Iranian MOIS Actors & the Cyber Crime Connection

By stcpresearch

Published: 2026-03-10 · Archived: 2026-04-29 02:10:12 UTC

Key Points

- **Iran-linked actors are increasingly engaging with the cyber crime ecosystem.** Their activity suggests a growing reliance on criminal tools, services, and operational models in support of state objectives.
- Iranian actors have long used cyber crime and hacktivism **as cover** for destructive activity, but the trend now suggests **direct engagement** with the criminal ecosystem.
- **This dynamic appears most prominently among Ministry of Intelligence and Security (MOIS)-linked actors**, particularly **Void Manticore (a.k.a "Handala Hack")** and **MuddyWater**, where repeated overlaps with criminal tools, services, or clusters have been observed.
- Such engagement offers a dual advantage: it **enhances operational capabilities** through access to mature criminal tooling and resilient infrastructure, while **complicating attribution** and contributing to recurring confusion around Iranian threat activity.

Introduction

For years, Iranian intelligence services have operated through deniable criminal intermediaries in the physical world. A similar pattern is now becoming visible in cyber space, where state objectives are increasingly pursued through criminal tools, services, and operational models. Notably, this dynamic appears with growing frequency in activity associated with actors linked to the **Ministry of Intelligence and Security (MOIS)**.

For a long time, Iranian actors sought to mask state activity behind the appearance of ordinary cyber crime, most often by posing as ransomware operators. The trend we are seeing now goes beyond imitation. Rather than simply adopting criminal and hacktivist personas to complicate attribution, some Iranian actors appear to be associating with the cyber criminal ecosystem itself, leveraging its malware, infrastructure, and affiliate-style mechanisms. This shift matters because it does more than improve deniability; it can also expand operational reach and enhance technical capability.

In this blog, we examine several cases that reflect this evolution, including Iranian-linked use of ransomware branding, commercial infostealers, and overlaps with criminal malware clusters. Taken together, these examples suggest that for some **MOIS-associated actors**, cyber crime is no longer just a cover story, but an operational resource.

Background – MOIS and Criminal Activity

Long before concern shifted to the digital arena, some of the clearest signs of cooperation between Iran's intelligence services and criminal actors appeared in plots involving surveillance, kidnappings, shootings, and assassination attempts. In those cases, the value of criminal networks was straightforward: they gave Tehran reach, deniability, and access to people willing to carry out violence at arm's length.

According to the U.S. Treasury, one of the clearest examples involved the network led by narcotics trafficker Naji Ibrahim Sharifi-Zindashti, which Treasury said operated at the behest of MOIS and targeted dissidents and opposition activists. The FBI has similarly said that an MOIS directorate operated the Zindashti criminal network and its associates against Iranian dissidents in the United States.

Sweden has described a similar pattern. According to Sweden's Security Service, the Iranian regime has used criminal networks in Sweden to carry out violent acts against states, groups, and individuals it sees as threats; Swedish officials later linked that concern to attacks aimed at Israeli and Jewish targets, including incidents near Israel's embassy in Stockholm.

Recent activity we have analyzed and associate with MOIS-affiliated cyber actors suggests that the same logic is now being applied in the cyber domain. The emphasis is not only on imitating cyber criminal behavior, but on **associating with the cyber criminal ecosystem itself:** drawing on its infrastructure, access brokers, marketplaces, and affiliate-style relationships.

Void Manticore (Handala) and Rhadamanthys

Void Manticore, an Iranian threat actor linked to several hack-and-leak personas, is one of the most active groups pursuing strategic objectives through cyber operations. It has leveraged "hacktivistic" personas such as Homeland Justice in attacks against Albania and Handala in operations targeting Israel. While the group is most commonly associated with "hack and leak" operations and disruptive attacks, particularly wiper operations, the emergence of its Handala persona also revealed the use of a commercial infostealer sold on darknet forums: **Rhadamanthys**.

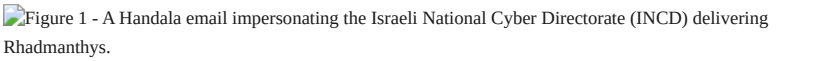
Figure 1 – A Handala email impersonating the Israeli National Cyber Directorate (INCD) delivering Rhadmanthys.

Rhadamanthys is a widely used infostealer employed by a range of threat actors, including both financially motivated groups and state-sponsored operators. It has built a strong reputation due to its complex architecture, active development, and frequent updates. Handala used Rhadamanthys on several occasions, pairing it with one of its custom wipers in phishing lures aimed at Israeli targets, most dominantly impersonating F5 updates.

MuddyWater – Tsundere Botnet and the Castle Loader Connection

MuddyWater, a threat actor that U.S. authorities have linked to Iran's MOIS, has conducted cyber espionage and other malicious operations focused on the Middle East for years. According to CISA, MuddyWater is a subordinate element within MOIS and has carried out broad campaigns in support of Iranian intelligence objectives, targeting government and private-sector organizations across sectors including telecommunications, defense, and energy.

Recent reports detailing the activity of MuddyWater link its operations to several cyber crime clusters of activity. This appears to work in the actors' favor: the use of such tools has created significant confusion, leading to misattribution and flawed pivoting, and clustering together activities that are not necessarily related. This demonstrates that the use of criminal software can be effective for obfuscation, and highlights the need for extreme caution when analyzing overlapping clusters.

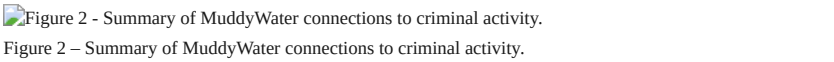
Figure 2 – Summary of MuddyWater connections to criminal activity.

To address this, we attempted to bring structure to the available evidence, to the best of our ability, and identify which activity is truly associated with MuddyWater.

Tsundere Botnet (a.k.a DinDoor)

The Tsundere Botnet was first uncovered in late 2025 and was later linked to MuddyWater. Large parts of its activity rely on Node.js and JavaScript scripts to execute code on compromised machines. In several instances observed in the wild, when the Node.js engine is detected, the botnet shifts to an alternative execution method using Deno, a runtime for JavaScript and TypeScript. Since Deno-based execution had not previously been associated with Tsundere, researchers linking this activity to MuddyWater designated this variant as DinDoor.

Given that two separate sources linked Tsundere to MuddyWater, one via a VPS and the other through vendor telemetry, it is likely that MuddyWater uses the botnet as part of its operations. Another overlap between DinDoor-related activity and known MuddyWater tradecraft is the use of rclone to access a Wasabi server, which traces back to an IP address previously associated with MuddyWater (18.223.24[.]218, linked to eb5e96e05129e5691f9677be4e396c88).

Castle Loader Connection (a.k.a FakeSet)

Another malware family recently linked to MuddyWater is FakeSet, which, according to our analysis, is a downloader used in recent infection chains delivering CastleLoader. CastleLoader operates as a Malware-as-a-Service offering used by multiple affiliates. Based on our understanding, the reported link between CastleLoader and MuddyWater stems from the use of a set of code-signing certificates, specifically under the Common Names "Amy Cherne" and "Donald Gay". Certificates with these common names were also used to sign MuddyWater malware ("StageComp"), Tsundere Deno malware ("DinDoor"), and CastleLoader ("FakeSet") variants.

In our assessment, this does not necessarily indicate that MuddyWater is a CastleLoader affiliate; rather, it suggests that both may have obtained certificates from the same source.

Iranian Qilin Affiliates

In October 2025, Israeli Shamir Medical Center was hit by a major cyber attack that was initially described as a ransomware incident. The attackers claimed to have stolen a large amount of data and demanded a ransom in exchange for not publishing it. Israeli officials said the attack did not affect hospital operations and patient care was not significantly disrupted. Still, some information appears to have been leaked, including limited email correspondence and certain medical data.


Figure 3 – Shamir Medical Center on Qilin Leak Site

At first, the attack was presented as a ransomware incident linked to the Qilin group, but later Israeli assessments pointed much more directly to **Iranian actors** as the real force behind it. Qilin is known as a **ransomware-as-a-service (RaaS)** operation, meaning it provides ransomware infrastructure and tooling to outside partners or "affiliates" who actually carry out intrusions. In this case, the emerging picture was that the attackers were likely **Iranian-affiliated operators working**

through the cyber criminal ecosystem, using a criminal ransomware brand and methods associated with the broader extortion market, while serving a strategic Iranian objective.

This attack did not occur in isolation. It appears to be part of a broader, sustained campaign by MOIS and Hezbollah to target Israeli hospitals, a pattern that has been evident since late 2023. The use of Qilin, and participation in its affiliate program, likely serves not only as a layer of cover and plausible deniability, but also as a meaningful operational enabler, especially as earlier attacks appear to have heightened security measures and monitoring by Israeli authorities.

Conclusion

The cases examined in this blog show that, for some Iranian actors, cyber crime is no longer just a cover for state-directed activity. Across these examples, the pattern is not limited to the appearance of criminal behavior, but includes the use of criminal malware, ransomware branding, and affiliate-style ecosystems in support of strategic objectives. This reflects a clear shift from simply imitating cyber criminals to actively leveraging the cyber crime ecosystem.

This shift matters because it delivers clear operational benefits. For MOIS-linked actors in particular, engagement with criminal tools and services enhances capabilities while complicating attribution and fueling confusion around Iranian activity. Taken together, the cases discussed here show that cyber crime has become not just camouflage, but a practical operational resource.

Indicators of Compromise

Handala Rhadmanthys Variants

aae017e7a36e016655c91bd01b4f3c46309bbe540733f82cce29392e72e9bd1f

Malware samples signed with suspicious certificates

sha256	Certificate Common Name	Certificate Thumbprint
077ab28d66abdafad9f5411e18d26e87fe43da1410ee8fe846bd721ab0cb52de	Amy Cherne	0902d7915a19975817ec1ccb0f2f6714aed1963
ddceade244c636435f2444cd4c4d3dc161981f3af1f622c03442747ecef50888	Amy Cherne	0902d7915a19975817ec1ccb0f2f6714aed1963
2b7d8a519f44d3105e9fde2770c75efb933994c658855dca7d48c8b4897f81e6	Amy Cherne	2087bb914327e937ea6e77fe6c832576338c2af
64cf334716f15da1db7981fad6c81a640d94aa1d65391ef879f4b7b6edf6e7f1	Amy Cherne	21a435ecaa7b86efbec7f6fb61fcda3da686125c
74db1f653da6de134bdc526412a517a30b6856de9c3e5d0c742cb5fe9959ad0d	Amy Cherne	389b12da259a23fa4559eb1d97198120f2a722fe
94f05495eb1b2ebe592481e01d3900615040aa02bd1807b705a50e45d7c53444	Amy Cherne	389b12da259a23fa4559eb1d97198120f2a722fe
4aef998e3b3f6ca21c78ed71732c9d2bdcc8a4e0284f51d7462c79d446fbc7be	Amy Cherne	579a4584a6eef0a2453841453221d0fb25c08c8
a4bd1371fe644d7e6898045cc8e7b5e1562bdfd0e4871d46034e29a22dec6377	Amy Cherne	d920ae0f8ea8b5bd42de49e01c6bbd4c2c6d084
64263640a6fdeb2388bca2e9094a17065308cf8dcb0032454c0a71d9b78327eb	Donald Gay	f8444dfc740b94227ab9b2e757b8f8f1fa49362a
a8c380b57cb7c381ca6ba845bd7af7333f52ee4dc4e935e98b48bb81facad72b	Donald Gay	9dcb994ea2b8e6169b76a524fae7b2d2dcd1807
24857fe82f454719cd18bcbe19b0cfa5387bee1022008b7f5f3a8be9f05e4d14	Donald Gay	b674578d4bdb24cd58bf2dc884eaa658b7aa250
a92d28f1d32e3a9ab7c3691f8bfca8f7586bb0666adbba47eab3e1a8faf7ecc0	Donald Gay	b674578d4bdb24cd58bf2dc884eaa658b7aa250
2a09bbb3d1ddb729ea7591f197b5955453aa3769c6fb98a5ef60c6e4b7df23a5	Amy Cherne	551bdf646df8e9abe04483882650a8ffae43cb55
