MANDIANT
YOUR CYBERSECURITY ADVANTAGE

Iranian Threat Landscape – September-October 2022

TLP: Amber

Summary

1. **APT42 (IRGC-IO[1])** was graduated from UNC788. Mandiant observed multiple new domains masquerading as US, IL and Middle East news outlets. Past TTPs suggest the infrastructure may be used to send malicious emails masquerading as journalists. This type of activity **may be leveraged for information operations or hack-and-leak operations**, which may be concerning in light of the upcoming US midterm elections and Israeli election, both will be held on November 2022.

2. **UNC3890 (IRGC)** continues to target various Israeli sectors, likely including healthcare, shipping and technology. Mandiant observed changes to the infrastructure published in a blog last August. **Intelligence related to the shipping sector**, especially concerning the tracking of cargos, **may be leveraged by the IRGC for kinetic operations**, in light of the ongoing naval conflict with Iran.

3. **UNC2448 (suspected as IRGC-IO)** was publicly mentioned in an alert released by CISA, attributing it to IRGC and exposing its infrastructure. Since the alert Mandiant observed a **decrease in activity** related to the exposed infrastructure, with most activity orginating from previously known infections in the Middle East and Africa.

4. **TEMP.Zagros[2] (MOIS[3])** targeted Jordanian government organizations and critical infrastructures, as well as a Saudi insurance company. Successful compromise of the suspected targets may have provided the Iranian MOIS with **intelligence regarding nuclear energy, as well as PII of citizens/travelers** in Saudi and Jordan which may have been **an enabler in tracking high-profile individuals abroad**.

[1] Isalmic Revolutionary Guard Corps Intelligence Organization
[2] A.K.A. MuddyWater
[3] Ministry of Intelligence and Security

Analysis & Indicators of Compromise

1. **APT42 (IRGC-IO)** – Mandiant observed multiple domains masquerading as Middle East and US news outlets. Registration patterns suggest the infrastructure is affiliated with APT42 or IRGC-affiliated clusters of activity. So far, the following infrastructure was identified (arranged by registration/update date in a descending order):

Malicious Domain	Masquerading as	Legitimate Entity	Geography	Registration/Update Date
maariv[.]net	maariv[.]co[.]il	Maariv	Israel	09/07/22
themedealine[.]org	themedialine[.]org	The Media Line	US	09/07/22
foreiqnaffairs[.]com	foreignaffairs[.]com	Foreign Affairs Magazine	US	04/20/22
washinqtonpost[.]press	washingtonpost[.]com	Washington Post	US	04/19/22
ynetnews[.]press	ynetnews[.]com	Ynet	Azerbaijan	04/16/22
azadlliq[.]info	azadliq[.]info	Azadliq	Azerbaijan	03/09/22
jpostpress[.]com	jpost[.]com	Jerusalem Post	Israel	01/08/22
accounts-drive[.]com[4]	OneDrive/Google Drive	Microsoft/Google	Global	12/22/21
jpost[.]press	jpost[.]com	Jerusalem Post	Israel	12/11/21
khaleejtimes[.]org	khaleejtimes[.]com	Khaleej Times	UAE	11/28/21

Mandiant identified Twitter discourse related to this cluster of activity as early as December 2021:

2. **UNC3890 (IRGC)** – Mandaint observed several changes in the cluster's infrastructure over the last month, summarized in the table below:

Type	Value	Comment
Domain	office365update[.]live	
Domain	pfizerpoll[.]office365update[.]live	Masquerades as Pfizer; Similar to the domain pfizerpoll[.]com exposed in the August blog
Domain	upmeload[.]com	
Domain	designsewup[.]live (suspect)	
IP	185.170.215.170	Hosts office365update[.]live
IP	159.223.195.247	Hosted upmload[.]com
URL	Hxxp[:]//185[.]170[.]215[.]170/HtmlSmuggling	
URL	Hxxp[:]//185[.]170[.]215[.]170/evilpdf	
URL	hxxp[:]//office365update[.]live/365-Stealer	
MD5	8aa95d3265b08090e9cfe72b264c096f	outMalware.pdf; Downloaded from 185.170.215.170
MD5	8971805628c1844a5a6066d8d04e171b	hi.exe; Downloaded from 185.170.215.170

[4] Publicly identified as a Charming Kitten domain in Certfac's publication in January 2020: "Fake Interview: The New Activity of Charming Kitten".

The files and directories hosted on the server 185.170.215.170 suggest UNC3890 have been experimenting with HTML Smuggling – a method for hiding malicious files in HTML files, and EvilPDF – a tool for embedding Executable files in PDF.

3. **TEMP.Zagros (MOIS)** continues using ScreenConnect, likely delivered via phishing emails, in order to gain initial access to its victims. During August-September 2022 Mandiant observed the following ScreenConnect instances submitted to a public scanning service, suspected to be used by TEMP.Zagros:

MD5	File/Archive Name	Masquerades As	Suspected Target[5]	Submission Date
dca5d5e4386fef023fdb3577ebb69837	Ertiqa.msi / Performance.msi / 123.msi / 2.msi	Ertiqa – Saudi non-profit organization	JAEC – Jordanian Atomic Energy Commission	09/05/22
83fc15519ff8e8f5258fec4baa25b96c	dpa[.]gov[.]jo.seminar.zip	DPA –Department of Palestinian Affairs (Jordan)	Polaris Technology – Jordan-based IT company	09/01/22
5ed41d6e208592512f57134c94660b42	cspd[.]gov[.]jo.program.msi	CSPD – Civil Status and Passports Department (Jordan)	gov[.]jo – Jordanian Government	08/29/22
3751a3abbfbdd1ee1a0adbdb93d2d51f	Cvdb.msi / smart employee.msi	CVDB – Cities and Villages Development Bank (Jordan)	"mojjoo" – Possibly the Jordanian Ministry of Justice	08/22/22
1a4c877b27f08bced944b73658c67589	Ertiqa.msi / promotion.msi	Ertiqa	SNIC – Saudi National Insurance Company	08/15/22

[5] Based on the ScreenConnect's embedded configuration.