GitHub - KittenBusters/CharmingKitten: Exposing CharmingKitten's malicious activity for IRGC-IO Counterintelligence division (1500)

By KittenBusters

Archived: 2026-04-06 00:13:15 UTC

Exposing CharmingKitten's malicious activity for IRGC-IO division Counterintelligence division (1500)

Episode 1

Today, we begin exposing the Iranian APT affiliated with the Counterintelligence Division (Unit 1500) of the IRGC-IO, known as **Charming Kitten**.

Leadership

Heading this operation is **Abbas Rahrovi** (aka **Abbas Hosseini**, National Number: 4270844116), an IRGC official who has established several front companies in recent years through which he manages the APT. Over the years, he directed attacks against dozens of targets including:

- Telecommunications companies
- Aviation companies
- Intelligence organizations
- and more...

The primary focus of this APT is on countries in the Middle East and Gulf region, including **Turkey, UAE, Qatar, Afghanistan, Israel, Jordan** and others.

Activities

Under the guidance of the head of the Counterintelligence division, this APT has also targeted and tracked **Iranians both within Iran and abroad** who have been identified as “regime opponents.”

Evidence of Operations

The exposure includes:

- Official documents from the APT’s internal network
- Employee photos
- Attack reports
- Translation documents
- Files from the APT’s internal chat networks (Issabelle, 3CX, Output Messenger)

…and much more evidence proving their malicious activities.

These individuals believed they were operating under the protective cover of the IRGC — **today, they will be recognized worldwide as agents of the IRGC.**

Episode 2

As we mentioned, every few days, we will upload more materials from the Charming Kitten network (Department 40) under the management of Abbas Rahrovi.

Before describing the new content we have uploaded, we would like to address several clarifications based on your questions:

- The unit responsible for intelligence gathering in the IRGC is called the IRGC Intelligence Organization (also known as IRGC-IO for short). Under this unit, there are several divisions, each with a cyber unit that serves the division's needs.
- In the cyber community, the term "Charming Kitten" is often used as a general term for the activities of the IRGC-IO without distinguishing between the various divisions.
- The Counterintelligence Division (Division 1500) operates under the IRGC, and as mentioned, Department 40 operates under it – this is the Charming Kitten whose disgraceful activities have now been exposed.
- For example, see reports on publicly available tools (such as BellaCiao and CYCLOPS) – these are malware tools used by the department. How do we know this? In the following episodes, we will provide information linking the publicly available data to the department's private reports.

The division utilizes the department's capabilities for its own needs (counterintelligence) – advancing cyberattacks against Iranian citizens, Iranian exiles ("regime opponents"), European, Israeli, and Arab citizens. All of this is to promote terrorist activities.

The files we have uploaded include:

- Additional attack reports (on government entities, civilian companies, media organizations, etc., in countries such as Jordan, Iran, Kuwait, Saudi Arabia, Turkey, and more)
- Daily work reports of department employees
- Department server logs (e.g., the AMEEN ALKHALIJ server, a website the department set up to recruit former government and security employees from the United Arab Emirates)

As we mentioned, we will begin exposing the identities of the unit's employees – one of the attackers from Karaj team we published in Episode 1 is called **Vahid Molawi (see the hours report) – his national ID number is 0323217087**.

Let's eliminate this APT once and for all!

Episode 3

Following through on our promise, this time adding new information regarding IRGC-IO , the counterintelligence division (unit 1500) "department 40" malware activity and source code.

In this episode, **you'll find the source code of the BellaCiao malware**, which has been analyzed and published by BitDefender (https://www.bitdefender.com/en-us/blog/businessinsights/unpacking-bellaciao-a-closer-look-at-irans-latest-malware.).

Technological analysis:

1. BellaCiao is a .NET-based dropper with two known variants:

- The first variant drops a C# webshell that enables file upload, file download, and command execution.
- The second variant drops a PowerShell script that establishes a reverse proxy using Plink (part of the PuTTY suite) and executes a customized version of a publicly available PowerShell webserver. (https://github.com/r00t-3xp10it/venom/blob/master/aux/Start-Webserver.ps1).

2. For example, look how Charming-Kitten carried out an attack on the Turkish Foreign Ministry using Bellaciao, and additional attacks using their webshells.
3. Additionally, a dedicated Python & Webshells Framework is included. This framework comprises dedicated webshells and Python scripts. The Python scripts act as a command management interface on the attacker's side, while the webshells deployed on the victim's system execute commands and relay the output back.
4. Details on the "TAGHEB system" intended for infecting and obtaining access to the Windows operating systems.
5. Furthermore, the documents include information such as: Testing of malware tools against AV products for stealthier operation (e.g., Microsoft Defender, Kaspersky, Avira, ESET, and others), Training programs, Technical details about espionage, malware tools, and Intelligence reports focusing on the Israeli entity in various ways.

Intelligence analysis

1. 682089f4bd1c3e6636e15b89e967bf4fa9d7861a_#78TPDD - The Iranian directive reflected in the campaign's activity, which includes Iranian involvement in cyber attacks and public influence platforms such as MOSESS STAFF, can also be seen.
2. 5e98006a2cf1c15a164279558eed4a15018e34a0_بسمه تعالی - Another cover company used by the campaign is now exposed.– " JARF/ZHARF ANDISHAN TAFACOR SEFID" (ژرف اندیشان تفکر سفید). The document is signed by the company director and an IRGC-IO official - MANOOCHEHR VOSOUGHI NIRI (منوچهر وثوقی نیری) and indicates another employee in this APT - MOHAMMAD ERFAN HAMIDI AREF (.(محمد عرفان حمیدی عارفا
3. Abbas Rahrovi is leading the campaign's activity, assets, and malicious activity against international targets. Abbas is a "shadow man", but the campaign he has set up has now been exposed, and is very embarrassing for the Iranian leadership.

Episode 4

Overview

In the previous release, we shared the **SOURCE CODE files** of the **BELLACIAO malware**. This release is a significant follow-up, exposing the **unified infrastructure Excel sheet** used by the group to document all their servers:

- **Procurement identities**
- **Server login credentials**
- **Details of attack servers** (e.g., Tunnel)
- **File storage servers**
- **Other operational infrastructure**

Key Personnel

- **MOHAMMAD NAJAFLOO** (ID: `4270878835`): A former senior employee who maintained these Excel sheets for years.
- **MOHAMMADERFAN HAMIDIAREF** (ID: `0023199709`): Took over the role after NAJAFLOO's departure and continued managing the infrastructure.

Proof of CHARMING KITTEN Connection

To verify the link to **CHARMING KITTEN**, analyze the servers listed in the Excel sheet. You will find that these servers were used by:

- **BELLACIAO**
- **CYCLOPS**
- Other related groups

Sensitive Information Exposed

The files include:

- Passwords for servers on the group's **internal network**.
- Access details for systems such as:
- Internal communication platforms (**ISABELLE**, **3CX**, **SIGNAL**)
- File extraction systems
- Storage servers

Additional Files Included

1. **Materials obtained by the group from the Dubai Police**
2. **"The Group's Phishing Guide"**
3. **Penetration report for a medical entity**

Call to Action

We encourage you to analyze the provided files and share your insights. Your findings will help further expose the group's operations and infrastructure.

Stay tuned for the next episode!

⚠️ **Ongoing Exposures:**
Every few days, we will release more evidence about their activities, along with additional information about their personal lives.

For further questions, feel free to reach out via email: orangemulator@outlook.com.
