Dark Web Profile: APT42 - Iranian Cyber Espionage Group - SOCRadar® Cyber Intelligence Inc.

Published: 2022-12-12 · Archived: 2026-04-02 10:44:19 UTC

1. Home
2. Blog
3. Threat Actor Profiles
4. Dark Web Profile: APT42 – Iranian Cyber Espionage Group

By SOCRadar Research

After the Stuxnet occurred in 2010 on Iran's nuclear program, Iran started to invest in and improve its **cyberwarfare** capabilities. From that turning point, Iranian hacker groups rose and became more dangerous for the cyber world. Their danger is not just from destructive attacks; the Iranian cybercriminal groups use cyber espionage campaigns as much as cyberattacks. Major cyber espionage activities of Iran approximately started with Madi, -a spyware operated in 2012, targeting business executives working on critical infrastructure and Middle Eastern government officials-. Following that, Iranian threat actors, specifically the groups counted as Advanced Persistent Threats (APT) such as **APT35** and **APT39** (Remix Kitten), became known in the world for their cyber espionage attacks. These attacks are meaningful to Iran because their primary goal is believed to improve Iran's industrial and military capabilities.

Operation categories of APT42

Recently, in July 2022, the Iranian threat actor APT42 conducted a cyber-attack against the Albanian government. In September 2022, Mandiant released a report detailing the APT42 with at least 30 confirmed cyber espionage operations dating back to 2015. APT42 -also known as **Crooked Charms and TA453**– is a cyber espionage group linked to Iran. The group is allegedly affiliated with the Islamic Revolutionary Guard Corps (IRGC) Intelligence Organization (IRGC-IO) and operates behalf of them. The group seems mainly focused on **spearphishing attacks**, which is a type of phishing attack targeting individuals or organizations known as high-profile or in a specific role—using impersonation to look like a trusted person during its attacks separates the group from other Iranian APT groups.

Targets of APT42

APT42 follows other Iranian state-sponsored cybercriminal groups' targeting patterns. The group focuses on the **Middle East** region. They mainly target individuals and organizations particularly interested in the Iranian government or who have **opposing ideas** from Iran's regime.

Also, the group is targeting a few specific sectors, as follows:

- Civil society and non-profit organizations,
- Education,
- Healthcare,
- Pharmaceuticals,
- Manufacturing,
- Media

From 2015 until the present, APT42's attacks have been observed in more than 15 countries, including the **United States**, Australia, **Germany**, the **United Kingdom**, and so on.

Countries affected by APT42 (Source: SOCRadar)

The group operates in three main categories:

1. Credential Harvesting

The group uses spearphishing campaigns to steal Multi-Factor Authentication codes to bypass authentication and gain access to the networks, devices, and accounts of their victim's colleagues. One example of this attack was observed by Mandiant in February 2021, when APT42 targeted the email credentials of a senior Israeli government official by mimicking the Gmail login page.

2. Surveillance Operations

Group has been observed using **Android malware** designed to gather information -such as locations, communications, etc.- from Iranian dissidents and individuals interested in the Iranian government. In 2022, from June to August, Mandiant observed that APT42 used **PINEFLOWER** malware to exfiltrate recorded calls, audio recordings, images, and SMS inboxes from Iran-based people linked to universities, reformist political groups, and human rights activists.

PINEFLOWER's MD5 Hash search output on SOCRadar's Threat Hunting page

3. Malware Deployment

Although APT42's main objective is credential harvesting, the group also uses lightweight tools and custom **backdoors** when its objective becomes wide-ranging. Mandiant observed in March 2022 that the APT42 had used **POWERPOST**, a custom reconnaissance tool built to collect data such as system information and local account names on a local host.

APT42's Connection with APT35

Some sources consider APT42 as one of the names of another Iran state-sponsored cyber espionage group APT35. Still, many resources show they are separate groups and correlate with each other.

Mandiant considers both **APT35** and **APT42** to be IRGC-affiliated. The two groups differ regarding missions, contracts, or contractors due to significant differences in their respective targeting patterns, tactics, techniques, and procedures. In addition, their targeting separates into specific points. APT35 targets the **U.S., Western Europe, and Middle Eastern** military, diplomatic and government personnel and organizations, defense industry, and telecommunications sectors. On the other hand, APT42 focuses on organizations and individuals interested in the Iranian government and opponents of Iran.

APT42's Connection with Nemesis Kitten

Nemesis Kitten -UNC2448 or DEV-0270- is an Iranian threat actor believed to belong to Phosphorus, same as APT42. The group is known for its ransomware campaigns and network operations on behalf of the government of Iran.

Diagram of Phosphorus and Charming Kitten (Source: Mandiant)

Nemesis Kitten is different from APT42 in its attacking style. During the initial access phase, Nemesis Kitten -or DEV-0270- typically exploits known **Exchange and Fortinet vulnerabilities** -e.g., CVE-2018-13379-. While Nemesis Kitten uses exploits to access, APT42 -as observed- uses spearphishing attacks during its initial access phase.

According to Mandiant, the APT42 and Nemesis Kitten have no relation technically, but allegedly, both may have ties with IRGC-IO.

APT42's Connection with TAG-56

TAG-56 group, which is included in the report published by Recorded Future on November 29, 2022, has common points with the APT42 group:

- From the observed cases, the TAG-56 threat actor has been seen using **fake registration pages**, such as a fake Microsoft login page, to lure its victims. There are similar observations in some of the APT42's attacks.

- Some of the domains used by the group (**mailer-daemon[.]org, net, me, and live**) stand out because **mailerdaemon[.]me** and **mailer-daemon-message[.]co** domains were observed in use before by the Phosphorus group -in which APT42 believed to belong to the group-.
- TAG-56 spreads malicious links to its victims using spearphishing or directly sending via encrypted chat platforms -such as WhatsApp or Telegram– by manipulating its victims using social engineering techniques as other Iran-nexus threat actors as APT42 do.

In light of these common points, TAG-56 and the APT42 strongly overlap.

Notable Operations of APT42

Multi-Persona Impersonation (MPI)emails -> The group uses a new phishing technique to dupe their victims. They use multiple impersonated journalists' profiles and create a realistic-looking fake mail thread. Then they add the victim journalist or researcher to the thread and continue communicating about the topic.

Example of MPI mail thread (Source: Proofpoint)

After a while, one of the fake personas sends a file link that directs a forged **Google Drive** or **OneDrive** website to steal credentials or deliver a malicious file.

Another Example of APT42 delivering a malicious document via phishing mail (Source: Proofpoint)

Mimicking login pages -> APT42 has been observed many times mimicking **Google, Yahoo!, and OneDrive's login page** for harvesting credentials. In this way, the group can steal the MFA codes of their victims to access the account.

Fake Yahoo! Login page designed by APT42 (Source: Mandiant)

List of the Malware Used by APT42

BROKEYOLK	GHAMBAR	POWERPOST
CHAIRSMACK	MAGICDROP	SILENTUPLOADER
DOSTEALER	PINEFLOWER	TABBYCAT
VINETHORN	VBREVSHELL	TAMECAT

Attack Cycle of APT42

As mentioned, the group uses spearphishing, credential harvesting, and malware deployment for its operations' first phase. Besides these methods, APT42 has also been observed using MFA bypassing techniques for initial access.

Once successfully accessed, the group registers its Authenticator to eliminate the MFA. Also, the group uses various malware -such as **GHAMBAR, BROKEYOLK, PINEFLOWER**, and so on- to establish its foothold.

- **GHAMBAR:** GHAMBAR is a **remote administration tool (RAT)** written in C#. It takes commands from the C2 (Command and Control) server using **SOAP (Simple Object Access Protocol)** API requests over HTTP protocol and can-do file system manipulation, keylogging, screen capture, shell command, uploading and downloading a file, and plugin execution. (Appendix 1)
- **BROKEYOLK:** BROKEYOLK is a downloader malware developed with **.Net** that downloads and executes a file from a hard-coded C2 using SOAP API requests over HTTP protocol. (Appendix 2)
- **PINEFLOWER:** PINEFLOWER is an Android Malware with many functions, such as **backdoor functionality**, stealing system information, recording calls, and reading-sending SMS messages. Also, PINEFLOWER can collect location tracking data and download, delete, and upload files besides reading Wi-Fi, Bluetooth, and mobile data connectivity states. (Appendix 3)

APT42's Attack Lifecycle (Source: Mandiant)

APT42 usually begins another spearphishing attack using its victims' **compromised emails** for the lateral movement part of the path. And during this process cycle, APT42 uses custom malware -CHAIRSMACK and GHAMBAR- to maintain its presence and continue its operations, also gaining more information about its victim.

Conclusion

Iranian APT groups are one of the most dangerous threat actors in cyberspace. It is vital to stay more secure and detect before it is too late when they access your organization's infrastructure.

There are to-dos to consider based on Iranian APT groups' activities:

- Evaluate and update your **block list** regularly.
- Back up your data and ensure it is **encrypted**.
- **Audit** user accounts and admin privileges regularly.
- Implement **MFA** when possible.
- **Monitor** remote access logs often.

Following these steps will work for you and your organization, but more is needed. Cyber Threat Intelligence (CTI) services could be an excellent choice to stay safe and informed without being affected.

SOCRadar has a Campaign panel that displays all observations about a specific event on a single page.

SOCRadar's Campaign page "Hackers Behind the Iran" (can be examined detailed from SOCRadar Labs' Campaign panel.)

Also, SOCRadar has a panel that holds all Threat actors and Malware information that can be inspected detailed.

SOCRadar's Threat Actors Panel

When it comes to APT42, the group is still a dangerous cyber espionage group. Because of the relations within IRGC, APT42 will continue targeting the organizations or individuals interested in the Iranian government.

According to the latest analysis published by **HRW (Human Rights Watch)** on December 5, 2022, the group used the WhatsApp platform as a different medium in its recent attacks. These incidents indicate that the group

has chosen the channels they attack from among the current communication channels.

APT42 took the stage using spearphishing, so keep in mind these facts to be safe from spearphishing attacks by APT42:

- They do not use institutional email domains.
- From observed cases, they have seen replying to a blank email as a start of a campaign.
- They ask to collaborate on research about issues relating to the Middle East.

You can analyze suspected emails using free SOC Tools on SOCRadar Labs.

SOCRadar Labs' SOC Tools Panel

Appendix:

Appendix 1. IOCs of GHAMBAR

Names:

- Pavilion.exe,
- MSPavilion.exe,
- tmpD9CB.exe,
- Tmpd9cb.exe

Basic Properties:

- **MD5:** 00b5d45433391146ce98cd70a91bef08
- **SHA-1:** 7649c554e87f6ea21ba86bb26ea39521d5d18151
- **SHA-256:** 2c92da2721466bfbdaff7fedd9f3e8334b688a88ee54d7cab491e1a9df41258f
- **File type:** Win32 EXE
- **File size:** 246.10 KB (252005 bytes)

IOCs of GHAMBAR:

- hxxp[:]//ipinfo[.]io/ip
- hxxp[:]//nvidia-update[.]com[:]5050/D6E90421-1C45-41A4-9250-3F18B9633CE
- 319dc449-ada5-50f7-428e-957db6791668
- hxxp[:]//tempuri[.]org/INew/RegisterNewUser
- hxxp[:]//tempuri[.]org/ITargetUtils/ImOnline
- hxxp[:]//tempuri[.]org/INew/RegisterNewPlugin
- hxxp[:]//tempuri[.]org/ITargetUtils/SendKeyLog
- hxxp[:]//tempuri[.]org/IBuilder/AreYouAvaliable
- hxxp[:]//tempuri[.]org/IMonitoring/GetPluginsInfo
- hxxp[:]//tempuri[.]org/IMonitoring/GetTargetsInfo
- hxxp[:]//tempuri[.]org/ITargetUtils/RegisterTarget
- hxxp[:]//tempuri[.]org/ITargetUtils/SendScreenshot

- hxxp[:]//tempuri[.]org/ICcPluginUtils/InstallPlugin
- hxxp[:]//tempuri[.]org/IMonitoring/GetTargetKeylogs
- hxxp[:]//tempuri[.]org/IMonitoring/TargetPluginsInfo
- hxxp[:]//tempuri[.]org/ICcPluginUtils/UninstallPlugin

Appendix 2. IOCs of BROKEYOLK

Names:

- diag[.]exe
- di2[.]exe
- 7a650d3b1e511a05_di2[.]exe

Basic Properties:

- **MD5:** df02a8a7cb2afb80cc2b789d96f02715
- **SHA-1:** 03d7ffd758e98c9a2c8c4716c93f09687000e22e
- **SHA-256:** 7a650d3b1e511a05d0441484c7c7df59a63003ce77cd4eb7081323fd79d2b9a3
- **File type:** Win32 EXE
- **File size:** 38.00 KB (38912 bytes)

IOCs of BROKEYOLK:

- hxxp[:]//tempuri[.]org/TU,
- hxxp[:]//tempuri[.]org/AbPidById,
- hxxp[:]//tempuri[.]org/Set2,
- hxxp[:]//tempuri[.]org/Set1,
- hxxp[:]//tempuri[.]org/IdCmOne,
- hxxp[:]//tempuri[.]org/CmSById,
- hxxp[:]//tempuri[.]org/HasF,
- hxxp[:]//tempuri[.]org/IdAbOne,
- hxxp[:]//tempuri[.]org/NameAbById,
- hxxp[:]//tempuri[.]org/AbByCount
- hxxp[:]//update-microsoft[.]bid/img/WebService[.]asmx
- hxxp[:]//update-driversonline[.]bid/img/WebService[.]asmx
- dns[.]msftncsi[.]com
- msdl[.]microsoft[.]com -> Request: GET /download/symbols/libcef.dll.pdb/FD4C20AFD16A4088AB999A485492C433b/libcef.dll.pd_ HTTP/1.1

Appendix 3. IOCs of PINEFLOWER

Names:

- Users.apk,
- 90e5fa3f382c5b15a85484c17c15338a6c8dbc2b0ca4fb73c521892bd853f226.bin,

- F3d25b1cedf39beee751eb9b2d8d2376.virus

Basic Properties:

- **MD5:** f3d25b1cedf39beee751eb9b2d8d2376
- **SHA-1:** dbb64b0202bb4da6796279b5fa88262a6e31787e
- **SHA-256:** 90e5fa3f382c5b15a85484c17c15338a6c8dbc2b0ca4fb73c521892bd853f226
- **File type:** Android
- **File size:** 71.03 KB (72734 bytes)

Android Info

- **Android Type:** APK
- **Package Name:** com.google.android.services.control
- **Main Activity:** com.google.android.services.control.Main
- **Internal Version:** 1
- **Displayed Version:** 1.0
- **Minimum SDK Version:** 10

Certificate Subject:

- **Distinguished Name:** O:GoogleServices
- **Organization:** GoogleServices

Permissions:

- android.permission.CHANGE_NETWORK_STATE
- android.permission.PROCESS_OUTGOING_CALLS
- android.permission.ACCESS_COARSE_LOCATION
- android.permission.BLUETOOTH
- android.permission.INTERNET
- android.permission.BLUETOOTH_ADMIN
- android.permission.ACCESS_FINE_LOCATION
- android.permission.SEND_SMS
- android.permission.WRITE_SMS
- android.permission.READ_CALL_LOG
- com.android.browser.permission.READ_HISTORY_BOOKMARKS
- android.permission.WRITE_EXTERNAL_STORAGE
- android.permission.RECORD_AUDIO
- android.permission.CALL_PHONE
- android.permission.READ_PHONE_STATE
- android.permission.READ_SMS
- android.permission.SYSTEM_ALERT_WINDOW
- android.permission.CAMERA
- android.permission.WAKE_LOCK

- android.permission.CHANGE_WIFI_STATE
- android.permission.RECEIVE_SMS
- android.permission.READ_CONTACTS
- android.permission.MODIFY_AUDIO_SETTINGS
- android.permission.ACCESS_WIFI_STATE
- android.permission.ACCESS_NETWORK_STATE
- android.permission.READ_EXTERNAL_STORAGE
- android.permission.RECEIVE_BOOT_COMPLETED

Activities

- com.google.android.services.control.Main
- com.google.android.services.control.Home

Services

- gs.g.CoreService

Intent Filters By Action

- android.intent.action.MAIN
- com.google.android.services.control.Main
- com.google.android.services.control.Home
- android.provider.Telephony.SMS_RECEIVED
- gs.f.SmsReceiver
- android.net.conn.CONNECTIVITY_CHANGE
- gs.f.NetReceiver
- android.intent.action.BOOT_COMPLETED
- gs.f.BootReceiver

Intent Filters By Category

- Android.intent.category.LAUNCHER
- com.google.android.services.control.Main
- Android.intent.category.HOME
- Com.google.android.services.control.Home

IOCs of PINEFLOWER

- hxxp[:]//hardship-management.com[:]4373/
- com.google.android.services.control

Source: https://socradar.io/dark-web-profile-apt42-iranian-cyber-espionage-group/