← Blog

Anastasia Tikhonova
Global Threat Research Lead

Nikita Rostovcev
APAC Technical Head - ASM, TI & DRP

Catching fish in muddy waters

How the hacker group MuddyWater attacked a Turkish manufacturer of military electronics

May 29, 2019 · min to read · Threat Intelligence

APT MuddyWater Threat Research Turkey

Iranian nation-state hackers are in trouble. Throughout the spring, unknown individuals published “secret leaks” on Telegram. They disclosed information about APT groups affiliated with the Iranian government (**OilRig** and **MuddyWater**), including their tools, victims, and links. But the leaks didn’t reveal everything. In April, Group-IB specialists discovered a leak of email addresses belonging to the Turkish corporation ASELSAN A.Ş, which produces tactical military radio stations and electronic defense systems for the Turkish military forces. **Anastasia Tikhonova**, Head of Group-IB’s APT Research Team, and **Nikita Rostovtsev**, Junior Analyst at Group-IB, examined the course of the attack on ASELSAN A.Ş and identified an alleged member of **MuddyWater**.

Telegram leak

The “disclosure” of Iranian APT groups began with someone by the username Lab Dookhtegan releasing the source code of six tools belonging to the group APT34 (aka OilRig and HelixKitten). The user disclosed the IP addresses and domains involved in the operations, as well as data about 66 victims, including Etihad Airways and Emirates National Oil. Lab Dookhtegan also leaked information about the group’s past operations and employees of the Iranian Ministry of Intelligence and Security who were allegedly linked to the group’s operations. OilRig is an Iran-backed APT group that has been operating in the wild since 2014. The group targets government, financial and military organizations as well as energy and telecommunications companies in the Middle East and China.

After the OilRig exposure, the leaks continued. Information about the activities of another Iranian state-sponsored group, MuddyWater, appeared on the dark web and Telegram. Unlike the first leaks, however, this time, the leaks contained not source codes but dumps, including screenshots of the source codes, C&C servers, and IP addresses of the victims. A hacker group called Green Leakers claimed responsibility for the MuddyWater leak. The group owns several Telegram channels and dark web sites advertising and selling data related to MuddyWater operations.

Cyber spies from the Middle East

MuddyWater is a hacker group that has been active in the Middle East since 2017. According to Group-IB experts, from February to April 2019, the hackers conducted a series of phishing campaigns targeting government entities, educational organizations, and financial, telecommunications, and defense companies in Turkey, Iran, Afghanistan, Iraq, and Azerbaijan.

The group used a proprietary PowerShell backdoor called **POWERSTATS**. The backdoor has the following functionalities:

- Collecting data about local and domain accounts, available file servers, internal and external IP addresses, and OS name and architecture;
- Executing code remotely;
- Uploading and downloads files via the C&C server;
- Detecting debugging programs used to analyze malicious files;
- Disabling the attacked device if malware analysis tools are detected;
- Deleting files from local drives;
- Taking screenshots;
- Disabling Microsoft Office security features.

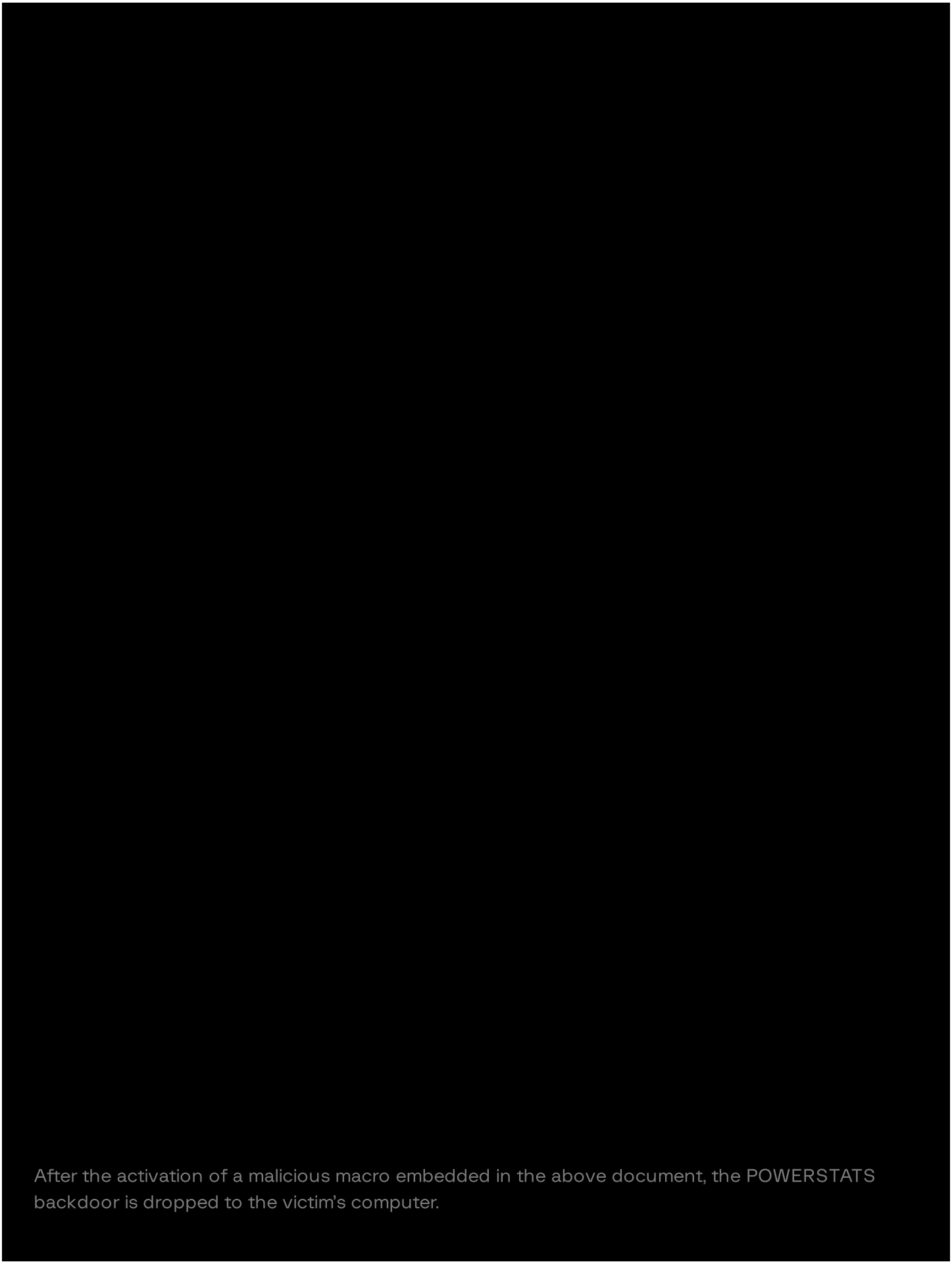
The group eventually made a mistake, and researchers from ReaQta were able to determine the threat actors' real IP address, which was located in Tehran. Based on the group's targets and cyber espionage goals, ReaQta experts suggested that the group represented the interests of the Iranian government.

Indicators of Attack

Turkey at gunpoint

On April 10, 2019, Group-IB specialists discovered a leak of email addresses belonging to ASELSAN A.Ş, the largest defense electronics company in Turkey. Its product range includes radar and electronic warfare, electro-optics, avionics, unmanned and air defense systems, as well as land, naval, and weapon systems.

While studying one of the new POWERSTATS samples, Group-IB experts established that MuddyWater used a license agreement between Koç Savunma (an information and defense technology solutions company) and Tubitak Bilgem (an R&D institute in the field of software technologies) as bait. The document specified Tahir Taner Tımış as a contact person for Koç Savunma. This person was the Programs Manager at Koç Bilgi ve Savunma Teknolojileri A.Ş. from September 2013 to December 2018. He later worked at ASELSAN A.Ş.



After the activation of a malicious macro embedded in the above document, the POWERSTATS backdoor is dropped to the victim's computer.

The metadata of that decoy document (MD5: **0638adf8fb4095d60fbef190a759aa9e**) revealed three additional samples containing identical values, including the timestamps, the username, and the list of contained macros:

ListOfHackedEmails.doc (**eed599981c097944fa143e7d7f7e17b1**)

asd.doc (**21aebece73549b3c4355a6060df410e9**)

F35-Specifications.doc (**5c6148619abb10bb3789dcfb32f759a6**)

One of the discovered documents, named **ListOfHackedEmails.doc**, contained a list of 34 email addresses relating to the domain **@aselsan.com.tr**.

Group-IB specialists checked the email addresses across all the publicly available leaks and established that 28 of them had been compromised as part of previously discovered leaks. Checking the mix of available leaks helped identify about 400 unique login details associated with this domain, including the passwords. It's possible that the threat actor used the publicly available data to target ASELSAN A.Ş.

The samples found contained a document called **F35-Specifications.doc**, which referred to the F-35 multi-functional fighter jet. The decoy document contained the specifications for the F-35, indicating the characteristics of the aircraft and its price. The subject of the decoy document relates to the US refusal to supply F-35s after Turkey purchased the Russian S-400 systems, which could lead to information about the F-35 Lightning II being transferred to Russia.

All the information obtained indicated that organizations in Turkey were the main target of the MuddyWater attacks.

Who are Gladiyator_CRK and Nima Nikjoo?

In March 2019, malicious documents created by a Windows user Gladiyator_CRK were detected. These documents also distributed POWERSTATS and communicated with a C&C server **gladiyator[.]tk**.

This may be related to the fact that on March 14, 2019, the user Nima Nikjoo posted a tweet in which they tried to decode an obfuscated code related to MuddyWater. In the comments to the tweet, the researcher said that they could not share the indicators of compromise for the malware as the information was confidential. The tweet was deleted, but its traces remain on the web:

Nima Nikjoo owns the Gladiyator_CRK profile on the Iranian video hosting services dideo.ir and videoi.ir. TThe user utilizes these two resources to demonstrate PoC exploits designed to disable antivirus tools by various vendors and bypass sandboxes. Nima Nikjoo claims to be a network security specialist, a reverse engineer, and a malware analyst at MTN Irancell, an Iranian telecommunications company.

Below is a screenshot of saved videos in Google search engine results:

On March 19, 2019, Nima Nikjoo changed his Twitter handle to "*Malware Fighter*" and removed posts and comments. All videos were also removed from the Gladiyator_CRK profile on dideo.ir, and the YouTube profile was deleted. On April 16, 2019, however, the Twitter account was again renamed "*Nima Nikjoo*".

Group-IB specialists established that Nima Nikjoo had already been mentioned in connection with cybercriminal activities. In August 2014, the Iran Khabarestan blog published information about individuals linked with the Nasr Institute. One of FireEye's investigations stated that the Nasr Institute was an APT33 contractor and was also involved in DDoS attacks on US banks between 2011 and 2013 as part of a campaign called Operation Ababil.

The same blog post mentioned Nima Nikju-Nikjoo, who had supposedly developed malware to spy on Iranians. The post mentioned the developer's email address: *gladiyator_cracker@yahoo[.]com*.

Below is a screenshot of information related to the Nasr Institute:

Translation of the highlighted text: Nima Nikio – Spyware developer – Email address:

As the screenshot shows, the email address is linked to the address used in the attacks and to the users Gladiyator_CRK and Nima Nikjoo.

In addition, in 2017, researchers revealed that Nikjoo had carelessly mentioned Kavosh Security Center in his resume. It has been reported that the Iranian state used Kavosh Security Center to fund nation-state hackers.

Information about the company at which Nima Nikjoo worked:

The LinkedIn profile of Nima Nikjoo lists Kavosh Security Center as his first place of work, where he worked between 2006 and 2014. He performed malware analysis, reverse engineering, and code obfuscation.

Information on LinkedIn about the company where Nima Nikjoo worked:

MuddyWater and inflated self-esteem

Interestingly, **MuddyWater monitors all reports and messages about it published by cybersecurity experts**. The group initially left false flags to throw researchers off their trail. For example, the group's first attacks misled experts, who discovered the use of DNS Messenger, commonly associated with the group FIN7. In other attacks, MuddyWater inserted strings in Chinese into the code.

The group also leaves messages for researchers. For example, they did not appreciate that Kaspersky Lab placed MuddyWater in 3rd place in its threat ranking. At the time, someone (presumably a member of MuddyWater) uploaded to YouTube a PoC exploit that disabled Kaspersky anti-virus software. They also left a comment under the article.

Screenshots of the video showing how to disable the Kaspersky Lab antivirus and the comment under Kaspersky's Security Bulletin can be found below:

It is still difficult to make an unambiguous conclusion about how and to what extent Nima Nikjoo was involved in the MuddyWater attacks. Group-IB experts are considering two possibilities. The first one is that Nima Nikjoo could be a hacker from MuddyWater who was identified due to his negligence and high online activity. The second possibility is that he was intentionally "outed" by other group members in order to divert suspicion from themselves. Group-IB experts will continue with their investigation and report what they find.

As for the Iranian APTs, the series of leaks means that they are likely to face a serious "debriefing". The hackers will be forced to change their tools, clean up any traces they have left, and find any "rats" among them. Experts had not ruled out that the groups would take a timeout, but after a short break, the Iranian APT attacks resumed.

Share this article

Found it interesting? Don't hesitate to share it to wow your friends or colleagues

Internship
Academic Aliance
Sustainability
Media Center
Contact

Subscription plans
Services
Resource Center

Contact

APAC: +65 3159 3798
EU & NA: +31 20 226 90 90
MEA: +971 4 568 1785

info@group-ib.com

Subscribe to stay up to date with the latest cyber threat trends