert(int,%String_Col%) and 1=1 israir_english MSSQL 2000 with error 0 56800 Filter: Start Row: 56800 0 0
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727) Havij http://int.israirairlines.c
Host IP: 212.179.31.84
Web Server: Microsoft-IIS/6.0
Powered-by: ASP.NET
DB Server: MSSQL 2000 with error
Current DB: israir_english
israir_english
israir_english.AIRCOMPANIES
israir_english.Article
israir_english.B2B_TimeStamp
israir_english.B2B_TimeStamp!
israir_english.B2B_XML
israir_english.BANNER_B2B
israir_english.Banner_Control
```

The attack was carried out on MSSQL 2000 servers that the company uses, and with the following user agent:

User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727) Havij

Attack on Teletus website and other hotel booking companies – a strategic report on an attack against the Israeli firm Teletus. Its goal was to obtain access to websites connected to hotel bookings in Israel. According to the report, the breach was successful. The information was presented in a strategic report from Spring 1393 (April –May 2014), but the nature of the report is unknown.

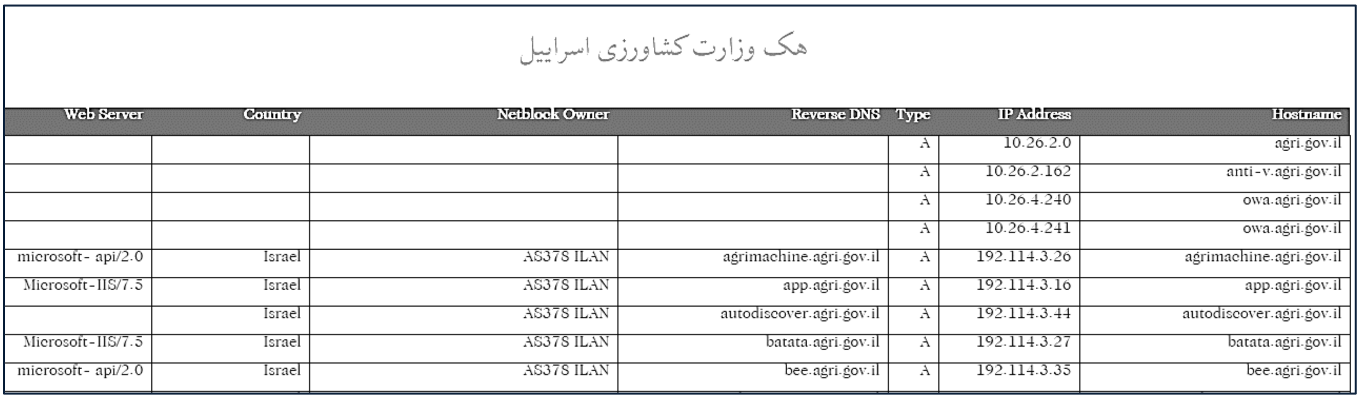


خلاصه گزارش بهار 93

مجموعه هتل‌های فلسطین اشغالی

teletus و چندین شرکت دیگر در زمینه مسائل تفریحی و توریستی فعالیت
می‌نمایند. هدف از نفوذ، دسترسی به پایگاه داده های مربوط به رزرو هتل
می‌باشد. به پایگاه داده‌های این شرکت‌ها نفوذ شده و اطلاعات مورد نیاز
استخراج گردید.

An attack on the Israeli Ministry of Agriculture – a table from a document with ambiguous content.



هک وزارت کشاورزی اسراییل

Web Server	Country	Netblock Owner	Reverse DNS	Type	IP Address	Hostname
				A	10.26.2.0	agri.gov.il
				A	10.26.2.162	anti-v.agri.gov.il
				A	10.26.4.240	owa.agri.gov.il
				A	10.26.4.241	owa.agri.gov.il
microsoft- api/2.0	Israel	AS378 ILAN	agrimachine.agri.gov.il	A	192.114.3.26	agrimachine.agri.gov.il
Microsoft-IIS/7.5	Israel	AS378 ILAN	app.agri.gov.il	A	192.114.3.16	app.agri.gov.il
	Israel	AS378 ILAN	autodiscover.agri.gov.il	A	192.114.3.44	autodiscover.agri.gov.il
Microsoft-IIS/7.5	Israel	AS378 ILAN	batata.agri.gov.il	A	192.114.3.27	batata.agri.gov.il
microsoft- api/2.0	Israel	AS378 ILAN	bee.agri.gov.il	A	192.114.3.35	bee.agri.gov.il

Attacks on non-Israeli targets

In addition to the above documents, there are also dozens of other documents relevant to other countries. For example, several documents contain information on attacks against government ministries in Kuwait. The goal of the attack was to obtain access to a Kuwaiti email service, and gather information on the Ministry of Foreign Affairs through it.

A strategic report from the first half of 1396 (March – August 2017) describes activity carried out against Kuwait. According to this document, two teams worked on the attack: the hacking team, and the social engineering team. The document was written in first person plural, and was most likely written by the attack team.

Below is an outline of the hacking team's operation

At first, the team carried out various tests, including penetration tests on systems of the Foreign Ministry. Then they mapped all the IP addresses, the domains, the websites, and the apps used by the ministry. The team carried out more tests to see what is open and accessible in the network. They found out that they could obtain the highest level of control of the targeted servers.

After a full examination, they transferred their conclusions to the social engineering team. The hacking team also obtained access to the ministry's employee database, and sent spam messages to everyone within the ministry in order to validate the emails using mail tracker.

Below is an outline of the social engineering team

Phishing – Phishing attacks on numerous firms, for example "Atam Alanya" hospital and the **Qatari oil company.**

Spear-phising– The team communicated directly with people related to the Foreign Ministry.

Concurrently, they worked on R&D: setting up a server and website, preparing the malware written in Python, and planning the activity together with the technical teams.

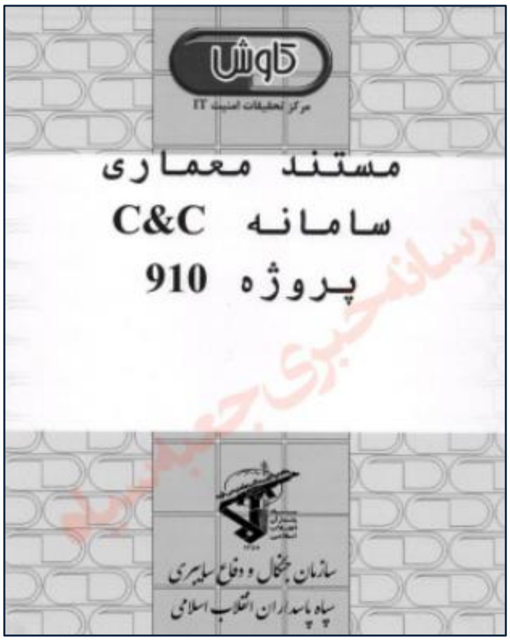
Based on another document that details an attack on the Foreign Ministry, it appears that the attack was successful.

IRGC Documents

Another document with the IRGC symbol contains a plan named **project 910**. It outlines development of a malware and a C2 (command and control) server.

According to the report, the project intended to damage SCADA systems. It is a botnet, but in fact behaves like an spy-malware with identification, espionage and remote connection abilities. As of 09/12/1394 (February 28th, 2016- the date the document was written), the project was unsuccessful and did not achieve its goals despite a large budget.

Additionally, we detected another document that extensively details the attack vector, but lacks the part about the bot in the leaked document. Further, the document does not have the IRGC symbol.



کاوش

مرکز تحقیقات امنیت IT

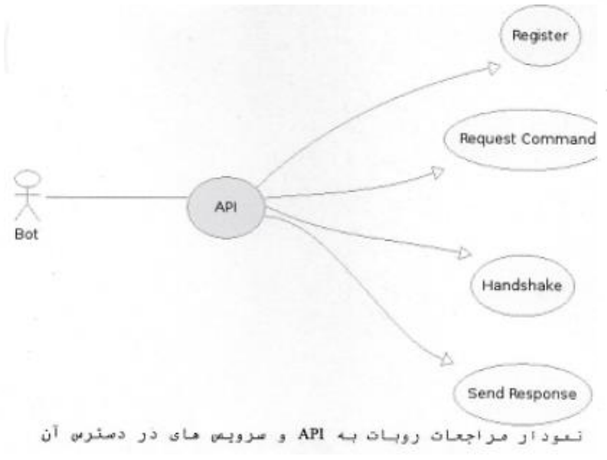
مستند معماری
سامانه C&C
پروژه 910

سازمان جنگال و دفاع سایبری
سپاه پاسداران انقلاب اسلامی

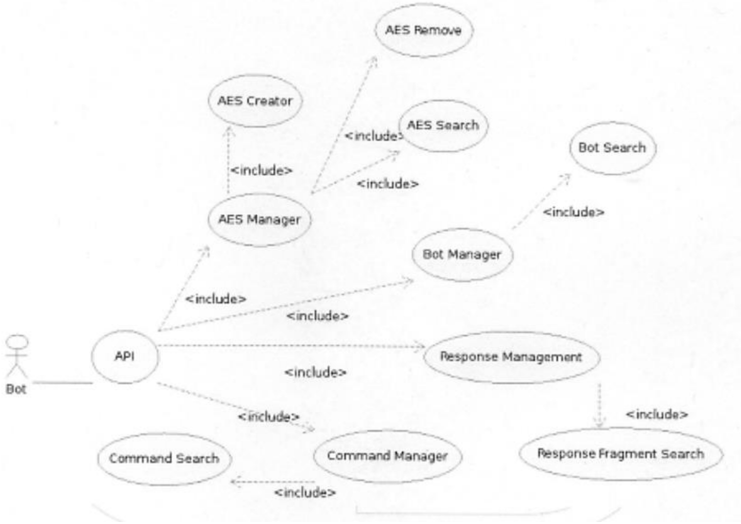
In this item we review only the document leaked, based on the assumption that the malware was modified for project 910.

Attack vector as presented in the document:

The documents in our possession are incomplete. Accordingly, we are unable to provide a full and accurate assessment of the attack vector. Below are screen captures from the documents showing flow charts of the attack vector.



Attack vector – flow chart 1



Attack vector – flow chart 2

Clearsky Cyber Security Report

Overview and Analysis of Exposed Documents

Targets, Plans, and Attack Vectors

Email: info@clearskysec.com
Website: clearskysec.com

CLEARSKY
Cyber Security

Ahead of the Threat Curve