FBI FLASH
ACTIONABLE CYBER INTELLIGENCE
20 March 2026
FLASH Number
FLASH-20260320-001

Government of Iran Cyber Actors Deploy Telegram C2 to Push Malware to Identified Targets

Summary

The Federal Bureau of Investigation (FBI) is releasing this FLASH to disseminate information on malicious cyber activity conducted by actors on behalf of the Government of Iran Ministry of Intelligence and Security (MOIS). Specifically, MOIS cyber actors are responsible for using Telegram as a command-and-control (C2) infrastructure to push malware targeting Iranian dissidents, journalists opposed to Iran, and other opposition groups around the world. This malware resulted in intelligence collection, data leaks, and reputational harm against the targeted parties. The FBI is releasing this information to maximize awareness of malicious Iranian cyber activity and provide mitigation strategies to reduce the risk of compromise.

Due to the elevated geopolitical climate of the Middle East and current conflict, the FBI is highlighting this MOIS cyber activity. The FBI assessed MOIS cyber actors are responsible for using Telegram as a C2 infrastructure to push malware targeting Iranian dissidents, journalists opposed to Iran, and other oppositional groups around the world. This FLASH warns network defenders and the public of continued malicious cyber activity by Iran MOIS cyber actors and outlines the tactics, techniques, and procedures (TTPs) used in this malware campaign.

Background Information

The FBI assesses Iran MOIS cyber actors deployed multiple versions of the malware to infect machines running Windows operating systems, dating back to the Fall of 2023. The observed victim profile included Iranian dissidents, journalists opposed to Iran, members of organizations with beliefs counter to Government of Iran narratives, and other individuals Iran perceives as a threat to the Iranian government. However, the malware could be used to target any individual of interest to Iran. The malware used as part of this cyber activity included a multi-stage payload enabling remote user access to the infected devices. Threat actors used social engineering to customize the first stage of the malware to masquerade as commonly used programs or services on Windows machines. The second stage connected the infected machine to Telegram command and control bots that enabled remote user access to exfiltrate screen captures or files from the victim devices.

In July 2025, the online entity known as “Handala Hack” claimed responsibility for a hack-and-leak operation targeting multiple persons voicing concerns about current events in Iran that conflicted with the Government of Iran’s rhetoric. The FBI assesses some of the information Handala Hack claimed to have acquired and posted online was obtained using malware as part of the group’s ongoing campaign to target

dissidents. Handala Hack is known for phishing, data theft, extortion, and destructive attacks involving custom wiper malware. Additionally, the FBI assesses Handala Hack is linked to the online entity "Homeland Justice," also operated by Iran MOIS cyber actors.

Iran MOIS cyber actors consistently leverage state-directed Advanced Persistent Threats (APT) and proxy groups to carry out hacktivist-style attacks, including hack-and-leak operations, which blend technical compromises with disinformation. The campaigns typically involve the theft of perceived sensitive data, its manipulation or selective exposure, and public distribution through aligned media channels to maximize reputational or political damage. MOIS' use of Telegram as the C2 to push malware to carry out a campaign targeting Iranian dissidents is an example of Iran MOIS cyber actors' efforts to advance Iran's geopolitical agenda.

Technical Details

Malware Overview

FBI obtained malware samples through investigations. The samples were categorized as masquerading malware (stage 1), persistent implant (stage 2), and related stage 2 malware that contained additional or unique functions (**Figure 1** shows the observed behavioral cluster of the malware). Stage 1 usually masqueraded as commonly used applications like Pictory, KeePass, and Telegram and contained the binaries for the next stage of malware. The persistent implant malware spawned following the masquerading malware's execution and possible user interaction with the malicious application. At this stage, the Iran MOIS cyber actors configured a command and control (C2) using a Telegram bot, allowing bidirectional communication between the compromised device and api.telegram[.]org. FBI considered the masquerading malware and persistent implant to be core functionality for the malware campaign. Related malware was usually found on compromised devices in addition to the core functionality. For example, malware found in MicDriver.zip contained logic to record screen and audio while a Zoom session was active.

FBI FLASH
ACTIONABLE CYBER INTELLIGENCE

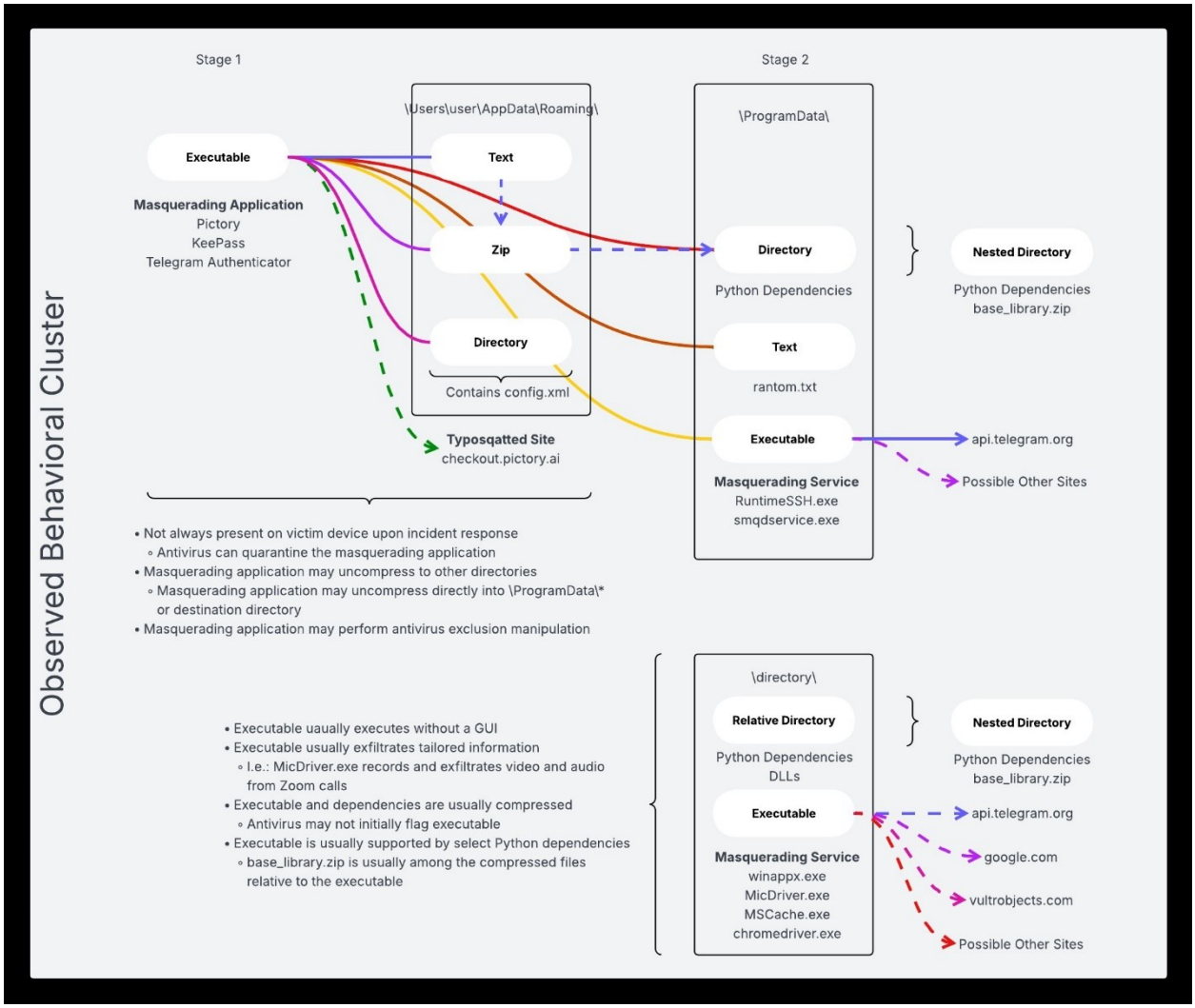

Figure 1. Observed Behavioral Cluster – While all malware samples function differently, each serve a specific purpose and can be placed in one of the above "executable" portions.

Initial Access

Threat actors relied upon social engineering to deliver malware and infect victim devices. The Iranian cyber actors engaged with a targeted victim via social messaging applications and masqueraded as a known individual or technical support from the social messaging platform. The Iranian cyber actors then convinced the victim to accept a file transfer consisting of the masquerading stage 1 malware. When the victim opened the file, the malware infected the victim's device and launched the persistent implant stage 2 malware. Based on multiple observations, stage 1 of the malware appeared to be tailored to the victim's pattern of life to increase likelihood of victim downloading the malware, which indicates the Iranian cyber actors likely performed target reconnaissance prior to engaging with the victim.

Execution

Malware analysis flagged the execution of numerous malware samples as part of the malware campaign. Once the initial access was established to the victim system the malware downloaded follow-on malware. The stage 1 or masquerading malware included the following:

- Telegram_authenticator.exe
- WhatssApp.exe
- KeePass.exe
- Pictory_premium_ver9.0.4.exe

Persistence

Malware performed defensive evasion, which excluded directories and allowed PowerShell to execute malware without warning. Furthermore, a reference to malware was added to the Windows registry to autorun stage 2 malware. Stage 2 malware samples served as persistent implants.

Collection and Exfiltration

The malware campaign used multiple malware samples to exfiltrate data. These included the following samples:

- MicDriver.exe/MicDriver.dll
- Winappx.exe
- MsCache.exe
- RuntimeSSH.exe
- smqdservice.exe

Functionality of the above-mentioned malware samples included: Screen recordings and audio, cache captures, perform file compression with a password, perform file deletion, and stage compressed files to be sent to api.telelgram[.]org.

Indicators

Malware Variations

File Name	*MD5 Hash*
KeePass.exe	7402F2F9263782A4C469570035843510
MicDriver.dll	F8B5554808428291ACC65D1FD2EFE01C
MicDriver.exe	D70EBF20E3D697897BAD5BEBF72EA271
MsCache.exe	3E7A2FCEF1D038D05B20148C573A6499
Pictory_premium_ver9.0.4.exe	1E6B601F733BC40EAA58916986BFC5B9

File Name	*MD5 Hash*
rantom.txt	A3394EF7FFA7E88B2E7EFAEE4617FE04
rantom.txt	2965817D063F1E8F9889F9126443D631
RuntimeSSH.exe	EBDD9595B79B39F53909D862499DBC94
RuntimeSSH.exe	E51FF37FB431767DCDEC0B5E6D2A786A
smqdservice.exe	7E23FFADB664B0E53D821478A249D84C
Telegram_Authenticator.exe	B9086413E7B6A0C6A11C25D14C22615F
winappx.exe	481C5B5E69A08C3DF206C59FD8DDC0DC

Recommended Mitigations:

The FBI recommends caution with regards to receiving emails or other online communications from unknown individuals, or communications of an unfamiliar nature from known individuals.

1. Ensure your devices are updated with latest operating system and install software updates regularly.
2. Only download software from trusted sources, such as official app stores or vendor websites.
3. Enable antivirus or anti-malware software on your device and run antivirus software regularly.
4. Use strong, unique passwords and enable multi-factor authentication.
5. Report suspicious emails or messages to the email client. If you suspect a crime, please report to your local FBI field office.

Reporting Notice

If you identify suspicious activity within your enterprise or have information related to the contents of this document, please contact your local FBI Cyber Squad immediately at **www.fbi.gov/contact-us/field-offices**. The FBI also encourages you to report suspicious or criminal activity to the FBI Internet Crime Complaint Center at **www.ic3.gov**. When available, each report should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact. Press inquiries should be directed to the FBI's National Press Office at npo@fbi.gov or (202) 324-3691.

Individual indicators included in this document should always be evaluated in light of your complete information security situation. Some indicators, particularly those of a nondeterministic or ephemeral nature (such as filenames or IP addresses), may not be indicative of a compromise.

Your organization has no obligation to provide information in response to this product. If, after reviewing the information provided, your organization decides to provide information to the FBI, it must do so consistent with applicable state and federal law.

Administrative Note

The information in this document is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cybersecurity professionals and system administrators guard against the persistent malicious actions of cyber actors. The FBI does not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by the FBI.

This product is marked **TLP:CLEAR**. The information in this product may be shared without restriction. Information is subject to standard copyright rules.