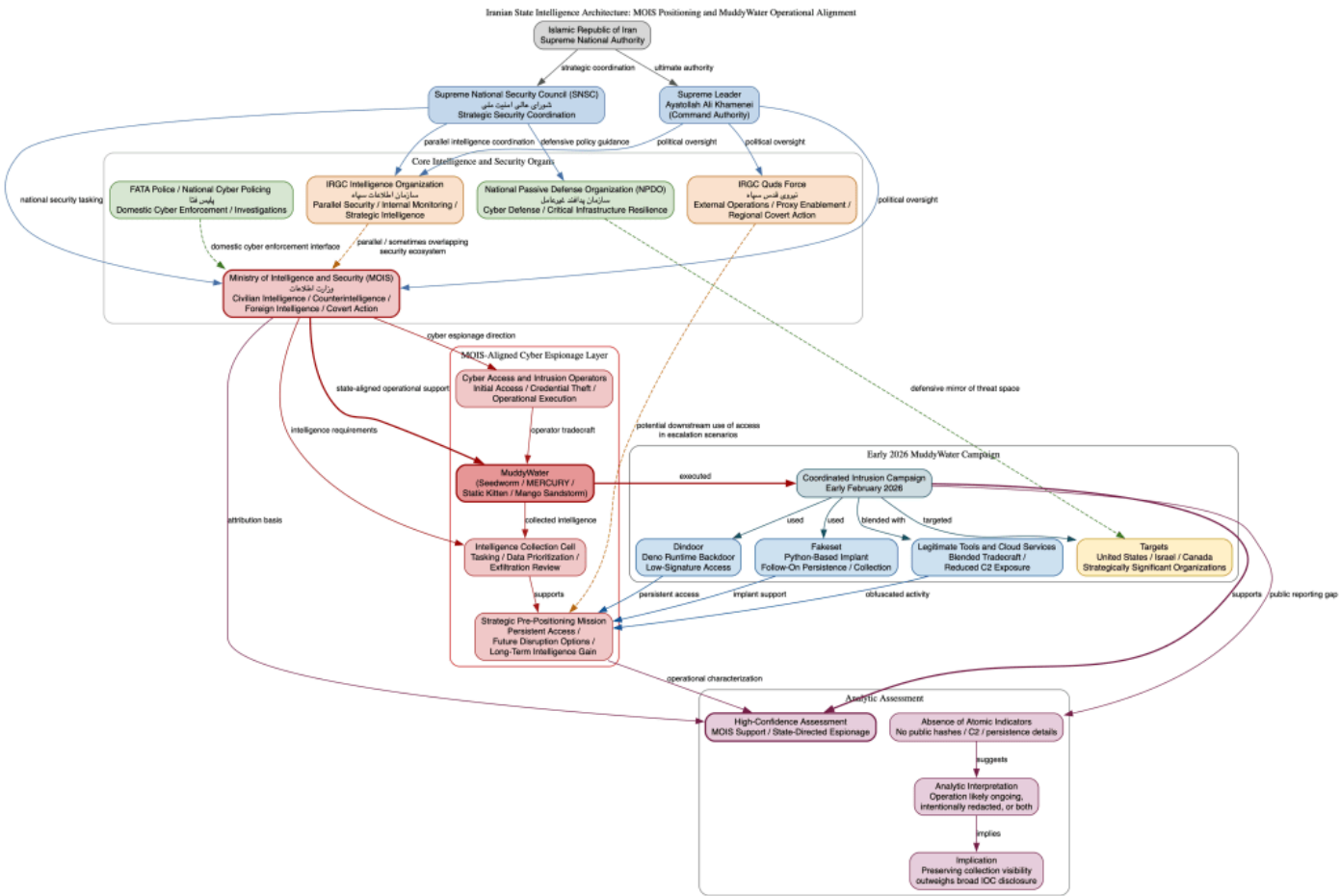


Threat Intelligence Report: MANGO SANDSTORM Dindoor / Fakezet Campaign

krypt3ia.wordpress.com/2026/03/20/threat-intelligence-report-mango-sandstorm-indoor-fakeset-activity

March 20, 2026



[with one comment](#)

Date: March 2026

By: Krypt3ia

Executive Summary

In early February 2026, the Iranian state-aligned cyber espionage group MuddyWater (also tracked as Seedworm, MERCURY, Static Kitten, MOIST KEYCHAIN, and Mango Sandstorm) conducted a coordinated intrusion campaign targeting a small but strategically significant set of organizations across the United States, Israel, and Canada. The campaign, publicly disclosed in

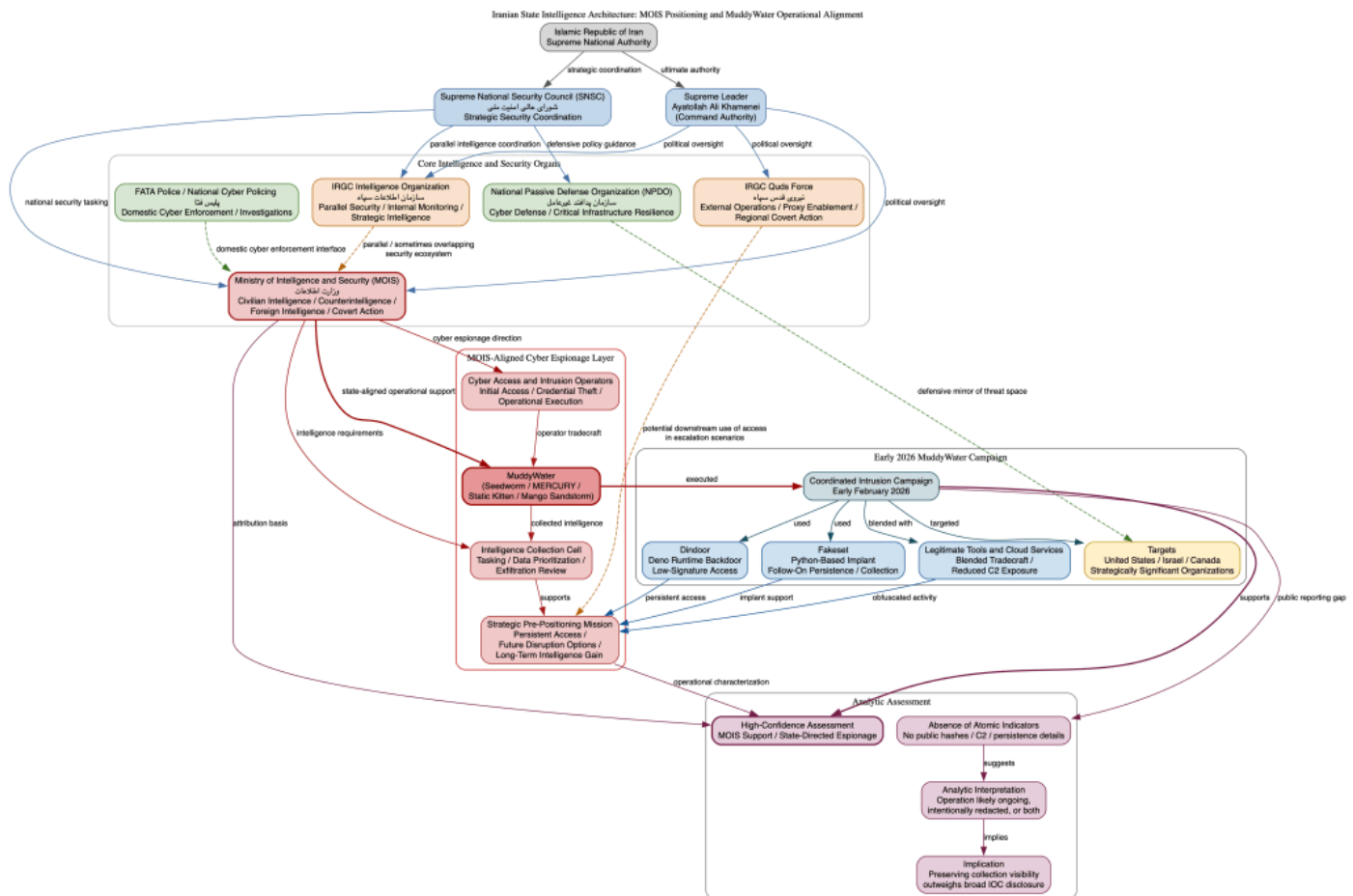
early March 2026, leveraged two malware families Dindoor, a backdoor utilizing the Deno runtime, and Fakeset, a Python-based implant alongside legitimate tooling and cloud infrastructure to establish persistent access and enable data exfiltration.

The available evidence supports a high-confidence assessment that this activity was conducted in support of Iran's Ministry of Intelligence and Security (MOIS) and is best characterized as a strategic pre-positioning and intelligence collection operation conducted during a period of geopolitical escalation following U.S. and Israeli military actions against Iran. The campaign demonstrates a continued evolution in MuddyWater's operational model toward low-signature, behavior-driven intrusion techniques, reduced reliance on traditional command-and-control infrastructure, and increased use of legitimate cloud services to obscure activity.

Critically, the absence of detailed atomic indicators such as file hashes, command-and-control domains, and persistence artifacts indicates that the operation is either ongoing, intentionally redacted by reporting entities, or both. This absence itself is analytically significant and suggests a higher-tier intelligence operation in which preserving visibility into adversary activity outweighs the immediate value of broad indicator disclosure.

Actor Overview

MuddyWater has operated since at least 2017 as a persistent Iranian cyber espionage actor aligned with MOIS. The group has historically targeted government, telecommunications, defense, energy, and financial sectors across the Middle East, Europe, Asia, Africa, and North America. Its tradecraft has consistently combined custom malware with dual-use administrative tools, including PowerShell, remote management frameworks, and credential harvesting utilities.



Previous campaigns have employed malware families such as PowGoop, Small Sieve, Mori, POWERSTATS, Canopy/Starwhale, and more recently MuddyViper and GhostBackDoor variants. These campaigns typically rely on spearphishing, exploitation of known vulnerabilities, DLL sideloading, and script-based execution to establish initial access and persistence.

Campaign Overview

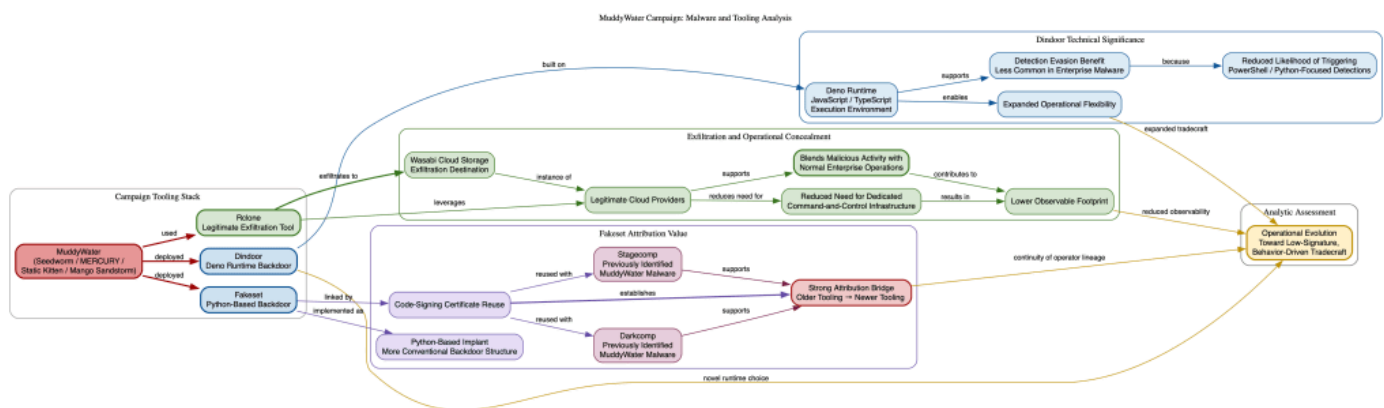
The intrusion activity observed between February and March 2026 resulted in confirmed compromises across a narrowly scoped but strategically meaningful set of targets. These included a United States based financial institution, a U.S. airport, a Canadian non-profit organization, and the Israeli subsidiary of a U.S. software company supporting defense and aerospace customers. The selection of these entities reflects a deliberate focus on sectors that provide both intelligence value and potential downstream operational leverage, particularly in the context of heightened geopolitical tensions.

Within these environments, operators associated with MuddyWater established and maintained access through the deployment of the Dindoor backdoor and the Fakeset Python-based implant. These tools enabled persistent footholds while minimizing overt indicators of compromise. In at least one instance, the operators attempted to exfiltrate data using Rclone, directing collected information to a Wasabi cloud storage bucket. Supporting infrastructure tied to malware delivery and staging was also observed leveraging Backblaze B2 storage services.

This pattern of activity is consistent with a broader operational model in which legitimate cloud platforms are repurposed to support intrusion workflows, allowing adversaries to blend malicious traffic with routine enterprise network activity and thereby reduce the likelihood of detection. with a broader shift toward leveraging legitimate infrastructure to minimize detection and complicate attribution.

Malware and Tooling Analysis

Dindoor constitutes the most notable technical evolution observed in this campaign. Its reliance on the Deno runtime a JavaScript and TypeScript execution environment that remains uncommon within enterprise malware ecosystems reflects a deliberate attempt to bypass detection controls calibrated for more traditional scripting frameworks such as PowerShell and Python. By shifting into a less-monitored execution context, the operators gain both increased operational flexibility and a measurable reduction in the probability of triggering established behavioral analytics.



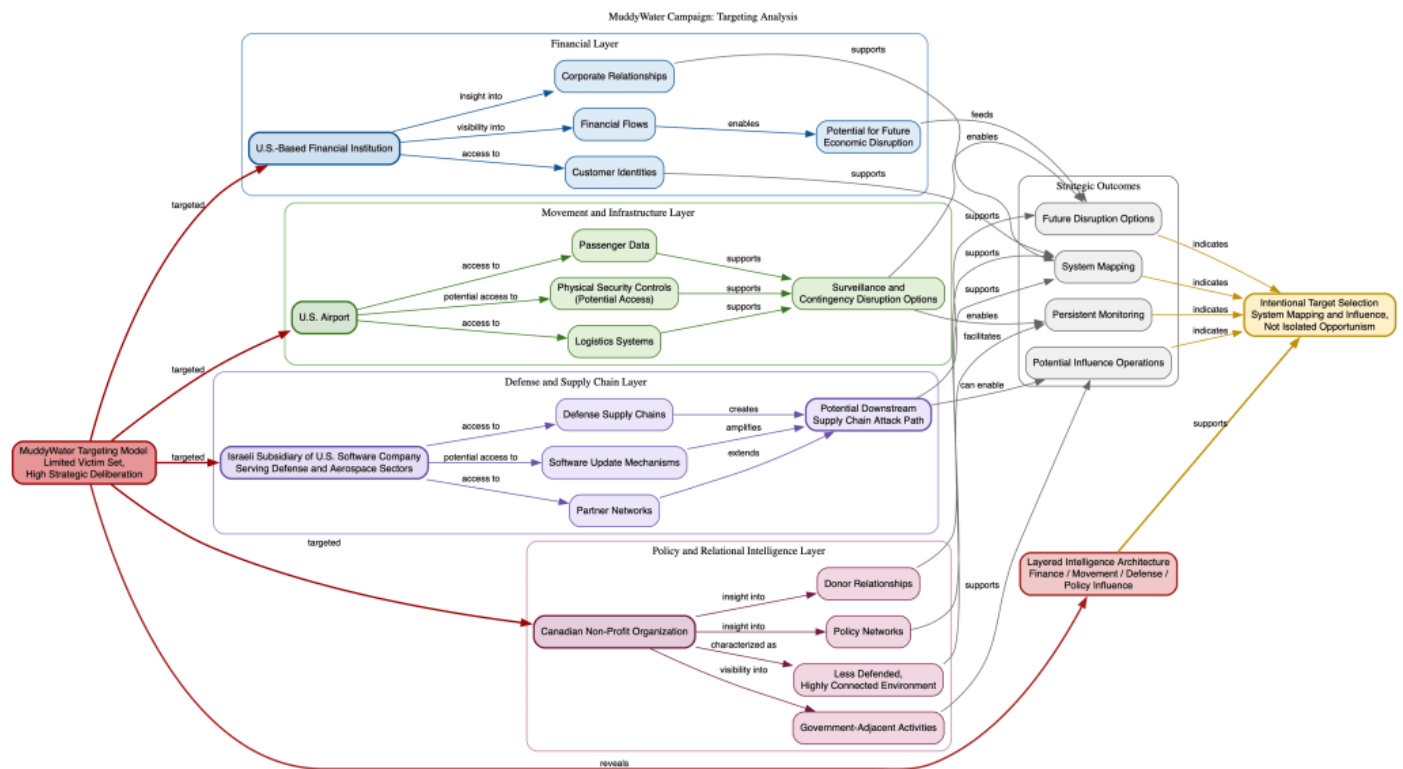
Fakeset, by contrast, adheres to a more conventional design as a Python-based backdoor. Its significance is not rooted in novelty, but in attribution. The reuse of code-signing certificates previously associated with MuddyWater malware families, specifically Stagecomp and Darkcomp, creates a direct lineage between legacy and current tooling. This continuity materially strengthens attribution confidence, linking the present operation to established development pipelines and operator tradecraft.

The incorporation of Rclone for data exfiltration further illustrates MuddyWater's preference for leveraging legitimate, widely deployed utilities to obscure malicious activity. By transmitting exfiltrated data to cloud storage platforms such as Wasabi, the operators eliminate the need for bespoke command-and-control infrastructure. This approach reduces their network signature, complicates detection, and allows malicious traffic to blend seamlessly with routine enterprise cloud usage.

Targeting Analysis

The observed victimology is limited in scale but exhibits clear intentionality in its composition. Each targeted entity occupies a distinct functional layer within the broader architecture of Western and allied systems, suggesting a selection process driven by systemic value rather than opportunistic access.

The compromised financial institution provides insight into financial flows, customer identities, and inter-organizational relationships. Access of this nature yields both immediate intelligence value and potential leverage for future economic disruption or coercive activity. It enables mapping of capital movement, identification of high-value individuals or entities, and the possibility of downstream financial manipulation.



The airport represents a critical node within transportation infrastructure. Intrusion into this environment offers access to passenger data, logistics systems, and, in some cases, elements of physical security control. Such positioning supports surveillance objectives, including movement tracking and pattern analysis, while also creating latent options for disruption under escalation conditions.

The Israeli subsidiary of a U.S. defense-aligned software company constitutes the highest-value target within the set. Access at this level introduces potential exposure to defense supply chains, partner ecosystems, and software distribution mechanisms. Compromise here is strategically significant, as it creates pathways for downstream supply chain operations, including the possibility of inserting malicious code into trusted update channels or leveraging interconnected partner networks.

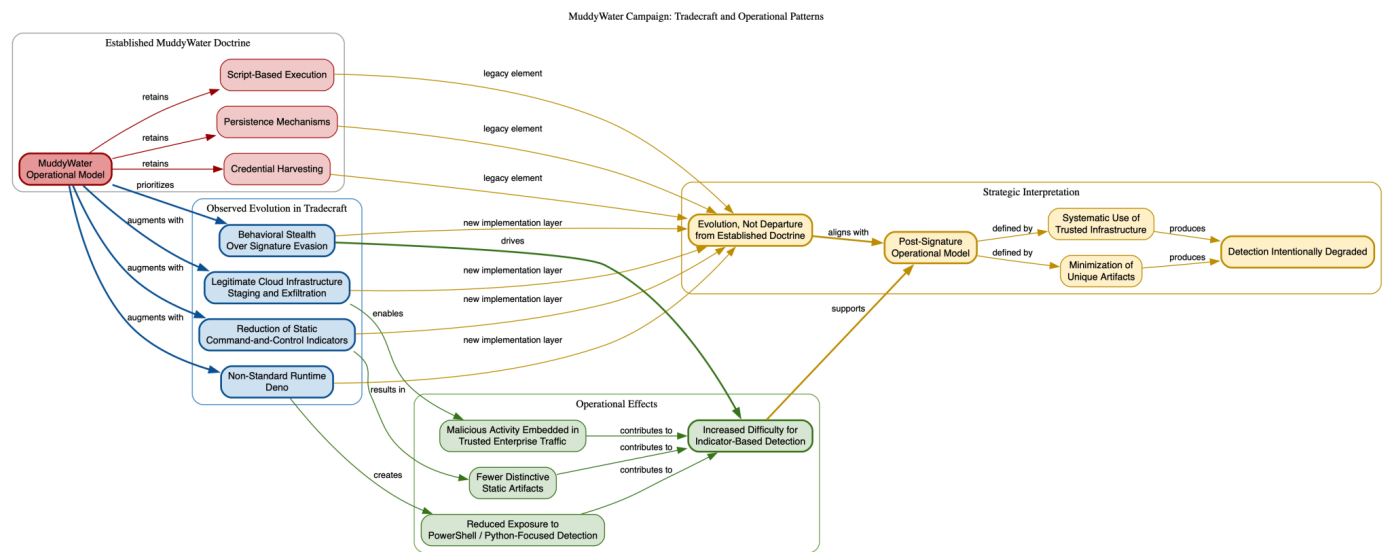
The Canadian non-profit organization, while less overtly critical, likely functions as a relational intelligence node. Organizations of this type often maintain extensive connections across policy, donor, and government-adjacent networks. Their comparatively weaker security postures, combined with high connectivity, make them effective entry points for intelligence collection and network mapping.

Taken collectively, these targets form a layered intelligence framework spanning finance, transportation, defense capability, and policy influence. This distribution is analytically consistent with a campaign designed to map, monitor, and potentially influence interconnected systems, rather than to exploit isolated organizations in isolation.

Tradecraft and Operational Patterns

The tradecraft exhibited in this campaign reflects a measured evolution in MuddyWater’s operational model rather than a break from its established doctrine. Core techniques script-based execution, persistence establishment, and credential harvesting remain foundational to the intrusion lifecycle. What has changed is the manner in which these techniques are implemented and concealed.

These traditional elements are now augmented by the adoption of less conventional execution environments, most notably the use of the Deno runtime. By shifting away from heavily monitored frameworks such as PowerShell and Python, the operators reduce exposure to detection logic that is optimized for those ecosystems. This introduces asymmetry into the defensive equation, forcing detection systems to account for less common execution patterns.



At the same time, the campaign demonstrates a deliberate reliance on legitimate cloud infrastructure for both staging and exfiltration. By embedding malicious workflows within widely used services, the operators are able to obscure activity within normal network traffic, effectively masking command-and-control and data movement within trusted channels.

A further defining characteristic is the reduction of static indicators typically associated with command-and-control infrastructure. Rather than relying on fixed domains or IP addresses, the operation minimizes persistent, easily attributable artifacts. This significantly complicates traditional indicator-based detection and response workflows.

Collectively, these adaptations indicate a shift toward behavioral stealth as the primary evasion strategy. Instead of focusing on signature evasion through obfuscation alone, MuddyWater is increasingly structuring operations to avoid generating distinctive signals altogether. This transition is consistent with a broader movement among advanced threat actors toward post-signature operational models, in which detection is systematically degraded through the minimization of unique artifacts and the extensive use of trusted, commoditized infrastructure.

Operational Intent Assessment

The tradecraft observed in this campaign reflects a clear evolution in MuddyWater's operational methodology, but not a fundamental break from its established doctrine. Core elements of the group's historical activity remain intact, including script-based execution, the establishment of persistence mechanisms, and the harvesting of credentials to facilitate lateral movement and sustained access. These familiar components, however, are now being augmented by a set of refinements designed to reduce detectability and increase operational resilience.

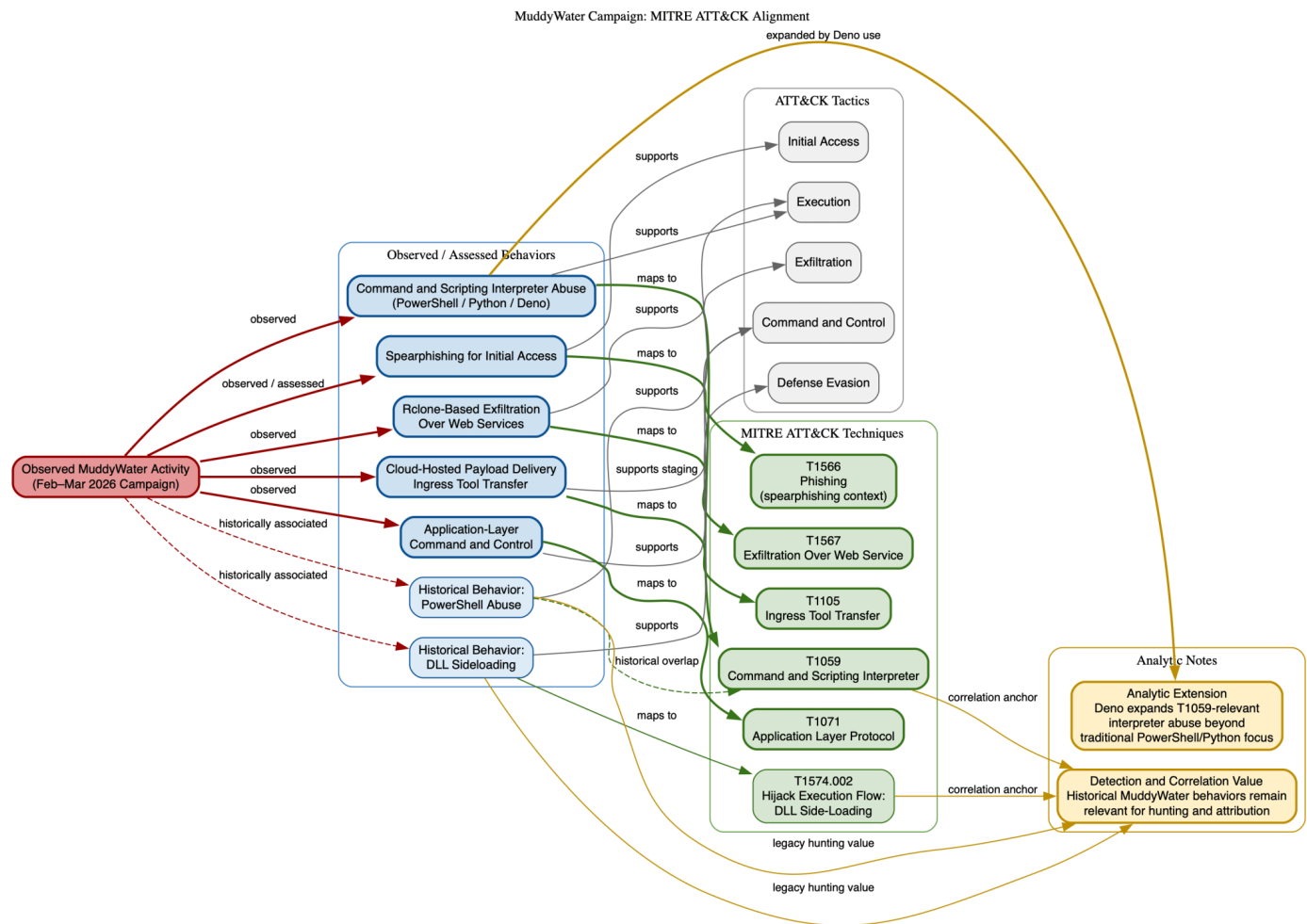
One of the most notable adaptations is the incorporation of non-standard execution environments, specifically the use of the Deno runtime. By operating outside the more commonly monitored ecosystems of PowerShell and Python, the actors reduce exposure to detection controls that are heavily tuned to those environments. This shift introduces variability into their execution layer, complicating both signature-based and behavioral detection.

In parallel, the campaign demonstrates a consistent reliance on legitimate cloud infrastructure for both staging and data exfiltration. Services such as commodity object storage platforms are leveraged in place of bespoke command-and-control systems, allowing malicious activity to blend with normal enterprise traffic. This approach reduces the need for dedicated infrastructure that might otherwise serve as a clear indicator of compromise.

Another defining characteristic is the deliberate reduction of static indicators. Traditional command-and-control artifacts, such as fixed domains or IP addresses, are either minimized or abstracted behind legitimate services. This forces defenders to rely less on indicator-based detection and more on identifying anomalous behavior within otherwise legitimate processes.

Taken together, these elements indicate a strategic shift toward behavioral stealth as the primary means of evasion. Rather than attempting to bypass detection through obfuscation alone, MuddyWater is increasingly structuring its operations to avoid generating distinctive signals in the first place. This aligns with a broader trend among advanced threat actors toward post-signature operational models, in which the effectiveness of detection is degraded through the deliberate minimization of unique artifacts and the systematic use of trusted infrastructure.

MITRE ATT&CK Alignment

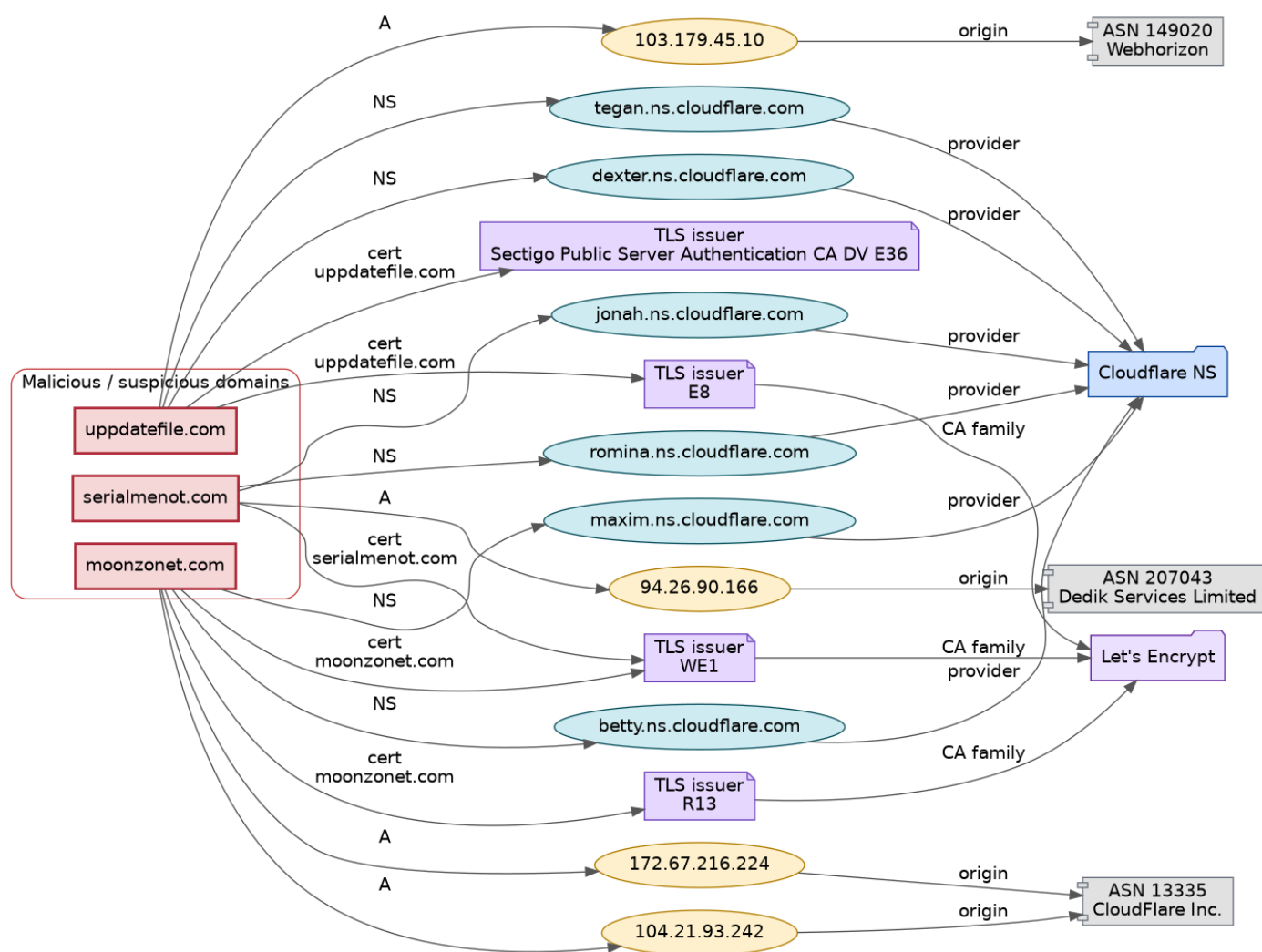


The observed activity maps to several established ATT&CK techniques, including spearphishing for initial access, command and scripting interpreter abuse (expanded to include Deno), ingress tool transfer via cloud-hosted payloads, exfiltration over web services using Rclone, and application-layer command-and-control mechanisms. Historical MuddyWater behaviors such as DLL sideloading and PowerShell abuse remain relevant for detection and correlation.

Domain Infrastructure Analysis

The IRIS dataset indicates a hybrid infrastructure model that combines trusted third-party services with a limited set of likely adversary-controlled domains. This structure is consistent with a low-signature operational approach designed to obscure malicious activity within legitimate traffic.

Legitimate infrastructure, including [deno.land](#), [dl.deno.land](#), and [deno.com](#), aligns with the use of the Deno runtime in Dindoor and supports script delivery and execution from highly trusted sources. The presence of [backblazeb2.com](#) further indicates reliance on commodity cloud storage for payload staging, reducing the need for dedicated attacker infrastructure.



In contrast, domains such as `updatefile.com` exhibit clear typo-squatting characteristics consistent with deceptive delivery mechanisms, while `moonzonet.com` reflects low-context naming typical of transient staging infrastructure. The repeated appearance of `serialmenot.com`, including tokenized request patterns, suggests use as a redirect or traffic distribution layer rather than a primary control node.

Hosting patterns reinforce this assessment. Use of commercial providers, Cloudflare fronting, and automated TLS issuance (e.g., Let's Encrypt) supports rapid deployment and rotation of infrastructure with minimal attribution risk.

Overall, the domain set reflects a distributed architecture that minimizes static indicators and blends malicious activity into legitimate service usage. This approach degrades the effectiveness of reputation-based detection and shifts the burden toward behavioral analysis and cross-layer correlation.

Detection and Defensive Implications

The campaign highlights the limitations of traditional IOC-based detection. Effective defense requires a shift toward behavioral and contextual monitoring, including:

- Detection of Deno runtime execution in non-development environments
- Monitoring for Rclone usage outside sanctioned backup workflows
- Identification of anomalous outbound traffic to cloud storage providers
- Detection of unusual Python execution patterns
- Analysis of code-signing certificate anomalies and reuse

Organizations should prioritize environment baselining and anomaly detection over reliance on static indicators.

Conclusion

The MuddyWater Dindoor/Fakeset campaign represents a mature, strategically aligned cyber espionage operation conducted during a period of geopolitical tension. It demonstrates a continued evolution toward low-observable, cloud-enabled tradecraft designed to evade traditional detection mechanisms and preserve long-term access within critical systems.

The deliberate selection of targets across financial, transportation, defense, and policy domains indicates a comprehensive approach to intelligence collection and pre-positioning within interconnected systems that underpin Western power structures.

Most significantly, the campaign illustrates a transition toward a post-IOC threat model, in which the absence of traditional indicators is not a limitation of analysis but a defining characteristic of the adversary's operational design.

In this context, MuddyWater should be assessed not as an opportunistic threat actor, but as a disciplined intelligence service operator executing a coordinated access strategy with latent escalation potential.

Indicators of Compromise (IOCs)

0f9cf1cf8d641562053ce533aaa413754db88e60404cab6bbaa11f2b2491d542 – Trojan.Dindoor

Any.Run: <https://app.any.run/tasks/7109f95d-0ded-486d-b960-7746ff43357c>

1d984d4b2b508b56a77c9a567fb7a50c858e672d56e8cf7677a1fca5c98c95d1 – Trojan.Dindoor

Any.Run: <https://app.any.run/tasks/18657ac8-35b1-46be-91b3-6d5b89e4c529>

2a00705cfd3c15cf8913e9eb4e23968efd06f1feceaef9987d26c5518887d043 – Trojan.Dindoor

Any.Run: <https://app.any.run/tasks/2aea5a2b-8896-491e-aa0c-a0775838a3cc>

2a09bbb3d1ddb729ea7591f197b5955453aa3769c6fb98a5ef60c6e4b7df23a5 – Trojan.Dindoor

Any.Run: <https://app.any.run/tasks/acba3305-d6db-4ce8-82c7-b64ce78a0f49>

[42a5db2a020155b2adb77c00cbe6c6ad27c2285d8c6114679d9d34137e870b3f](#) – Trojan.Dindoor

Any.Run: <https://app.any.run/tasks/cc068d45-0b6d-4341-be23-d0fded91d463>

[7467f326677a4a2c8576e71a832e297e794ea00e9b67c4fcbe78b5aec697cec4](#) – Trojan.Dindoor

Any.Run: <https://app.any.run/tasks/dd8354f2-121d-4ca6-9a21-342d98cd5e75>

[7c30c16e7a311dc0cdb1cdfd9ea6e502f44c027328dbe7d960b9bcd85ccf5eef](#) – Trojan.Dindoor

Any.Run: <https://app.any.run/tasks/635099a7-6185-4d91-b19f-5bd3eac7b569>

[b0af82de672d81f3c2f153977923b3884a8a9e7045b182c2379b19a1996931a0](#) – Trojan.Dindoor

Any.Run: <https://app.any.run/tasks/56bfa25e-751e-4806-a444-e2b8587a920f>

[bd8203ab88983bc081545ff325f39e9c5cd5eb6a99d04ae2a6cf862535c9829a](#) – Trojan.Dindoor

Any.Run: <https://app.any.run/tasks/e1833116-914e-435a-b2d3-a4252b627955>

[c7cf1575336e78946f4fe4b0e7416b6ebe6813a1a040c54fb6ad82e72673478e](#) – Trojan.Dindoor

Any.Run: <https://app.any.run/tasks/7b26bf81-9a0a-4302-b8f1-3bc70b1cc37c>

[077ab28d66abdafad9f5411e18d26e87fe43da1410ee8fe846bd721ab0cb52de](#) – Trojan.Fakeset

Any.Run: <https://app.any.run/tasks/01aeaa8d-1a52-43cd-9b85-c9d065c0f2cd>

[15061036c702ad92b56b35e42cf5dc334597e7311e98d2fdd3815a69ac3b1d84](#) – Trojan.Fakeset

[2b7d8a519f44d3105e9fde2770c75efb933994c658855dca7d48c8b4897f81e6](#) – Trojan.Fakeset

Any.Run: <https://app.any.run/tasks/c086fc3f-efff-4fe6-a681-009fc01d7611>

[4aef998e3b3f6ca21c78ed71732c9d2bdcc8a4e0284f51d7462c79d446fbc7be](#) – Trojan.Fakeset

Any.Run: <https://app.any.run/tasks/a5f599ba-1d6c-4c55-a03c-6d0de8dbed04>

[64263640a6fdeb2388bca2e9094a17065308cf8dcb0032454c0a71d9b78327eb](#) – Trojan.Fakeset

Any.Run: <https://app.any.run/tasks/c905f05a-3d53-499a-baba-f83bdcab0998>

[64cf334716f15da1db7981fad6c81a640d94aa1d65391ef879f4b7b6edf6e7f1](#) – Trojan.Fakeset

Any.Run: <https://app.any.run/tasks/639bc43a-75a6-4324-86ec-5d6a1db4c1b0>

[74db1f653da6de134bdc526412a517a30b6856de9c3e5d0c742cb5fe9959ad0d](#) – Trojan.Fakeset

Any.Run: <https://app.any.run/tasks/9212ebe8-43ce-4402-b34a-498db035730f>

[94f05495eb1b2ebe592481e01d3900615040aa02bd1807b705a50e45d7c53444](https://app.any.run/tasks/94f05495eb1b2ebe592481e01d3900615040aa02bd1807b705a50e45d7c53444) – Trojan.Fakeset

[a4bd1371fe644d7e6898045cc8e7b5e1562bdfd0e4871d46034e29a22dec6377](https://app.any.run/tasks/a4bd1371fe644d7e6898045cc8e7b5e1562bdfd0e4871d46034e29a22dec6377) – Trojan.Fakeset

Any.Run: <https://app.any.run/tasks/97d1959d-53bc-4eb6-911f-843835f45050>

[a5d4d6be3bfe0cba23fe6b44984b5fc9c7c7e10030be96120bb30da0f2545d4c](https://app.any.run/tasks/a5d4d6be3bfe0cba23fe6b44984b5fc9c7c7e10030be96120bb30da0f2545d4c) – Trojan.Fakeset

[ddceade244c636435f2444cd4c4d3dc161981f3af1f622c03442747ecef50888](https://app.any.run/tasks/ddceade244c636435f2444cd4c4d3dc161981f3af1f622c03442747ecef50888) – Trojan.Fakeset

Any.Run: <https://app.any.run/tasks/a1e3b0f4-dadf-4920-9359-618d90bf8579>

[24857fe82f454719cd18bcbe19b0cfa5387bee1022008b7f5f3a8be9f05e4d14](https://app.any.run/tasks/24857fe82f454719cd18bcbe19b0cfa5387bee1022008b7f5f3a8be9f05e4d14) – Trojan.Stagecomp

Any.Run: <https://app.any.run/tasks/9f7c5041-8c5d-46d3-be86-a62fbec6c7>

[A92d28f1d32e3a9ab7c3691f8bfca8f7586bb0666adbba47eab3e1a8faf7ecc0](https://app.any.run/tasks/A92d28f1d32e3a9ab7c3691f8bfca8f7586bb0666adbba47eab3e1a8faf7ecc0) – –
Trojan.Stagecomp

[3df9dcc45d2a3b1f639e40d47eceeafb229f6d9e7f0adcd8f1731af1563ffb90](https://app.any.run/tasks/3df9dcc45d2a3b1f639e40d47eceeafb229f6d9e7f0adcd8f1731af1563ffb90) – Trojan.Darkcomp

Any.Run: <https://app.any.run/tasks/c33bbc75-7a8f-4784-9e39-ab7c4e58b364>

[1319d474d19eb386841732c728acf0c5fe64aa135101c6ceee1bd0369ecf97b6](https://app.any.run/tasks/1319d474d19eb386841732c728acf0c5fe64aa135101c6ceee1bd0369ecf97b6) – Trojan.Darkcomp

Any.Run: <https://app.any.run/tasks/5deb96db-42cd-4a6e-a0b2-2f30bdfb33f5>

Network Indicators

- [gitempire.s3.us-east-005.backblazeb2\[.\]com](https://gitempire.s3.us-east-005.backblazeb2[.]com)
- [elvenforest.s3.us-east-005.backblazeb2\[.\]com](https://elvenforest.s3.us-east-005.backblazeb2[.]com)
- [updatefile\[.\]com](https://updatefile[.]com)
- [serialmenot\[.\]com](https://serialmenot[.]com)
- [moonzonet\[.\]com](https://moonzonet[.]com)
- dl.deno.land
- deno.com
- deno.land

Rate this:

1 Votes

Written by Krypt3ia

2026/03/20 at 14:58

Posted in [APT](#), [Iran](#), [MOIS](#), [Threat Intelligence](#), [Uncategorized](#)

« [Intelligence Assessment Report: Iranian Cyber Warfare Capability Degradation Amid the 2026 Conflict](#)

One Response

Subscribe to comments with [RSS](#).

1. [...] Date: March 2026By: Krypt3ia Executive Summary In early February 2026, the Iranian state-aligned cyber espionage group MuddyWater (also tracked as Seedworm, MERCURY, Static Kitten, and Mango Sandstorm) conducted a coordinated intrusion campaign targeting a small but strategically significant set of organizations across the United States, Israel, and Canada. The campaign, publicly disclosed in early March 2026, leveraged twoKrypt3iaRead More [...]

[Threat Intelligence Report: MANGO SANDSTORM Indoor / Fakeset Activity – Yet Another News Aggregator Channel](#)

2026/03/20 at

Leave a comment

This site uses Akismet to reduce spam. [Learn how your comment data is processed.](#)