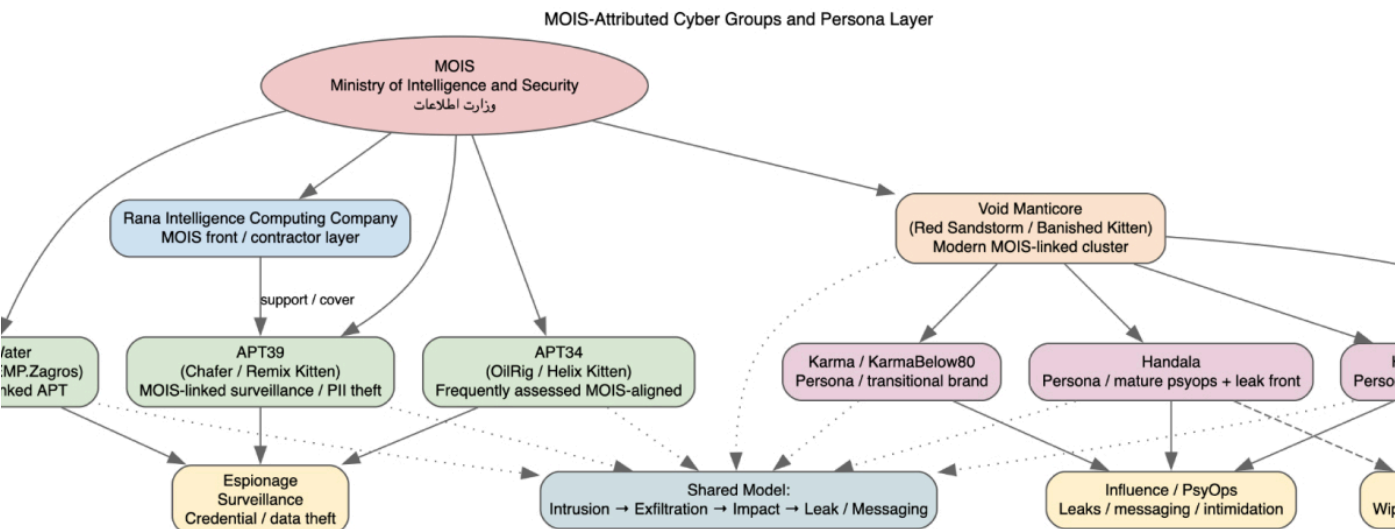


MOIS Linked MOIST GRASSHOPPER / Homeland Justice / KarmaBelow80 / Handala Hackers / Campaigns and Evolution



Executive Overview

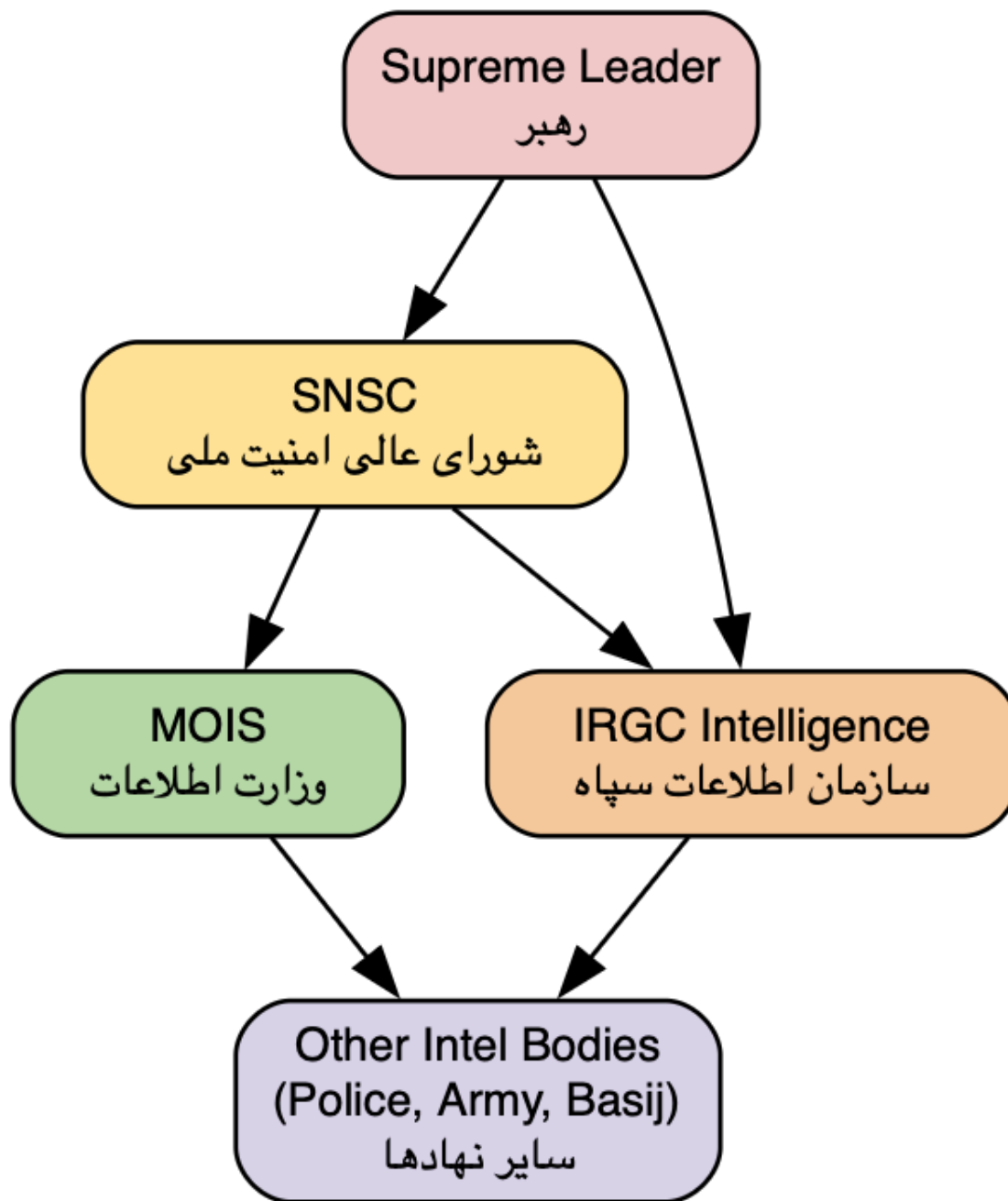
The evidence examined across this analysis spanning U.S. government reporting, private-sector threat intelligence research, passive DNS and infrastructure enrichment, and longitudinal review of archived web and Telegram content supports a high-confidence assessment that the personas *Homeland Justice*, *Karma*, and *Handala* do not represent discrete or ideologically independent hacktivist groups. Rather, they constitute a coordinated, [MOIS-aligned cyber influence ecosystem](#) operating under multiple branded identities that serve distinct but complementary operational roles.

This assessment is supported by multiple converging lines of evidence, including clear temporal continuity, operational consistency, infrastructure linkage, and behavioral alignment. Activity transitions seamlessly from Homeland Justice operations targeting Albania in 2022 to Karma campaigns against Israeli entities in late 2023, and subsequently to Handala-branded operations from 2024 onward. Across these phases, the actors consistently employ a repeatable pattern of intrusion, data exfiltration, disruptive or destructive action, and rapid public disclosure through controlled infrastructure. This is reinforced by shared or cross-referenced domains, persistent use of Telegram for amplification and coordination, and common hosting and obfuscation strategies. The personas also exhibit consistent rhetorical framing, target selection logic, and methods of psychological coercion. Taken together, these indicators support the conclusion that these identities function as operational layers applied to a single underlying capability,

enabling segmentation of audiences and messaging while maintaining continuity of tradecraft. This modular branding approach aligns with broader state-aligned cyber operations that leverage multiple personas to project decentralization while masking centralized control.

Since its emergence in 2022, the campaign has evolved from a destructive intrusion operation into a multi-functional cyber influence framework. The initial Albania operation combined long-term compromise with ransomware-style encryption, disk wiping, and public attribution, already indicating that technical disruption was paired with narrative objectives. Over time, the campaign expanded to incorporate espionage, persistent access, structured data exfiltration, and coordinated hack-and-leak activity designed to shape perception and behavior. The addition of surveillance capabilities, particularly those leveraging Telegram-based command-and-control, marks a further shift toward continuous monitoring and transnational repression targeting both institutions and individuals. In its current form, the campaign represents a cohesive and adaptive system in which intrusion, disruption, surveillance, and information operations are integrated into a unified strategy aligned with MOIS objectives, capable of applying sustained pressure across both cyber and cognitive domains.

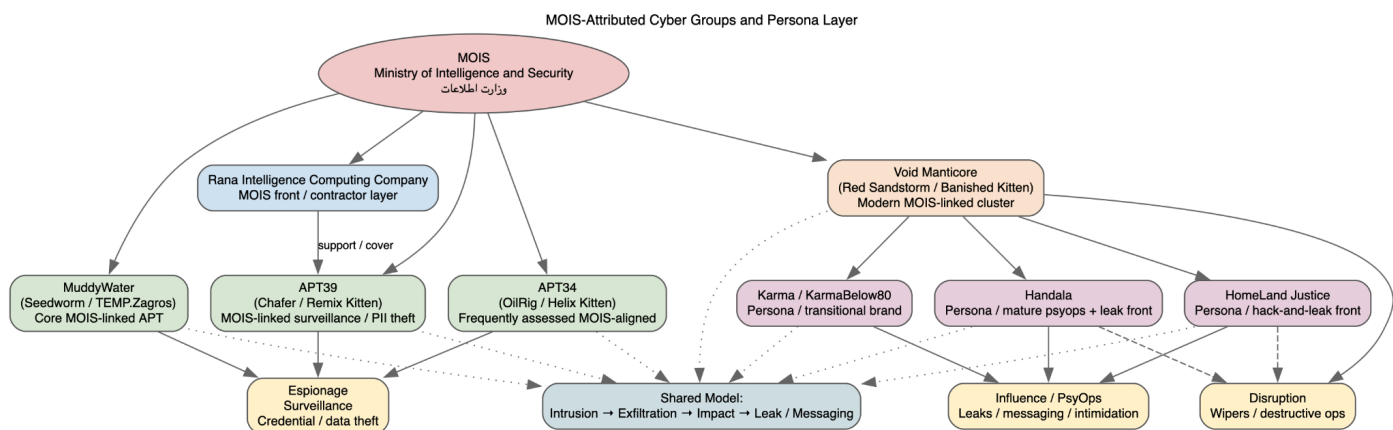
Ministry of Intelligence and Security (MOIS) Connection



The operational ecosystem encompassing Handala, Homeland Justice, and the persona cluster associated with Karma and [KarmaBelow80](#) is most coherently understood not as a loose federation of ideologically aligned actors, but as a structured, state-directed campaign operating under the authority of Iran's Ministry of Intelligence and Security (MOIS). When viewed through the lens of command-and-control, tradecraft consistency, and synchronized effects, the activity attributed to these brands reflects the hallmarks of an intelligence service executing coordinated cyber operations in support of national objectives rather than independent or purely proxy-driven behavior.

At the center of this structure is the reported involvement of [Seyed Yahya Hosseini Panjaki](#), an individual assessed to be affiliated with MOIS and linked to its internal security and counter-terrorism apparatus. The significance of this attribution lies less in the identity of the individual operator and more in what it implies structurally. His role represents a command-level function within an institutional hierarchy, indicating that these cyber operations are subject to formal tasking, oversight, and strategic alignment. This shifts the analytical framing away from contractor-driven or semi-deniable activity and toward a model in which operations are integrated into the broader intelligence mandate of the Iranian state.

Within this framework, the distinct public-facing identities of Handala, Homeland Justice, and KarmaBelow80 function as operational veneers rather than discrete entities. Each brand aligns with a specific subset of MOIS objectives while drawing from a shared pool of capabilities, infrastructure, and tradecraft. Handala's activity is most closely aligned with psychological and information operations, characterized by curated leaks, narrative shaping, and the deliberate amplification of politically resonant material. The timing and framing of these disclosures indicate coordination with broader messaging goals, suggesting that the technical intrusion component is only one phase of a larger influence cycle.



Homeland Justice, by contrast, represents the disruptive and punitive arm of this ecosystem. Its operations, particularly those conducted against Albanian government infrastructure, demonstrate a full-spectrum intrusion lifecycle in which long-term access is leveraged to enable data exfiltration, destructive deployment, and overt attribution. The combination of wiper activity, ransomware-style encryption, and coordinated public messaging reflects a model of calibrated escalation designed to impose both operational and reputational costs on the target. This is consistent with MOIS mandates involving internal security and retaliatory action against perceived adversaries.

The Karma and KarmaBelow80 personas introduce an additional layer of flexibility into the ecosystem. Rather than being tied to a single operational profile, these identities appear to function as adaptive interfaces that can be deployed across different phases of an operation. They enable the same underlying capability set to be presented under different contextual narratives, enhancing deniability while maintaining continuity of effect. This is particularly relevant in environments where attribution pressure is high, as it allows operators to fragment their public footprint without fragmenting their operational infrastructure.

The coherence across these actor clusters is most evident in the structure of their operations. Intrusions frequently follow a repeatable progression: *initial access is established through credential compromise or exploitation of exposed services, followed by the deployment of webshells or other persistence*

mechanisms. Once footholds are secured, actors conduct internal reconnaissance and lateral movement using enterprise-scale tooling, enabling them to map the target environment and identify high-value data stores. Exfiltration is then carried out in a controlled manner, often staged to support subsequent public release. The final phase varies depending on strategic intent, ranging from silent intelligence collection to destructive action or coordinated leak publication.

What distinguishes this ecosystem is the degree to which these phases are integrated and interchangeable. The same intrusion can evolve from a covert surveillance operation into a disruptive attack or an influence campaign without requiring a fundamental shift in tooling or access. This reflects the modular architecture described earlier, but at an organizational level it also implies centralized capability management. MOIS oversight provides the mechanism through which these modules can be allocated, combined, and sequenced in accordance with mission objectives.

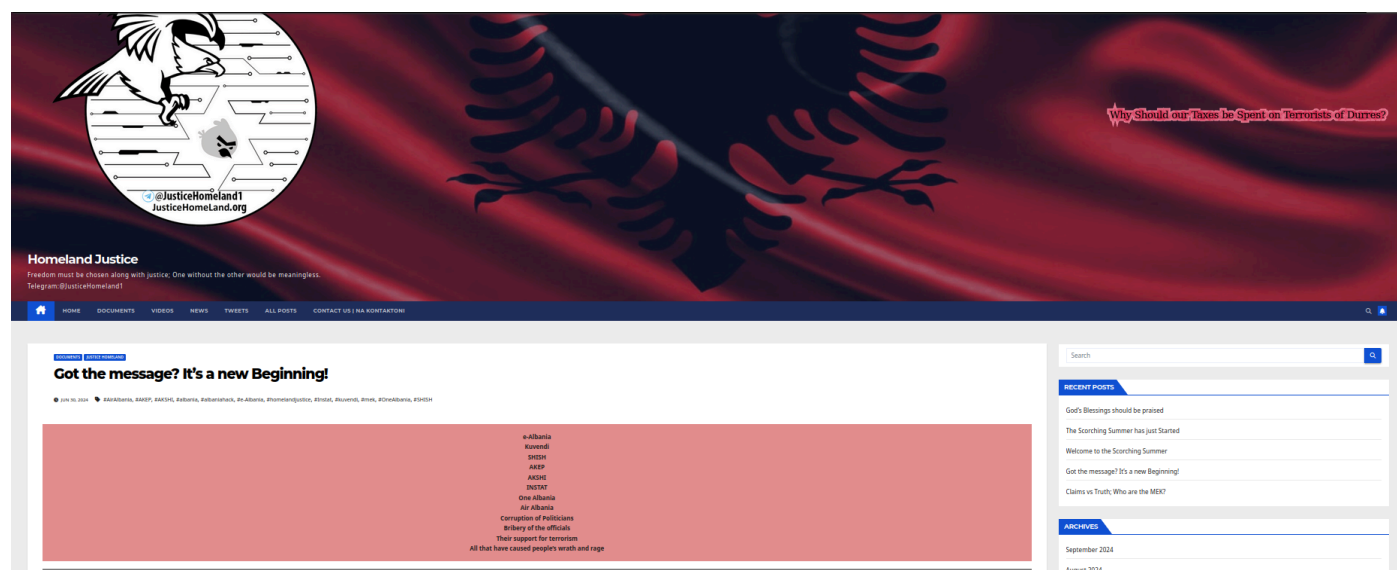
The involvement of a command-level figure such as Panjaki provides a unifying explanation for this consistency. It accounts for the alignment between technical operations and information effects, the disciplined escalation observed in target engagements, and the reuse of infrastructure and tooling across ostensibly separate actor brands. It also explains the resilience of the ecosystem. Disrupting one public-facing identity or infrastructure cluster does not degrade the underlying capability, because those assets are components of a larger, centrally managed system.

From an analytical standpoint, this structure necessitates treating Handala, Homeland Justice, and KarmaBelow80 as manifestations of a single operational apparatus rather than independent threat actors. Their differences are functional rather than organizational, reflecting the segmentation of roles within a coordinated campaign. The strategic value of this model lies in its flexibility: MOIS can conduct espionage, disruption, and influence operations in parallel, or transition between them as conditions dictate, all while maintaining a coherent operational footprint.

This convergence of command authority, modular capability, and multi-domain execution underscores the maturation of MOIS cyber operations into a fully integrated instrument of state power. It is not simply the presence of advanced tooling or destructive capability that defines this ecosystem, but the way in which those capabilities are orchestrated under centralized direction to produce layered, cumulative effects across technical and informational domains.

Campaign Expansion and Evolution

Initial Emergence in Albania (2022)



Homeland Justice[.]org website

The campaign first became publicly visible during the 2022 attacks against the Government of Albania, which established both its technical baseline and its enduring operational model. Iranian state actors operating under the Homeland Justice persona achieved initial access approximately fourteen months prior to public disclosure by exploiting an internet-facing Microsoft SharePoint vulnerability. This early foothold indicates a deliberate pre-positioning phase, consistent with long-dwell intrusion strategies observed across MOIS-aligned operations.

Following initial compromise, the actors transitioned into a structured post-exploitation workflow designed to ensure persistence, expand access, and map the target environment. Webshells were deployed on compromised servers, providing durable and low-friction access while enabling command execution without reliance on large malware payloads. From this foothold, operators conducted systematic internal reconnaissance, enumerating network topology, identifying key systems, and mapping trust relationships across the enterprise.

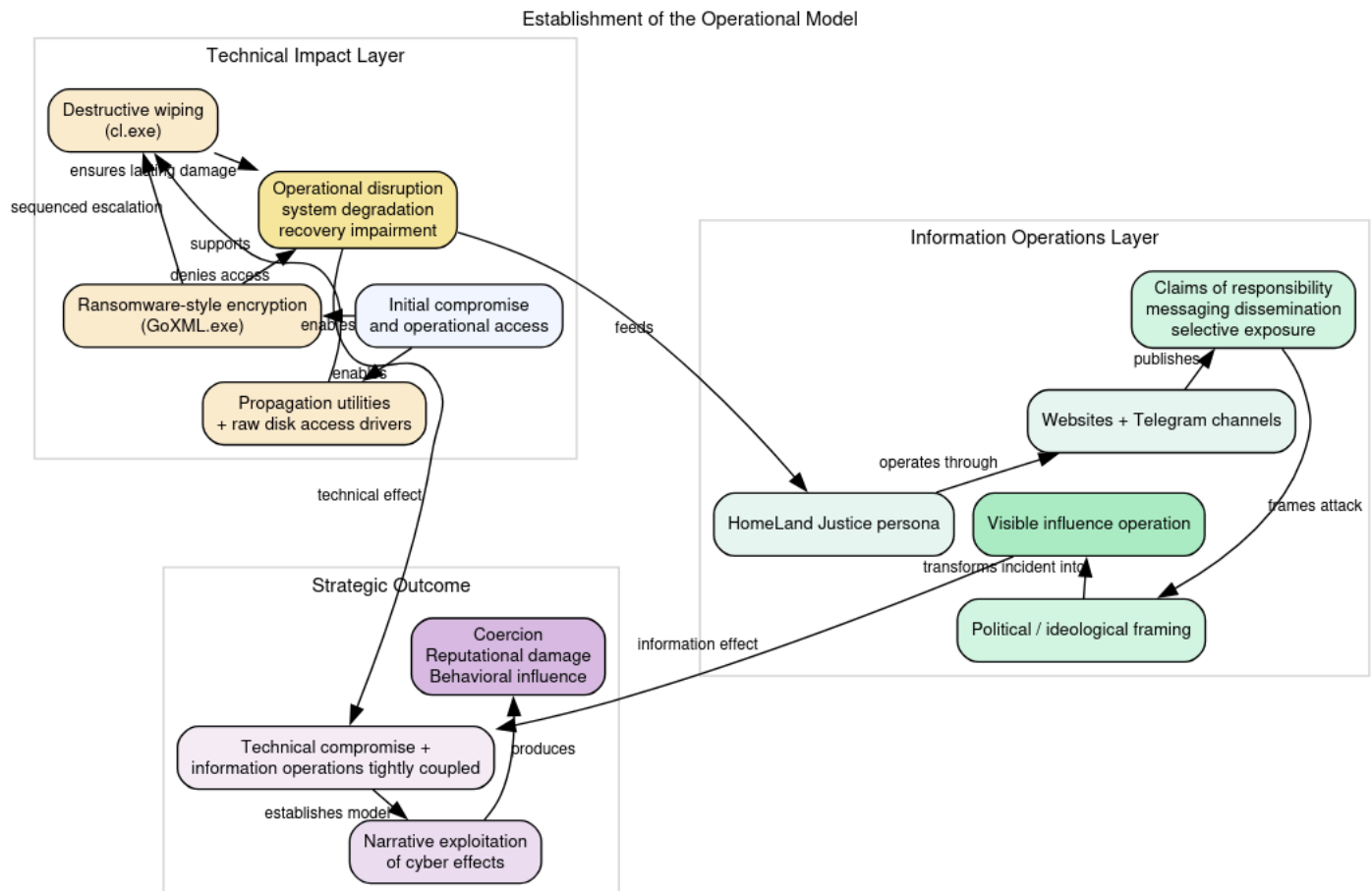
Credential harvesting was a central component of this phase. Through a combination of mailbox access, credential dumping, and account manipulation, the actors obtained privileged credentials that enabled lateral movement and escalation. Movement across the environment was conducted using standard administrative protocols, including Remote Desktop Protocol (RDP), Server Message Block (SMB), and File Transfer Protocol (FTP), allowing activity to blend with legitimate administrative traffic and reducing the likelihood of early detection.

The compromise of Microsoft Exchange infrastructure further expanded access. By leveraging Exchange, the actors were able to access and manipulate mailboxes, create or modify accounts, and extract large volumes of sensitive communications. This email corpus provided both intelligence value and material for later disclosure, aligning with the campaign's hack-and-leak model.

Data exfiltration occurred in parallel with lateral expansion, with operators systematically staging and extracting large datasets from across the environment. Only after sufficient access, intelligence collection, and data acquisition had been achieved did the actors transition to the destructive phase. This sequencing – extended pre-positioning, comprehensive collection, and delayed disruption – demonstrates a disciplined operational approach in which technical compromise is leveraged to maximize both intelligence yield and downstream psychological impact.

Establishment of the Operational Model

The impact phase of the Albania operation combined ransomware-style encryption with destructive wiping, employing tools such as [GoXML.exe](#) and [cl.exe](#), supported by propagation utilities and raw disk access drivers that enabled direct manipulation of underlying storage. These capabilities were deployed in a coordinated manner to maximize operational disruption, impair system recovery, and degrade institutional functionality. The sequencing of encryption followed by wiping reflects a deliberate approach designed not only to deny access to systems and data, but to ensure lasting damage and complicate remediation efforts.

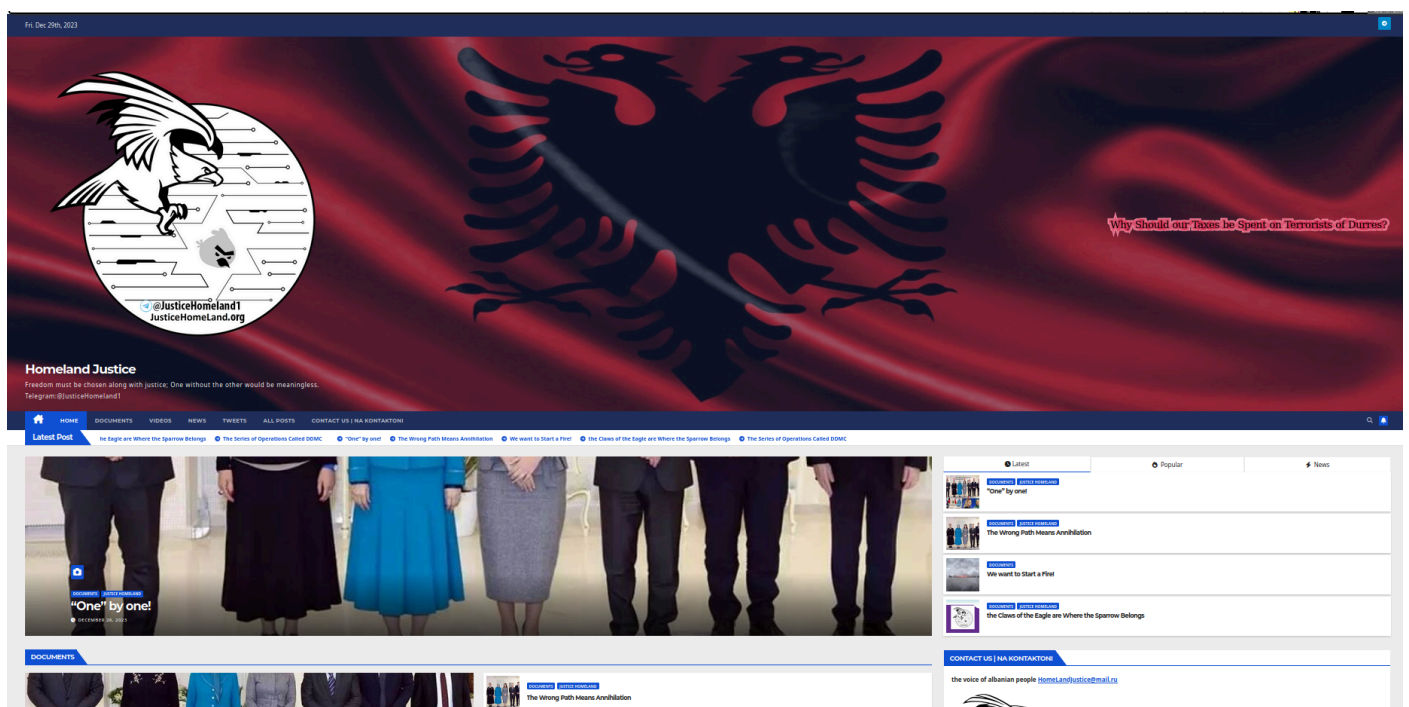


More significant than the tooling itself, however, was the deliberate integration of public-facing infrastructure into the attack lifecycle. The [Homeland Justice](#) persona was used to claim responsibility, disseminate messaging, and frame the operation within a broader political and ideological narrative. Websites and Telegram channels functioned as controlled dissemination platforms through which the

actors published statements, amplified claims, and selectively exposed information. This layer transformed what would otherwise have been a destructive cyber incident into a visible and ongoing influence operation.

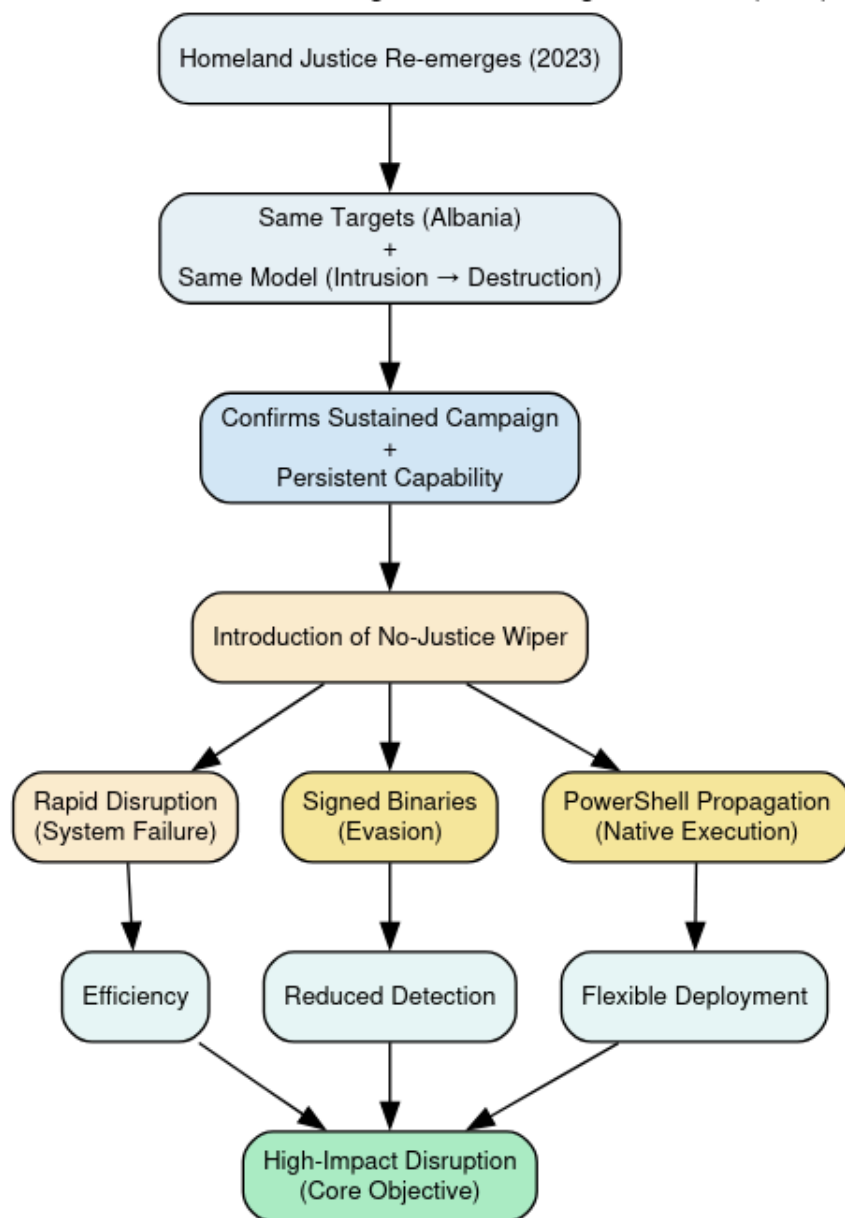
This approach established a foundational operational model in which technical compromise and information operations were inseparably linked. Cyber intrusion and destruction served as enabling mechanisms for narrative exploitation, with the ultimate objective extending beyond disruption to include coercion, reputational damage, and behavioral influence. In this model, the value of the operation was realized not solely through the technical impact, but through the controlled release of information and the shaping of perception in the aftermath of the attack.

Continued Activity and Tooling Refinement (2023)



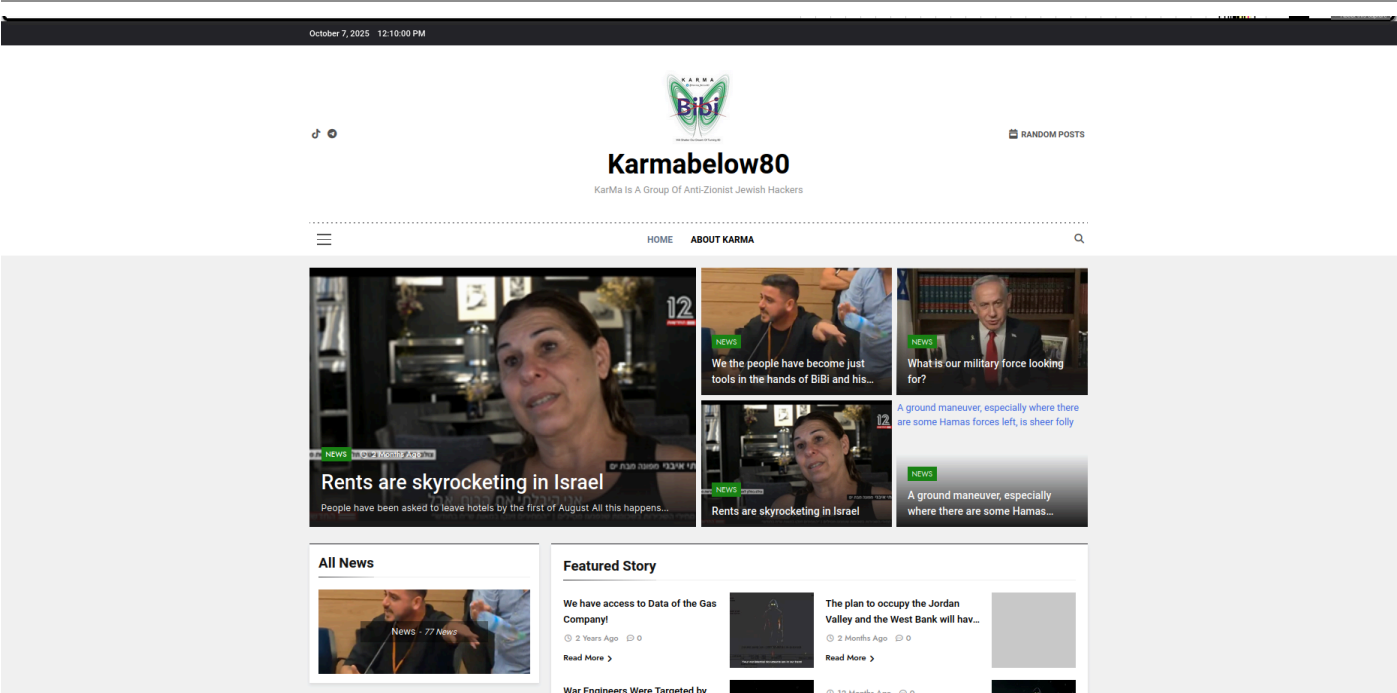
In late 2023, the Homeland Justice campaign re-emerged with renewed activity targeting Albanian entities, demonstrating clear continuity in both target selection and operational methodology. This phase reinforced that the earlier Albania operations were not isolated incidents, but part of a sustained and adaptive campaign. The actors maintained their focus on politically relevant targets while reapplying the same core model of intrusion followed by destructive impact, indicating both persistence of intent and retention of operational access or capability.

Homeland Justice Re-Emergence and Tooling Refinement (2023)



During this period, the introduction of the [No-Justice Wiper](#) marked a refinement in destructive tooling. Designed for rapid and irreversible disruption, the malware emphasized system incapacitation, including preventing successful operating system boot. The use of signed binaries suggests an increased emphasis on evasion and trust abuse, while PowerShell-based propagation reflects a growing reliance on native system capabilities to enable flexible and low-friction deployment. Together, these developments indicate an evolution toward more efficient, harder-to-detect operations while preserving the campaign's core objective of high-impact disruption.

Geographic Expansion and Rebranding: Karma Phase (2023-2024)



Following the Israel-Hamas conflict in October 2023, the campaign expanded geographically and adopted the Karma persona.

Despite this rebranding, the underlying tradecraft remained consistent. Operations targeted Israeli organizations and employed a hybrid approach combining custom tooling with publicly available utilities, including bespoke webshells, credential validation tools, reverse SSH tunneling, and destructive mechanisms such as [BiBi Wiper](#).

Actors increasingly relied on hands-on-keyboard techniques, including manual file deletion and disk formatting, prioritizing speed and operational impact. Evidence from this phase suggests a division of labor between intrusion and destructive operators, indicating a modular and coordinated ecosystem.

HANDALA HACK TEAM

Kash Patel current director of the FBI Hacked

2026-03-27 Uncategorized

Today, once again, the world witnessed the collapse of America's so-called security legends. While the FBI proudly seized our domains and immediately announced a \$10 million reward for the heads of Handala Hack members, we decided to respond to this ridiculous show in a way that will be remembered forever. Kash Patel, the current head...

HANDALA NEW TELEGRAM

2026-03-27 Uncategorized

JOIN AND WAIT FOR FBI: https://t.me/HANDALA_INTEL https://t.me/HANDALA_INTEL https://t.me/HANDALA_INTEL

Lockheed Martin Employees Given 48 Hours to Respond: A Tight Deadline Looms

2026-03-26 Uncategorized

Lockheed Martin Employees Given 48 Hours to Respond: A Tight Deadline

Handala-hack.tw 2026

The expansion of the Handala infrastructure set with the inclusion of `handala-hack[.]ps` and, more importantly, `handala-hack[.]tw`, provides a clearer view into how the actor operationalizes its domain layer over time. These domains are not isolated artifacts. They are part of a repeatable system in which naming conventions, narrative timing, and platform coordination matter more than persistence of any single asset. The repeated appearance of the *handala-hack* string across multiple TLDs indicates that the domain itself is not intended to endure. It is intended to be recognized, replaced, and reactivated, carrying forward an identity that survives takedown actions and jurisdictional pressure.

Kash Patel current director of the FBI Hacked

2026-03-27

Today, once again, the world witnessed the collapse of America's so-called security legends. While the FBI proudly seized our domains and immediately announced a \$10 million reward for the heads of Handala Hack members, we decided to respond to this ridiculous show in a way that will be remembered forever.

Kash Patel, the current head of the FBI, who once saw his name displayed with pride on the agency's headquarters, will now find his name among the list of successfully hacked victims. The so-called "impenetrable" systems of the FBI were brought to their knees within hours by our team. All personal and confidential information of Kash Patel, including emails, conversations, documents, and even classified files, is now available for public download.

This is the security that the U.S. government boasts about?! This is the cyber giant that thinks threats and bribes can silence the voice of resistance?! To the whole world, we declare: the FBI is just a name, and behind this name, there is no real security. If your director can be compromised this easily, what do you expect from your lower-level employees?

Dedicated to the martyrs of the Dena destroyer.

This is just our beginning...

[Download PoC](#)

Pass: handala

The .tw variant is particularly instructive when placed in historical context. Earlier iterations of the ecosystem relied heavily on .to infrastructure, which has long been associated with abuse-tolerant hosting and low-friction registration. The shift into .ps and .tw reflects both symbolic and operational adaptation. The .ps domain carries clear political signaling aligned with the actor's ideological framing, reinforcing the Palestinian narrative embedded throughout the campaign. By contrast, handala-hack[.]tw appears to serve a different function: jurisdictional dispersion and operational redundancy. Taiwan's namespace does not inherently carry the same ideological weight, which suggests its use is pragmatic rather than symbolic. In effect, the actor is separating message-layer signaling (.ps) from resilience-layer infrastructure (.tw).

When mapped against the historical leak cadence observed across the full archive, these domains align with distinct phases of campaign activity. Early in the lifecycle, Handala has relied on single-domain publication points tied to specific claim sets. These initial leaks focused on individual targets, often

framed as penetrations of named Israeli intelligence or defense figures. The content emphasized access mailboxes, communications, and internal correspondence without attempting to demonstrate systemic reach. Domains in this phase acted as announcement boards, each tied to a discrete narrative event.

As the campaign matured, the scale of claims expanded. The archive shows repeated assertions of large-volume email exfiltration, often in the range of tens of thousands to over one hundred thousand messages. These claims were accompanied by broader institutional framing, suggesting not just individual compromise but organizational penetration. It is in this phase that domain rotation becomes more pronounced. Rather than maintaining a single persistent site, the actor begins to distribute content across multiple similarly branded domains, each capable of hosting or referencing new disclosures. The emergence of domains like handala-hack[.]to and handala-redwanted[.]to reflect this shift toward functionally differentiated nodes, one for breach claims, another for intimidation or doxxing.

The introduction of handala-hack[.]tw appears to correspond with the later stages of this evolution, where the campaign moves beyond exposure into strategic signaling and maximalist claims. Posts associated with this period increasingly reference infrastructure targeting, large-scale destructive capability, and systemic access. Claims such as multi-petabyte data wipes or pre-mapped critical infrastructure targets emerge alongside continued email leak narratives. The domain layer, in this context, becomes less about hosting data and more about anchoring the claim itself. The presence of a new domain signals a new phase of activity, regardless of whether the underlying data is verifiable.


HANDALA HACK
 2.7K subscribers

Q Search

March 27


HANDALA HACK
 Hello FBI
 @HANDALA_INTEL
 48 20 16 8 7 4 3
 4.55K edited 07:22


HANDALA HACK



Hello, Kash Patel, the current Director of the FBI
 @HANDALA_INTEL
 55 51 17 7 5 5 5


HANDALA HACK
 @HANDALA_INTEL
 2.7K 1 1 2
 Subscribers Photo Video Links
www.handala-team.to
 DOWNLOAD TELEGRAM
 About Blog Apps Platform

Historically, each wave of leaks follows a recognizable pattern. A new or resurfaced domain appears, often with the familiar *handala-hack* naming structure. Within a short time window, posts are published asserting compromise of a high-value target. These posts are then amplified through Telegram channels now including identifiers such as @HANDALA_INTEL and further propagated via X accounts. The domain serves as the canonical reference point, but the operational impact is generated through distribution. Even when domains are seized or taken offline, the narrative persists because it has already been exported to other channels.

The content associated with these domains consistently emphasizes three categories of disclosure. The first is email data, which remains the dominant theme across the archive. Whether targeting individuals like Eran Ortal or broader institutional mailboxes, the actor repeatedly frames access to communications as evidence of deep penetration. The second category is identity and contact data, including phone numbers and membership lists, often used in campaigns against dissidents or civilian networks. The third is strategic or infrastructural intelligence, where the actor claims to possess detailed knowledge of critical systems such as water and electricity networks. Each category serves a distinct psychological function: exposure, intimidation, and deterrence.

HANDALA HACK TEAM

Stryker Hit by Unprecedented 12-Petabyte Data Wipe

2026-03-16

Today, for the first time, we proudly release the documentation of a unique cyber operation, an operation that will etch the name Handala Hack into the minds of all players in the global cybersecurity arena.

In a swift and calculated attack, we succeeded in penetrating the deepest layers of the network belonging to the medical technology giant, Stryker. No system was safe from our sharp and capable eyes. During this operation, over 200,000 critical systems of this company were targeted and 12 petabytes of data (equivalent to 12,000 terabytes) were permanently wiped. Such a scale of data destruction is unprecedented to this day.

Data that took years to collect and billions of dollars to protect was erased in just a few hours. Stryker and all its allies are now faced with a harsh reality: no defensive wall can stand against our will. Our power can cripple the enemy's vital infrastructure at any moment and bring them to their knees.

To demonstrate our strength and authority, images documenting this operation have now been released and are available to the public. This is only the beginning; those who think they are safe had better be prepared. Our voice will be heard not only by Stryker, but by all those who walk the path of oppression and aggression.

We have come to change the equations.

We have shown that no power is greater than the will of the people.

The inclusion of corporate targets, such as Stryker Corporation, marks another important shift visible in the historical record. Earlier phases of the campaign were tightly focused on Israeli state and intelligence entities. Later phases expand outward, incorporating Western corporate actors to demonstrate global

reach. The claims associated with these targets are often the most extreme, including assertions of large-scale data destruction. Whether or not these claims are technically accurate is secondary to their narrative role. They signal that the actor's reach is not confined to a single geography or sector.

Across all these phases, the domain layer including handala-hack[.]tw remains structurally consistent. The sites themselves are simple, often WordPress-based, with minimal technical sophistication. They do not host malware, nor do they expose command-and-control infrastructure. Instead, they function as narrative anchors, providing a stable URL that can be cited, shared, and referenced across platforms. The real operational activity occurs elsewhere, in the intrusion layer (which remains opaque) and the amplification layer (Telegram and X). The domain is simply the point where those layers intersect publicly.

What emerges from the full dataset, now augmented by the newly observed domains, is a clear pattern: Handala's infrastructure is designed to be expendable, but its identity is designed to persist. Domains are created, used, and abandoned. Telegram channels are taken down and reconstituted. Yet the naming conventions *handala-hack*, *HANDALA_* and the narrative structure remain constant. This allows the actor to survive disruption without losing coherence. Each new domain, including handala-hack[.]tw, is not a fresh start but a continuation of an ongoing campaign.

In historical context, the leaks themselves should be understood not as isolated incidents but as components of a sustained psychological operation. Early disclosures establish credibility, mid-phase leaks expand perceived capability, and later claims introduce strategic and deterrent messaging. The domain infrastructure evolves in parallel, moving from single-use publication points to a distributed, rotating set of narrative nodes. The result is a system in which the appearance of a new domain is itself a signal, an indication that the next cycle of claims, amplification, and psychological effect is underway.

Ultimately, the addition of handala-hack[.]tw does not represent a new capability. It represents the continued refinement of an existing model. The actor does not depend on any specific domain to achieve its objectives. Instead, it relies on the predictable regeneration of infrastructure combined with consistent narrative execution. In that sense, the domain is not the asset. The campaign is.

Adverse Effects and Real-World Impact of Handala Leak Operations

Analysis of the Handala archive, corroborated with external reporting, demonstrates a consistent divergence between claimed impact and verified operational consequences. While the group presents its activities as large-scale, destructive cyber intrusions, the observable real-world effects fall into a narrower set of categories: operational disruption (rare), exposure and reputational damage (common), and psychological or coercive effects (systematic).

The most clearly substantiated case of material operational impact is the attack against Stryker Corporation. Reporting indicates that the intrusion disrupted core business functions, including order processing, manufacturing, and shipment operations, with recovery extending over multiple days. The incident also reportedly resulted in the remote wiping of tens of thousands of devices, affecting employees across multiple regions and, in some cases, impacting personally owned devices enrolled in enterprise systems. This represents a genuine destructive and operational cyber event, distinguishing it

from the majority of Handala's activity. The scale and severity of this incident further triggered a law enforcement response, including domain seizures targeting Handala infrastructure, indicating that the event crossed the threshold from influence activity into infrastructure-level concern.

A second category of confirmed impact involves high-profile personal data exposure, exemplified by the breach of Kash Patel. In this case, the publication of personal emails, images, and documents created reputational harm and potential counterintelligence risk, even though the exposed material was not assessed as containing sensitive government information. The significance of this event lies less in technical compromise and more in its function as a public humiliation and signaling operation, consistent with Handala's broader objectives of intimidation and reputational pressure against Western officials.

Other reported incidents fall into a more ambiguous category. The claimed attack against Hebrew University of Jerusalem, involving tens of terabytes of wiped and exfiltrated data, represents a credible, but not fully independently verified, destructive event. While multiple secondary sources describe the incident, there is limited primary confirmation of the full scale of impact. This pattern — where claims are partially supported but not conclusively validated — is characteristic of the Handala ecosystem and complicates direct attribution of operational consequences.

In contrast, some claims appear to have produced primarily reputational or narrative effects without technical confirmation. The alleged compromise of Verifone, for example, was publicly denied by the company, with no evidence of disruption or data loss. In such cases, the adverse effect is not system compromise but forced defensive communication, in which the targeted organization must respond to public allegations, thereby amplifying the narrative regardless of its validity.

A substantial portion of the archive consists of operations targeting individuals within the Israeli intelligence and security ecosystem, including Sima Shine, Ilan Steiner, Deborah Oppenheimer, and Eran Ortal. In these cases, the adverse effects are consistently limited to exposure of alleged communications, reputational damage, and intelligence-related pressure. Although large-scale email leaks are claimed, there is no strong independent evidence of downstream operational disruption, institutional failure, or policy impact. These incidents function primarily as hack-and-leak influence operations, designed to erode trust and project vulnerability rather than to degrade capability.

The campaign also includes a distinct category of identity exposure and intimidation, illustrated by the targeting of VahidOnline. The leak of tens of thousands of user identities and phone numbers associated with dissident networks constitutes a form of digital repression, exposing individuals to harassment, surveillance, or potential physical risk. Unlike corporate or institutional targets, the impact here is distributed across a population, amplifying fear and discouraging participation in opposition or media activities.

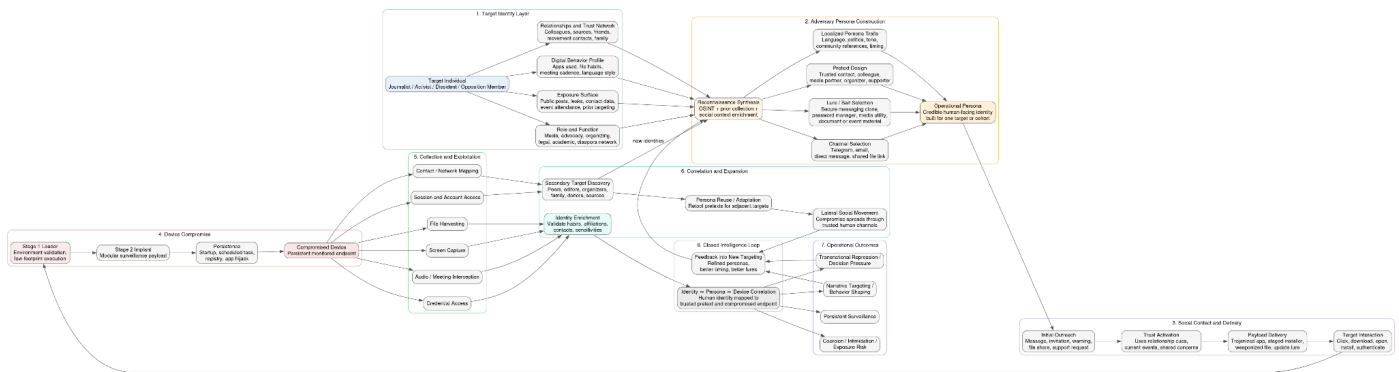
Beyond digital exposure, the archive and supporting reporting indicate a pattern of coercive escalation into the physical domain. Handala has been linked to doxxing campaigns against individuals such as defense-sector employees, including alleged exposure of personal details of engineers associated with defense contractors. These actions are often accompanied by explicit threats, transforming cyber activity into psychological coercion with potential real-world implications. Even when the accuracy of the leaked data is uncertain, the act of publication itself generates fear and imposes a defensive burden on victims.

Taken together, these cases demonstrate that Handala’s operational impact is best understood across three tiers. At the highest tier are rare but significant operational disruptions, such as the Stryker incident, which produce measurable effects on systems and services. At the intermediate tier are verified exposures of personal or organizational data, which create reputational and intelligence risks but do not necessarily disrupt operations. At the lowest tier are narrative-driven claims and unverified leaks, which nonetheless generate psychological and informational effects by forcing responses and sustaining uncertainty.

The overall pattern supports a clear analytical conclusion: Handala’s effectiveness does not depend on consistent technical success. Instead, it derives from the ability to convert a limited number of real or plausibly real intrusions into a sustained campaign of perception management, intimidation, and coercive signaling. The majority of adverse events observed are therefore not technical in nature, but psychological and reputational, aligning closely with the broader doctrine of cyber-enabled influence operations.

Parallel Surveillance and Influence Operations

Expansion into Surveillance (2023-2026)



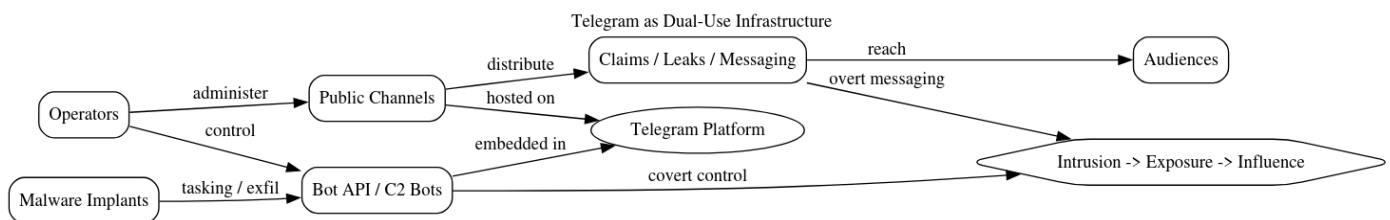
In parallel with its destructive and hack-and-leak operations, the campaign expanded significantly into surveillance and transnational repression beginning in late 2023 and continuing through 2026. *This shift represents a broadening of operational scope from institutional disruption to targeted monitoring of individuals, particularly dissidents, journalists, activists, and members of opposition networks.* Rather than relying solely on network exploitation, the actors adopted a more tailored approach centered on social engineering and user-level compromise, indicating both improved targeting intelligence and a strategic intent to exert pressure beyond traditional cyber domains.

Access in this surveillance branch is typically achieved through trojanized applications masquerading as legitimate software, including messaging tools, password managers, and media utilities. These lures are often aligned with the expected behavior and digital environment of the target, suggesting prior reconnaissance and profiling. Upon execution, these files deploy staged malware chains that establish persistence and initiate communication with operator-controlled infrastructure. The second-stage implants are modular and designed for continuous data collection, including screen capture, audio interception (with specific capability to monitor conferencing platforms), file harvesting, and credential access. Data is often staged locally, compressed, and prepared for exfiltration in a manner that minimizes detection while maximizing collection efficiency.

A defining characteristic of this surveillance capability is its use of Telegram as a command-and-control channel, leveraging the legitimate Telegram API to transmit instructions and exfiltrated data. This approach allows malicious traffic to blend with normal user activity, complicating network-based detection while simultaneously enabling rapid, distributed control of infected hosts. In some cases, the same platform is used for both covert communication and overt messaging, reinforcing the campaign's broader integration of technical and informational operations. Taken together, this surveillance expansion demonstrates a transition toward a persistent, person-centric operational model, in which intrusion, monitoring, and psychological pressure are applied in tandem to influence both institutional behavior and individual decision-making.

Telegram as Dual-Use Infrastructure

Telegram occupies a central and multifaceted role within this ecosystem, functioning simultaneously as a covert command-and-control (C2) channel and an overt platform for messaging, amplification, and audience engagement. This dual-use design is not incidental; it reflects a deliberate operational choice to consolidate multiple functions, control, communication, and influence within a single, widely trusted platform. By embedding operational activity within a legitimate and globally used service, the actors reduce their reliance on dedicated infrastructure while increasing resilience against disruption. At the same time, the platform's scale and accessibility allow it to serve as a high-capacity distribution mechanism for narrative content, enabling rapid dissemination of messaging to both targeted and broad audiences.



From a technical perspective, the use of Telegram as C2 is enabled through abuse of the Telegram Bot API, which allows malware to communicate with operator-controlled bots over encrypted channels that are indistinguishable from normal application traffic. This design significantly complicates detection, as network telemetry alone is often insufficient to differentiate benign from malicious use. Implants can issue commands, upload exfiltrated data, and receive tasking through standard API calls, effectively turning Telegram into a low-cost, low-visibility control infrastructure. Because Telegram traffic is commonly permitted in enterprise and personal environments, this approach provides a reliable communication channel that blends seamlessly into expected user behavior, reducing the likelihood of interception or blocking.

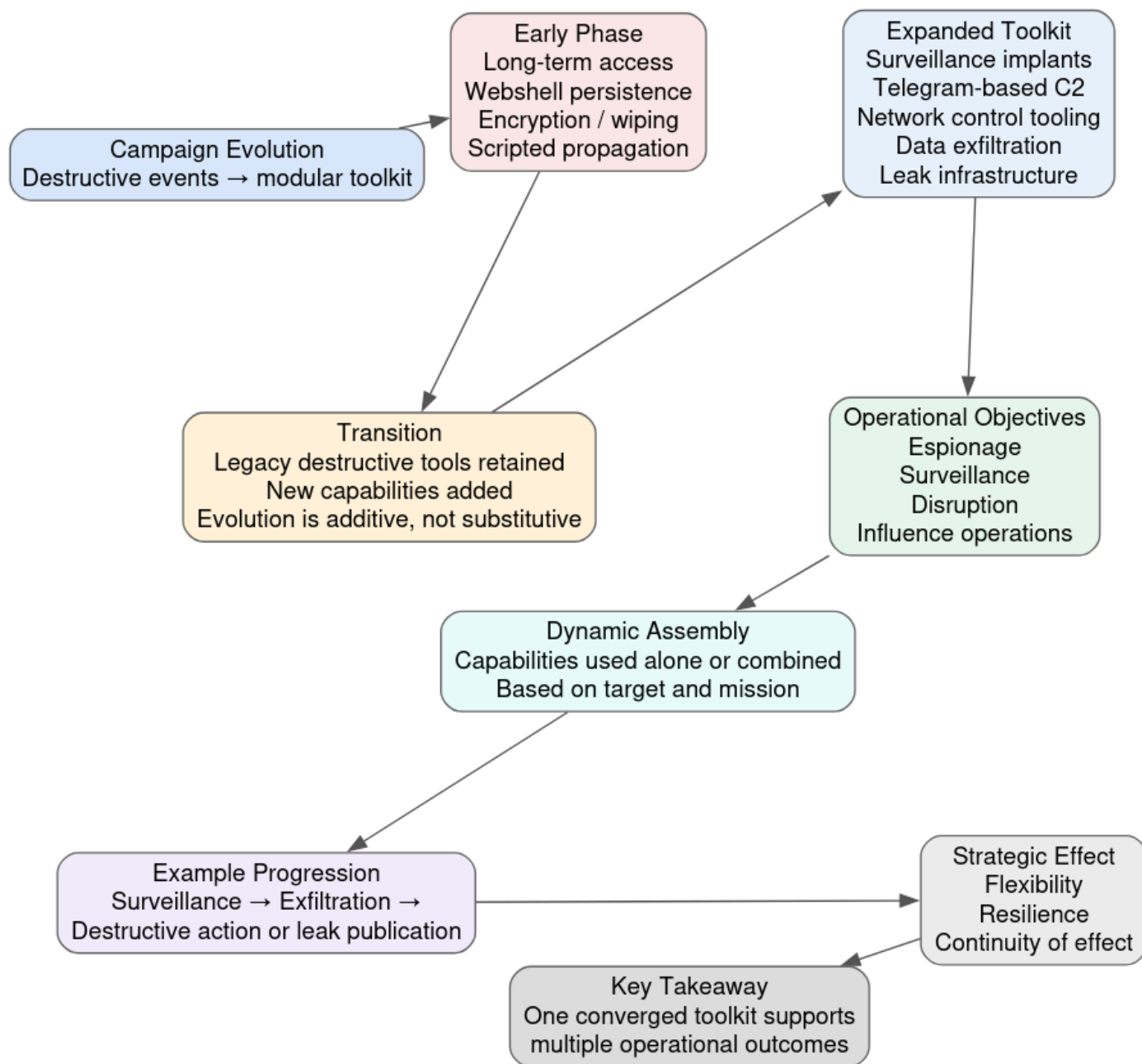
Concurrently, Telegram channels associated with the campaign function as public-facing dissemination nodes, distributing propaganda, operational claims, and references to leaked data. Channels such as those linked to the Homeland Justice persona serve as hubs where messaging is curated, amplified, and framed within ideological or political narratives. The presence of archive files, named data releases, and coordinated messaging indicates that these channels are not passive outlets, but active components of the operational workflow. This convergence of covert C2 and overt communication within the same

platform effectively bridges the technical and informational domains, allowing the actors to move seamlessly from intrusion and data collection to public exposure and psychological influence, all within a unified infrastructure.

Malware and Operational Evolution

Evolutionary Overview

The campaign demonstrates a progression from discrete, high-impact destructive events into a modular and adaptive operational toolkit capable of supporting a wide range of objectives across multiple target sets. Early activity, particularly during the Albania operations, was centered on singular, coordinated events in which long-term access culminated in ransomware-style encryption, wiping, and public attribution. Over time, however, these capabilities were not abandoned; instead, they were retained and integrated into a broader operational framework that supports espionage, surveillance, disruption, and influence operations in parallel.



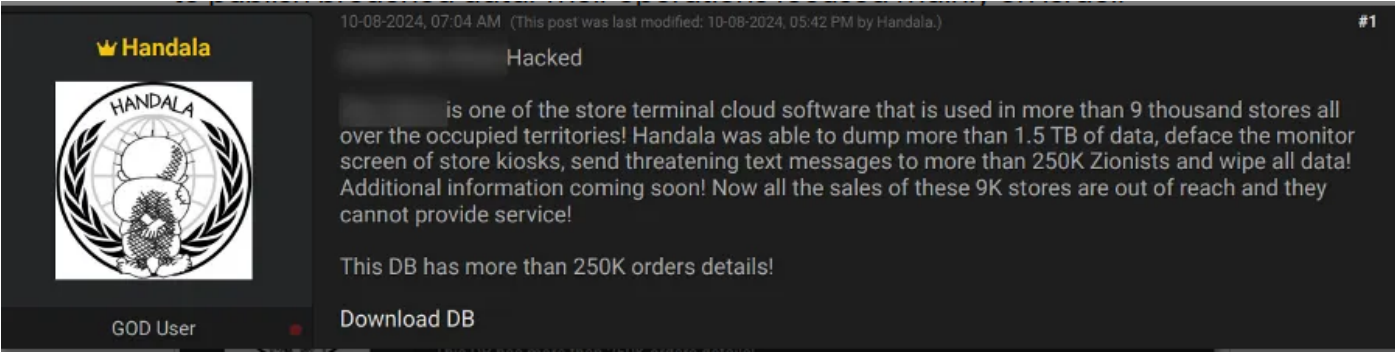
This evolution is distinctly additive rather than substitutive. Earlier destructive tools and techniques such as disk wiping, scripted propagation, and webshell-based persistence remain in active use, while newer capabilities have been layered on top. These include modular malware implants for surveillance, Telegram-based command-and-control, enterprise-scale tooling for network enumeration and control, and structured leak infrastructure for public disclosure. The result is a toolkit that can be dynamically assembled based on operational requirements, allowing actors to shift between stealthy collection, overt disruption, and psychological operations without fundamentally altering their underlying tradecraft.

The modular nature of this toolkit also enables operational flexibility and resilience. Components can be deployed independently or in combination, depending on the target environment and desired outcome. For example, an intrusion may begin as a surveillance operation, transition into data exfiltration, and culminate in either destructive action or controlled leak publication, all using elements of the same toolkit.

This layered approach reduces dependency on any single capability and allows the campaign to adapt to defensive pressures, infrastructure disruption, or shifting strategic priorities while maintaining continuity of effect.

Phase I: Destructive Intrusion Model

The Albania campaign established a repeatable model centered on prolonged, covert access followed by synchronized destructive impact and overt attribution. Operators achieved initial entry well in advance of the impact phase, maintained persistence through webshells and credential reuse, and conducted systematic reconnaissance and lateral movement across the environment. During this period, they harvested credentials, mapped network topology, and accessed email systems, enabling large-scale data exfiltration and the prepositioning of tools required for coordinated execution. This extended preparation phase indicates a deliberate emphasis on operational depth and positioning, rather than opportunistic disruption.



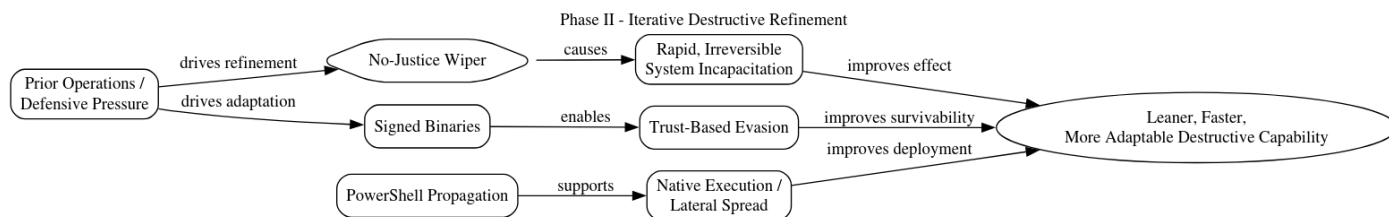
The transition to the impact phase was tightly orchestrated. Encryption and wiping components were deployed in sequence to maximize disruption, degrade recovery options, and ensure sustained operational impact across affected systems. The use of propagation mechanisms and administrative access allowed the actors to execute these actions broadly and nearly simultaneously, amplifying the scale of disruption. This was not a simple ransomware event; it was a destructive operation designed to disable systems, disrupt services, and create immediate strategic effect, particularly within government infrastructure.

Equally important was the deliberate and immediate move to public attribution and narrative control. Under the Homeland Justice persona, the actors claimed responsibility, released messaging, and framed the attack within a political and ideological context. This transformed the operation from a purely technical incident into a hybrid cyber–influence event, where the technical damage served as the foundation for broader psychological and reputational impact. The Albania campaign thus established a durable operational model: gain long-term access, prepare the environment, execute coordinated destruction, and rapidly exploit the event through controlled public disclosure to achieve strategic influence.

Phase II: Iterative Destructive Refinement

The introduction of the No-Justice Wiper reflects a clear refinement in the actor’s destructive capability, emphasizing speed, reliability, and operational efficiency. Compared to earlier tooling that combined encryption and wiping in a more sequential and resource-intensive manner, the No-Justice variant appears optimized for rapid execution and immediate impact. Its design prioritizes system incapacitation,

including corruption of critical structures required for operating system startup, thereby preventing recovery through conventional means. This shift indicates a move toward direct, irreversible disruption, reducing the time between execution and effect while minimizing the opportunity for defensive response.

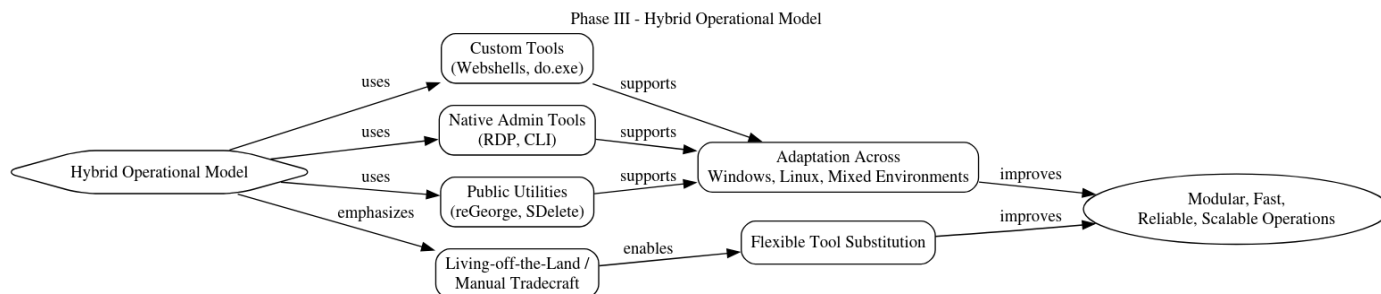


At the same time, the use of signed binaries demonstrates an increased focus on evasion through trust abuse. By leveraging code-signing mechanisms, the actors are able to bypass or reduce scrutiny from endpoint protection systems that rely on signature-based trust models. This reflects a more sophisticated understanding of defensive controls and suggests that the tooling has been adapted based on prior detection and mitigation efforts. The combination of trusted execution and destructive functionality allows the malware to operate with a lower likelihood of immediate detection, increasing the probability of successful deployment across multiple systems.

The reliance on PowerShell-based propagation and execution further underscores a transition toward living-off-the-land techniques. By utilizing native system capabilities, the actors reduce their dependency on large or complex malware payloads, enabling more flexible and stealthy deployment within compromised environments. PowerShell scripts can be rapidly modified, obfuscated, and distributed using existing administrative channels, allowing for efficient lateral spread and coordinated execution. Together, these elements – streamlined destructive logic, trust-based evasion, and native execution – illustrate a broader evolution toward leaner, more adaptable tooling that enhances both effectiveness and survivability within contested network environments.

Phase III: Hybrid Operational Model

The Karma phase introduced a distinctly hybrid operational approach that combined bespoke tooling with hands-on-keyboard techniques and widely available utilities, enabling flexible execution across heterogeneous environments. Rather than relying exclusively on custom malware, operators blended lightweight webshells and purpose-built components with native administrative tools and publicly available software. This reduced development overhead, shortened deployment time, and allowed rapid adaptation to differences in target infrastructure whether on-premises Windows domains, Linux servers, or mixed environments while preserving the ability to execute high-impact actions.

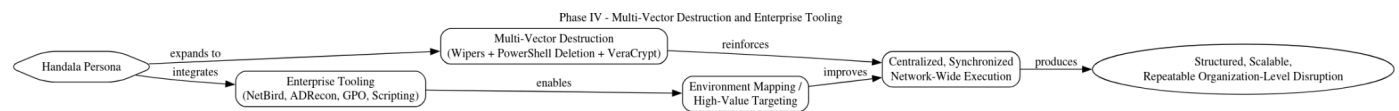


A defining feature of this phase was the increased emphasis on manual tradecraft and living-off-the-land techniques. Operators leveraged standard system utilities and administrative protocols such as RDP for lateral movement, built-in command-line tools, and common utilities like SDelete or disk formatting to perform destructive actions without introducing large, easily detectable binaries. Custom elements, including webshells (e.g., Karma Shell) and credential validation tools (e.g., do.exe), were used selectively to maintain access and verify privileges, while publicly available tools such as reGeorg enabled post-compromise control. This blend allowed operators to pivot quickly within compromised networks, execute tasks with minimal friction, and evade signature-based defenses by masking activity as legitimate administration.

The result was a modular, operator-driven execution model that prioritized flexibility, speed, and reliability over stealth alone. By combining custom implants with manual techniques and off-the-shelf tools, the actors could tailor operations to the specific constraints of each target, escalate privileges, propagate across systems, and initiate disruption with minimal dependency on a single capability. This hybridization also improved resilience: if one tool or method was detected or blocked, operators could readily substitute alternatives without disrupting the overall operation. In effect, the Karma phase marked a transition toward a more adaptable and scalable approach, capable of sustaining coordinated campaigns across diverse technical environments while maintaining alignment with the campaign’s broader objectives of disruption and influence.

Phase IV: Multi-Vector Destruction and Enterprise Tooling

Under the Handala persona, operations expanded into a coordinated, multi-method destruction model that reflects a clear increase in operational maturity and planning discipline. Rather than relying on a single payload or technique, actors began employing parallel destructive mechanisms, including custom wipers, PowerShell-based recursive deletion, and encryption via legitimate tools such as VeraCrypt. These methods were often executed in tandem across multiple systems, ensuring redundancy in effect and significantly reducing the likelihood of recovery. This approach demonstrates a shift from opportunistic disruption to deliberate, layered impact engineering, where multiple techniques reinforce one another to guarantee system failure and data loss.



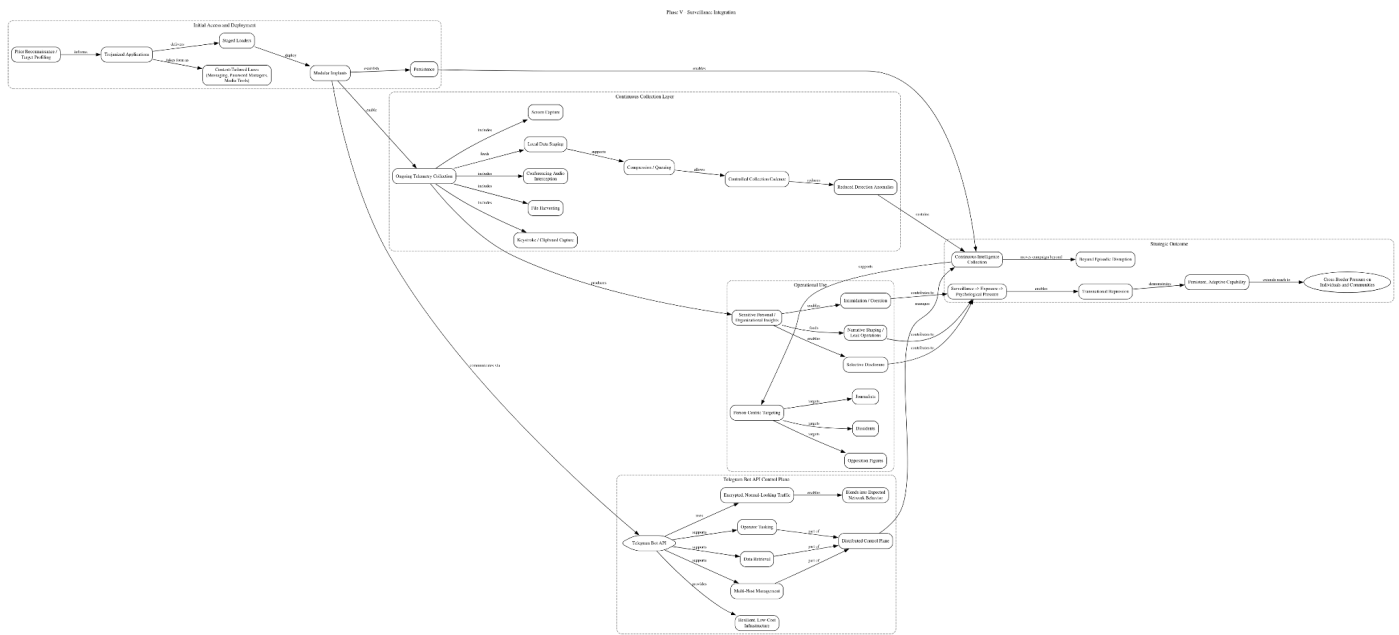
At the same time, the incorporation of enterprise-scale tooling enabled the actors to operate more effectively within complex network environments. Tools such as NetBird facilitated persistent internal connectivity and remote control across segmented networks, while ADRecon provided comprehensive visibility into Active Directory structures, users, and permissions. This combination allowed operators to map target environments in detail, identify high-value systems, and coordinate execution across domains with greater precision. The use of Group Policy and administrative scripting further enabled centralized deployment of destructive actions, amplifying scale and synchronizing impact across large portions of the network.

These developments collectively indicate a transition toward a structured, scalable operational model capable of sustaining complex campaigns within enterprise environments. The reliance on both custom and legitimate tools, combined with coordinated execution and network-wide visibility, reflects an

evolution beyond isolated incidents into systematic, organization-level disruption capability. Under Handala, the campaign demonstrates not only technical sophistication, but also an increased ability to integrate access, control, and destruction into a cohesive and repeatable operational framework aligned with broader strategic objectives.

Phase V: Surveillance Integration

Telegram-based malware campaigns introduced a persistent monitoring layer that materially expanded the campaign’s scope beyond episodic disruption into continuous intelligence collection. Initial access is commonly achieved through trojanized applications tailored to the target’s context, such as messaging clients, password managers, or media tools suggesting prior reconnaissance and profiling. Once executed, staged loaders deploy modular implants that establish persistence and enable ongoing telemetry collection, including screen capture, keystroke or clipboard capture, file harvesting, and, in some cases, audio interception of conferencing applications. Data is typically staged locally, compressed, and queued for exfiltration, allowing operators to control the cadence of collection and minimize anomalies that might trigger detection.

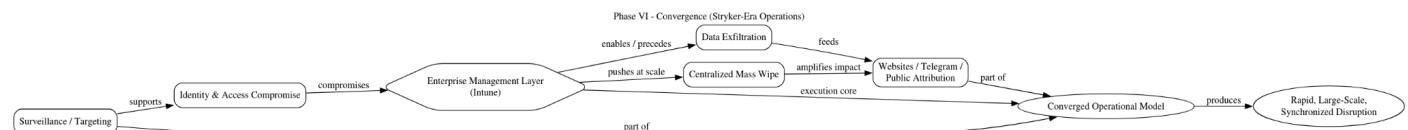


A defining feature of this capability is the use of Telegram’s Bot API as command-and-control, which allows implants to communicate over encrypted channels indistinguishable from normal Telegram traffic. This design provides a resilient, low-cost infrastructure that blends into expected network behavior and is difficult to block without disrupting legitimate use. Operators can issue tasking, retrieve data, and manage multiple hosts via bot commands, effectively turning Telegram into a distributed control plane. Because Telegram is widely permitted across enterprise and personal environments, this approach increases reliability while reducing dependence on bespoke infrastructure that is more easily identified and taken down.

Operationally, this surveillance layer supports transnational repression by enabling targeted, person-centric campaigns against dissidents, journalists, and opposition figures. Continuous monitoring yields sensitive personal and organizational insights that can be selectively disclosed, used to intimidate, or leveraged to shape narratives in subsequent leak operations. This tight coupling between covert

collection and overt exposure allows actors to move seamlessly from surveillance to psychological pressure, aligning technical activity with influence objectives. The result is a persistent, adaptive capability that extends the campaign's reach from network disruption to sustained coercion of individuals and communities across borders.

Phase VI: Convergence (Stryker-Era Operations)



Recent activity, particularly the Stryker incident (March 2026), demonstrates a clear convergence of destructive, surveillance, and influence capabilities into a unified operational model, while also marking a significant evolution in how these effects are delivered. Unlike earlier phases that relied heavily on malware deployment within compromised networks, emerging reporting indicates that Handala-linked actors achieved administrative access to enterprise management infrastructure, specifically Microsoft Intune, and used it as a force-multiplier for both disruption and scale. ([Cyber Magazine](#))

In the Stryker case, investigators and multiple reports suggest that attackers compromised an Intune administrative account or management console, allowing them to issue remote commands directly to enrolled endpoints. Intune, as a cloud-based endpoint management platform, is designed to enforce policies, deploy software, and remotely wipe devices. By gaining privileged access to this system, the actors were able to bypass traditional malware deployment entirely and instead execute a centralized wipe command across tens of thousands of devices simultaneously. Reports indicate that as many as 80,000–200,000 devices, including laptops and mobile endpoints, were wiped, while approximately 50 terabytes of data were exfiltrated prior to the destructive action. ([TechRadar](#))

This technique represents a fundamental shift in operational tradecraft. Rather than relying on endpoint-level persistence and execution, the actors targeted the control plane of the enterprise itself. With access to Intune, they effectively inherited the organization's own administrative authority, allowing them to push destructive actions at scale with minimal friction and high reliability. As one analysis noted, once inside such a system, “an adversary... just need[s] to press a button,” highlighting how legitimate enterprise tooling can be weaponized for immediate, large-scale impact.

The implications of this approach are significant. First, it dramatically reduces the need for detectable malware artifacts, complicating traditional detection strategies that rely on endpoint indicators. Second, it enables near-instantaneous, synchronized disruption across globally distributed infrastructure, as seen in the simultaneous impact across dozens of countries in the Stryker event. Third, it allows actors to combine data exfiltration, destructive wiping, and public attribution within a tightly compressed timeline, reinforcing the campaign's hack-and-leak model while increasing operational tempo. ([Tenable](#))

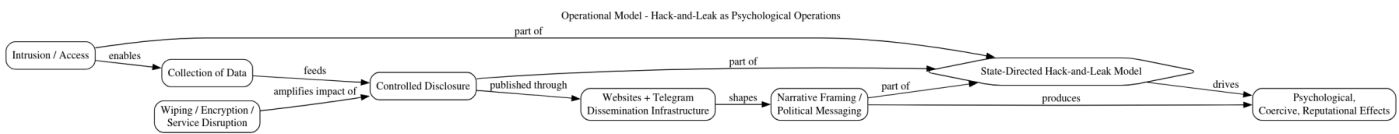
Critically, this evolution does not replace earlier capabilities but integrates with them. The same ecosystem that previously relied on wipers, PowerShell scripts, and Telegram-based command-and-control now demonstrates the ability to pivot into identity and access compromise at the enterprise

management layer, effectively collapsing the distinction between intrusion, execution, and impact. In this model, surveillance capabilities provide intelligence and targeting, administrative compromise enables execution at scale, and influence infrastructure websites and Telegram amplify the effects through public messaging and data release.

Taken together, the Stryker incident illustrates the campaign’s progression into a fully converged operational framework, where destructive, surveillance, and influence capabilities are no longer sequential phases but simultaneous, interdependent components. The abuse of Intune marks a notable escalation in both technical sophistication and strategic impact, demonstrating that the actors are not only adapting their tooling, but are increasingly targeting the centralized control mechanisms of modern enterprise environments to achieve rapid, large-scale disruption aligned with broader geopolitical objectives.

Operational Model: Hack-and-Leak as Psychological Operations

The Homeland Justice and Handala campaigns are best understood as state-directed hack-and-leak operations engineered for psychological impact, in which technical intrusion serves as a means to produce exploitable narratives rather than an end in itself. From their earliest manifestation, these operations have been structured to convert access into influence: compromise enables collection, collection enables disclosure, and disclosure is shaped to achieve coercive or reputational effects. This framing distinguishes the activity from financially motivated ransomware or purely clandestine espionage, positioning it instead within a model of cyber-enabled information warfare aligned with state objectives.



From the Albania campaign onward, data theft has been systematically paired with controlled, curated public disclosure through actor-operated infrastructure, including websites and Telegram channels such as @Homeland Justice1. These platforms function as dissemination nodes where messaging is crafted, amplified, and aligned with political narratives. The release of stolen material, often selective, staged, or thematically framed, is designed to maximize audience impact, reinforce claims of legitimacy, and sustain attention over time. In this sense, the infrastructure is not merely a repository for leaked data, but an active component of the operational workflow, bridging the gap between technical compromise and public perception.



Homeland Justice
 4.13K subscribers

 Search



Homeland Justice
[@JusticeHomeland1](#)

4.13K
Subscribers

245
Photos

51
Videos

139
Files

301
Links

<https://justicehomeland.info>
<https://t.me/boost/JusticeHomeland1>
<https://t.me/JusticeHomeland1?direct>


DOWNLOAD TELEGRAM

[About](#)
[Blog](#)
[Apps](#)
[Platform](#)



Homeland Justice



We are approaching the Zero Hour.. ⌚
 We hope you understand what we mean!

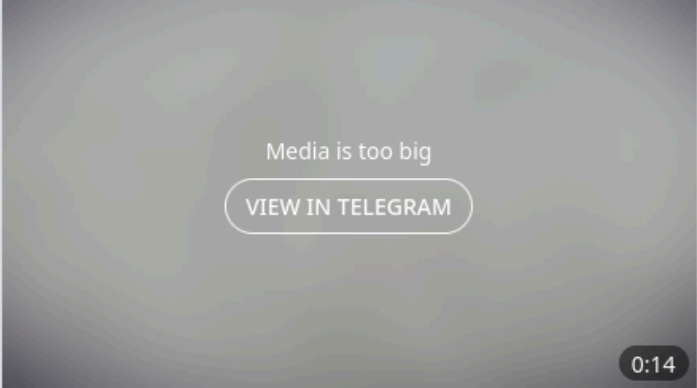
[@JusticeHomeland1](#)
[JusticeHomeland.info](#)
[T.me/boost/JusticeHomeland1](#)

 4
  2

649
  09:33



Homeland Justice



The Return of the Native
 Homeland Justice is back. More empowered!

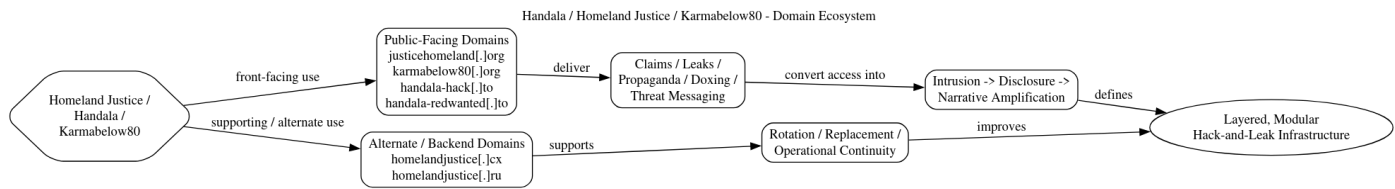
[#HomelandJustice](#)
[@JusticeHomeland1](#)
[JusticeHomeland.info](#)

@Homeland Justice1 Telegram Channel

Within this model, destructive actions serve primarily to amplify visibility and urgency, creating conditions that heighten the impact of subsequent disclosures. Wiping, encryption, and service disruption draw attention to the incident and signal capability, but the strategic value is realized through narrative amplification of how the event is presented, interpreted, and circulated. The transition to the Handala persona reflects a further refinement of this approach, with increased segmentation of infrastructure to support distinct functions such as leak publication, propaganda, and targeted exposure of individuals.

This specialization indicates a maturing operational framework in which success is measured less by persistence or financial return, and more by the ability to shape perception, apply pressure, and influence behavior across both institutional and individual targets.

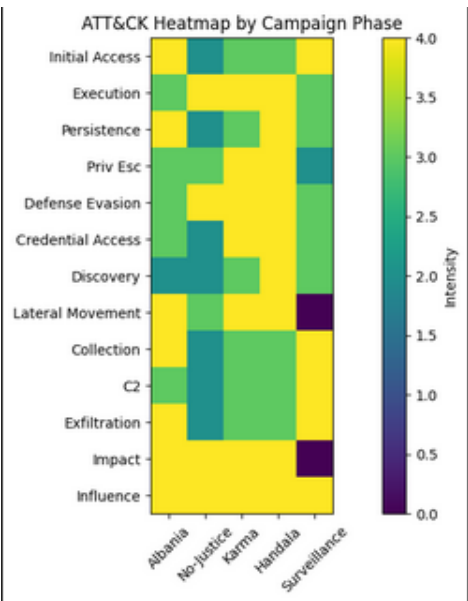
Infrastructure and Domain Ecosystem



The infrastructure supporting the Homeland Justice and Handala campaigns reflects a deliberate, layered architecture designed to separate public-facing operations from backend control while enabling specialized functions across the ecosystem. Core domains such as Homeland Justice[.]org, handala-hack[.]to, handala-redwanted[.]to, and karmabelow80[.]org operate as visible nodes for messaging, leak publication, and intimidation, serving as the primary interface through which the actors communicate with both targets and broader audiences. These platforms are used to disseminate propaganda, frame narratives, and release or reference stolen data, transforming technical intrusions into publicly consumable events aligned with the campaign’s psychological objectives.

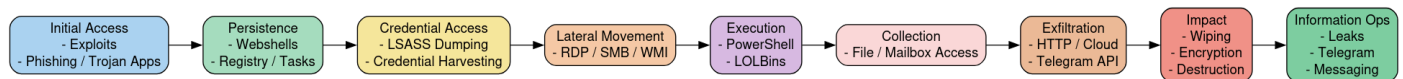
Behind this visible layer, additional domains such as homelandjustice[.]cx and Homeland Justice[.]ru likely function as alternate or backend infrastructure, supporting operational continuity and resilience. This separation suggests an architecture in which public-facing assets can be replaced or rotated without disrupting underlying capabilities, thereby reducing exposure while maintaining persistence. Within this system, each domain appears to serve a distinct and purpose-driven role, contributing to a modular framework that supports narrative framing, data publication, and targeted exposure. This functional segmentation reinforces the broader operational model, enabling the actors to coordinate technical compromise with controlled disclosure and messaging in a cohesive and scalable manner.

Tactics, Techniques, and Procedures (TTPs)



The campaign demonstrates a high degree of consistency in its tactics, techniques, and procedures (TTPs) across all observed phases, reflecting a mature and repeatable operational playbook. Initial access is typically achieved through a combination of exploitation of internet-facing services and targeted social engineering depending on the operational context. In earlier phases, actors leveraged vulnerabilities in externally exposed systems such as Microsoft SharePoint or Exchange to gain footholds within enterprise environments. In parallel, particularly in later surveillance-oriented activity, access has been obtained through user-centric compromise, including phishing and the delivery of trojanized applications tailored to specific targets. This dual approach allows the actors to flexibly pursue either broad network intrusion or highly targeted individual access depending on mission requirements.

Once access is established, persistence is maintained through a mix of webshell deployment and registry-based mechanisms, enabling continued control over compromised systems even in the face of remediation efforts. Webshells, often deployed on IIS or similar web servers, provide durable remote access and are frequently reused or redeployed as needed. Registry modifications and scheduled tasks are used to ensure execution at startup or at defined intervals, supporting long-term presence within the environment. Lateral movement is conducted using standard administrative protocols such as RDP, SMB, and Windows Management Instrumentation (WMI), often leveraging harvested credentials to blend activity with legitimate administrative behavior. This reliance on native protocols reduces the need for specialized tooling and helps evade detection by appearing consistent with normal network operations.



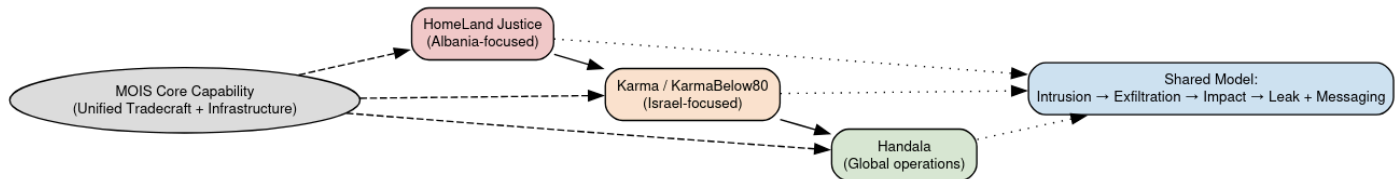
Credential access is a critical component of the campaign and is achieved through both credential harvesting and memory dumping techniques. Actors extract credentials from configuration files, email systems, and browser stores, while also leveraging native Windows components such as rundll32 and comsvcs.dll to dump LSASS memory and obtain plaintext credentials or hashes. These credentials are then used to escalate privileges and expand access across the network. Execution throughout the campaign frequently relies on PowerShell and command-line utilities, reflecting a strong preference for living-off-the-land techniques. PowerShell scripts are used for payload delivery, lateral movement, and destructive actions, and can be easily obfuscated or modified to evade detection while maintaining operational flexibility.

Data exfiltration is conducted using a combination of traditional methods and platform abuse, depending on the target environment and desired level of stealth. Files are typically staged locally, compressed, and transferred using standard protocols such as HTTP(S), FTP, or cloud storage services. In more advanced phases, particularly those involving surveillance, the actors leverage Telegram-based exfiltration, using the platform's API to transmit data through encrypted channels that blend with legitimate traffic. This approach provides both resilience and deniability, as it reduces dependence on dedicated command-and-control infrastructure and leverages widely permitted network activity.

The impact phase integrates multiple destructive techniques, including disk wiping, file encryption, and manual system destruction, often executed in a coordinated manner across numerous endpoints. Custom wipers, PowerShell-based deletion scripts, and legitimate tools such as disk formatting utilities or

encryption software are used in combination to maximize damage and complicate recovery. In some cases, actors manually execute commands to delete critical files or disable services, reinforcing the overall impact. This phase is frequently followed by immediate public disclosure, with the actors claiming responsibility and releasing messaging or data through controlled infrastructure. This rapid transition from technical action to public exposure is a defining characteristic of the campaign, linking operational execution directly to its broader objective of psychological influence and coercion.

Evolution of Personas



The progression from Homeland Justice to Karma and ultimately Handala reflects deliberate rebranding rather than a change in the underlying actor set. Core tradecraft, targeting logic, infrastructure patterns, and operational sequencing remain consistent, indicating continuity of capability and control. Homeland Justice was tightly aligned with the Albania campaign, emphasizing retaliation and coercive political messaging. As operations expanded, particularly after the Israel-Hamas conflict, the Karma persona enabled repositioning within a broader ideological frame while preserving the same methods. Handala represents a further evolution toward a durable, scalable identity suited for sustained, multi-theater activity.

These personas function as operational “skins” layered over a stable technical and organizational foundation. Each is tailored to specific audiences and narratives: Homeland Justice to Albanian political dynamics and the [MEK](#) (Mojahedin-e-Khalq), Karma to anti-Israeli messaging, and Handala to broader symbolic framing applicable across conflicts. This segmentation optimizes psychological resonance while complicating attribution by creating the appearance of distinct groups.

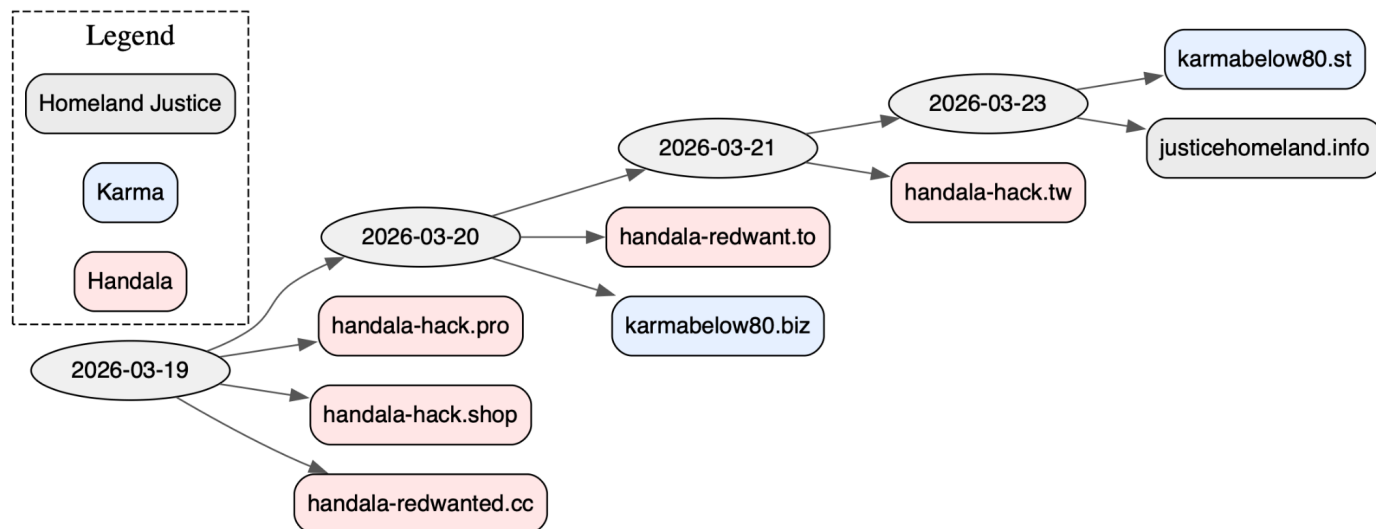
Multiple personas also manage exposure and risk. Branding shifts allow actors to distance current activity from prior campaigns, reset perception, and adapt to changing conditions without abandoning infrastructure or tradecraft. Parallel operations can run under different identities, reinforcing perceived decentralization. Despite this, consistent use of hack-and-leak workflows, Telegram and leak sites, and similar tooling confirms these are not separate entities but components of a unified, centrally directed ecosystem.

Strategic Assessment

These campaigns represent a state-directed, cyber-enabled influence capability that aligns closely with the operational doctrine of Iran’s Ministry of Intelligence and Security (MOIS), in which cyber operations are employed not solely for intelligence collection or disruption, but as instruments of coercion, signaling, and psychological pressure. The integration of intrusion, disruption, and narrative manipulation into a single operational system reflects a deliberate strategy in which technical access is leveraged to produce effects in the information domain. In this model, network compromise enables data acquisition and

operational positioning; disruption amplifies visibility and urgency; and controlled disclosure shapes perception, imposes reputational cost, and pressures decision-making. These elements are not sequential but interdependent, forming a cohesive framework designed to influence both institutional behavior and individual actors across geopolitical contexts.

New Domain Registrations (March 19–23, 2026)



Recent infrastructure activity over the last several weeks provides direct, empirical support for this assessment and demonstrates that this capability remains active, adaptive, and operationally synchronized. Between 19 March and 23 March 2026, the actor cluster executed a compressed domain registration burst, provisioning at least eight new domains across all three personas: *Handala*, *Karma/KarmaBelow80*, and *Homeland Justice*. The majority of these domains are Handala-branded, including [handala-hack\[.\]pro](#), [handala-hack\[.\]shop](#), [handala-hack\[.\]tw](#), [handala-redwanted\[.\]cc](#), and [handala-redwant\[.\]to](#), indicating that Handala remains the primary outward-facing operational identity. In parallel, the registration of [karmabelow80\[.\]biz](#), [karmabelow80\[.\]st](#), and notably [Homeland Justice\[.\]info](#) demonstrates that legacy personas are being actively reconstituted rather than retired.

This pattern is analytically significant. It indicates that personae evolution within this ecosystem is not linear but additive and concurrent. The actors are not transitioning from one identity to another; instead, they are maintaining multiple branded layers simultaneously, enabling them to pivot narratives, distribute operational risk, and complicate attribution. The near-simultaneous reactivation of Homeland Justice alongside active Handala expansion suggests deliberate attribution shaping and historical continuity signaling, reinforcing the perception of a persistent, ideologically driven campaign lineage.

The temporal characteristics of this activity further reinforce its operational intent. The tight clustering of registrations within a five-day window is consistent with pre-operational staging or infrastructure regeneration following disruption rather than routine domain churn. The inclusion of both “hack”-labeled domains and “redwanted”-style domains within this burst indicates parallel preparation for both intrusion-linked branding and leak-and-shame operations, which are central to this ecosystem’s influence model. This aligns with prior observed behavior in which compromised data is rapidly operationalized for public dissemination and psychological effect.

Comparable operational patterns can be observed in other state-aligned ecosystems, including Russian influence campaigns such as those associated with the Doppelgänger campaigns and hack-and-leak operations attributed to GRU-linked actors, and DPRK multi-cluster activity, where distinct operational units specialize in intrusion, financial operations, or disruption. However, the Homeland Justice / Handala ecosystem is distinguished by its consistent and tightly coupled integration of hack-and-leak operations with overt psychological messaging. Whereas Russian operations often separate intrusion from amplification, and DPRK activity frequently prioritizes financial or espionage outcomes, this campaign persistently merges technical compromise with immediate public attribution, curated disclosure, and ideological framing. The latest domain registrations reinforce this distinction by showing that infrastructure supporting both compromise and narrative dissemination is provisioned in parallel, not sequentially.

Accordingly, this activity should not be interpreted as a series of isolated incidents or campaigns, but as a persistent, evolving capability embedded within a broader state strategy. The newly observed domain registrations demonstrate that this capability can be rapidly reconstituted, expanded, and rebranded on demand, even in the face of prior takedowns or disruptions. The reuse of naming conventions, the continuity of tradecraft, the simultaneous operation of multiple personas, and the structured expansion of domain infrastructure all indicate an enduring operational framework rather than ad hoc activity. This capability can be activated, scaled, or redirected in response to changing geopolitical conditions, allowing it to remain relevant across multiple theaters and target sets. As such, it represents a sustained mechanism through which the state can project influence, apply pressure, and shape narratives in the cyber and information domains over time.

A.1 Albania Campaign (Homeland Justice)

Timeframe: ~May 2021–September 2022 (Initial Access → Impact)

Destructive / Encryption Malware

File	Type	Hash (MD5)	Notes
GoXML.exe	Ransomware / Encryptor	bbe983dba3bf319621b447618548b740	Primary encryption payload
cl.exe	Disk Wiper	7b71764236f244ae971742ee1bc6b098	Raw disk overwrite
mellona.exe	Propagation Tool	78562ba0069d4235f28efd01e3f32a82	Lateral movement support

Webshells (Persistence)

File	Type	Hash (MD5)	Notes
Error4.aspx	Webshell	81e123351eb80e605ad73268a5653ff3	Initial persistence
ClientBin.aspx	Webshell	a9fa6cfdba41c57d8094545e9b56db36	IIS-based control
Pickers.aspx	Webshell	8f766dea3afd410ebcd5df5994a3c571	Additional access vector

Supporting / Staging Tools

File	Type	Hash (MD5)	Notes
disable_defender.exe	Defense Evasion	60afb1e62ac61424a542b8c7b4d2cf01	AV disable
win.bat	Script	1635e1acd72809479e21b0ac5497a79b	Execution chain
win.bat (variant)	Script	18e01dee14167c1cf8a58b6a648ee049	Variant
bb.bat	Script	59a85e8ec23ef5b5c215cd5c8e5bc2ab	Deployment
rwdsk.sys	Driver	8f6e7653807ebb57ecc549cef991d505	Raw disk access
Goxml.jpg	Decoy / Payload Carrier	0738242a521bdfe1f3ecc173f1726aa1	Masquerading artifact

A.2 Albania Follow-On Campaign (No-Justice Wiper)

Timeframe: Late 2023–Early 2024

Destructive Malware

File	Type	Hash (SHA-256)	Notes
Ptable.exe / NACL.exe	Disk Wiper	36cc72c55f572fe02836f25516d18fed1de768e7f29af7bdf469b52a3fe2531f	Signed binary; prevents OS boot

Supporting Scripts

File	Type	Notes
p.ps1	PowerShell propagation script	Lateral spread
zip.zip	Archive	Payload staging

A.3 Israel Campaign (Karma / Void Manticore)

Timeframe: October 2023–Mid 2024

Custom Tooling

Tool	Type	Notes
Karma Shell	Webshell	Disguised as error page
do.exe	Credential validation tool	Domain admin check
reGeorge	Webshell	Post-auth access

Destructive / Wiper Activity

Tool	Type	Notes
BiBi Wiper (Windows/Linux)	Disk Wiper	Multi-platform destruction
SDelete	Secure deletion tool	Living-off-the-land
format utility	Disk formatting	Manual destruction

A.4 Handala Campaign (Destructive Operations)

Timeframe: 2025–2026

Primary Wipers

File	Type	Hash (MD5)	Notes
handala.exe	Custom Wiper	5986ab04dd6b3d259935249741d3eff2	Core destructive payload
PowerShell Wiper	Script	3cb9dea916432ffb8784ac36d1f2d3cd	Recursive deletion

Supporting / Abuse of Legitimate Tools

Tool	Type	Hash (MD5)	Notes
VeraCrypt Installer	Encryption tool	3236facc7a30df4ba4e57fddfb41ec5	Destructive encryption
NetBird Installer	Networking	3dfb151d082df7937b01e2bb6030fe4a	Lateral connectivity
NetBird	Networking	e035c858c1969cffc1a4978b86e90a30	Persistence

A.5 MOIS Telegram C2 Malware Campaign

Timeframe: Fall 2023–2026

Stage 1 (Initial Access / Lures)

File	Type	Hash (MD5)
Telegram_Authenticator.exe	Loader	B9086413E7B6A0C6A11C25D14C22615F
KeePass.exe	Loader	7402F2F9263782A4C469570035843510
Pictory_premium_ver9.0.4.exe	Loader	1E6B601F733BC40EAA58916986BFC5B9
WhatssApp.exe	Loader	(filename observed, hash unknown)

Stage 2 (Persistence / Exfiltration)

File	Type	Hash (MD5)	Notes
RuntimeSSH.exe	Backdoor	EBDD9595B79B39F53909D862499DBC94	Reverse SSH
RuntimeSSH.exe (variant)	Backdoor	E51FF37FB431767DCDEC0B5E6D2A786A	Variant
MicDriver.exe	Surveillance	D70EBF20E3D697897BAD5BEBF72EA271	Audio capture
MicDriver.dll	Support	F8B5554808428291ACC65D1FD2EFE01C	
MsCache.exe	Data theft	3E7A2FCEF1D038D05B20148C573A6499	Cache extraction
winappx.exe	Execution	481C5B5E69A08C3DF206C59FD8DDC0DC	
smqdservice.exe	Persistence	7E23FFADB664B0E53D821478A249D84C	

Supporting Artifacts

File	Type	Hash (MD5)
rantom.txt	Data artifact	A3394EF7FFA7E88B2E7EFAEE4617FE04
rantom.txt (variant)	Data artifact	2965817D063F1E8F9889F9126443D631

Command-and-Control

api.telegram.org

A.6 Cross-Campaign Observations

Malware Evolution Pattern

Phase	Characteristic
2022	Custom ransomware + wiper combo
2023	Signed wipers + propagation scripts
2024	Hybrid manual + custom destruction
2025–2026	Modular wipers + LOTL tooling + mesh networking
Parallel	Telegram-based surveillance malware

Key Trends

- Increasing reliance on **living-off-the-land tools**
- Use of **signed binaries for evasion**
- Shift toward **multi-method destruction**
- Expansion into **surveillance + repression tooling**
- Persistent integration with **information operations**

Appendix B – MITRE ATT&CK Matrix by Campaign Phase

his appendix presents a **matrix-style mapping** of the Homeland Justice / Karma / Handala ecosystem across the **MITRE ATT&CK Enterprise framework**, broken down by campaign phase. It highlights how capabilities evolved while maintaining continuity across tactics.

B.1 Albania Campaign (2022) – Homeland Justice

Tactic	Techniques
Initial Access	T1190 Exploit Public-Facing Application
Execution	T1059 Command Interpreter, T1059.001 PowerShell
Persistence	T1505.003 Web Shell
Privilege Escalation	T1078 Valid Accounts
Defense Evasion	T1070 Indicator Removal
Credential Access	T1003.001 LSASS Memory
Discovery	T1087 Account Discovery
Lateral Movement	T1021.001 RDP, T1021.002 SMB

Tactic	Techniques
Collection	T1114.002 Remote Email Collection
Command & Control	T1105 Ingress Tool Transfer
Exfiltration	T1041 Exfiltration Over C2
Impact	T1486 Data Encryption, T1561.001 Disk Wipe, T1485 Data Destruction

B.2 No-Justice Wiper Phase (Late 2023)

Tactic	Techniques
Execution	T1059.001 PowerShell
Persistence	T1078 Valid Accounts
Defense Evasion	T1218 System Binary Proxy Execution, T1036 Masquerading
Lateral Movement	T1021 Remote Services
Command & Control	T1105 Ingress Tool Transfer
Impact	T1561.001 Disk Wipe, T1485 Data Destruction, T1490 Inhibit Recovery

B.3 Karma Phase (Israel Operations 2023–2024)

Tactic	Techniques
Initial Access	T1190 Exploit Public-Facing Application
Execution	T1059, T1059.001 PowerShell
Persistence	T1505.003 Web Shell
Privilege Escalation	T1078 Valid Accounts
Defense Evasion	T1070 File Deletion, T1562 Impair Defenses
Credential Access	T1003.001 LSASS Memory
Discovery	T1018 Remote System Discovery
Lateral Movement	T1021.001 RDP, T1021.002 SMB
Collection	T1005 Data from Local System
Command & Control	T1105 Ingress Tool Transfer
Exfiltration	T1041 Exfiltration Over C2

Tactic	Techniques
Impact	T1485 Data Destruction, T1561 Disk Wipe

B.4 Handala Phase (2024–Present)

Tactic	Techniques
Initial Access	T1190, T1566 Phishing
Execution	T1059.001 PowerShell, T1218.011 Rundll32
Persistence	T1547 Boot/Logon Autostart
Privilege Escalation	T1078 Valid Accounts
Defense Evasion	T1036 Masquerading, T1562 Impair Defenses
Credential Access	T1003.001 LSASS, T1555 Credential Stores
Discovery	T1087 Account Discovery, T1069 Permission Groups
Lateral Movement	T1021 RDP/SMB
Collection	T1005 Local Data
Command & Control	T1105 Tool Transfer
Exfiltration	T1041 Exfiltration
Impact	T1485 Data Destruction, T1486 Encryption, T1490 Inhibit Recovery

B.5 Telegram Surveillance Campaign (2023–2026)

Tactic	Techniques
Initial Access	T1566 Phishing, T1204 User Execution
Execution	T1059.001 PowerShell
Persistence	T1547 Registry Run Keys
Defense Evasion	T1036 Masquerading
Credential Access	T1555 Credential Stores
Discovery	T1087 Account Discovery
Collection	T1113 Screen Capture, T1123 Audio Capture, T1005 Data Collection
Command & Control	T1071.001 Web Protocols (Telegram API)

Tactic	Techniques
Exfiltration	T1041 Exfiltration via C2
Impact	(Indirect – psychological/repression rather than system destruction)

B.6 Persona / Influence Infrastructure Layer

Tactic	Techniques
Resource Development	T1583.001 Domains, T1583.003 VPS
Establish Accounts	T1585.001 Social Media Accounts
Stage Capabilities	T1608 Upload/Stage Data
Command & Control	T1102 Web Service (Telegram as platform)

B.7 Cross-Phase ATT&CK Heat Map (Summary)

Tactic	Consistency Level
Initial Access	High
Execution (PowerShell / CLI)	Very High
Persistence	High
Credential Access	Very High
Lateral Movement	Very High
Collection	High
Command & Control	High
Exfiltration	High
Impact	Very High
Influence / Persona Ops	Unique / Defining

APPENDIX C Leaks Impact

Victim	Leak (Relative Timeline)	Claimed Data	Confirmed Adverse Event	Impact Type	Confidence
Stryker Corporation	Late (T10)	Large-scale data + "wipe"	Operational disruption to manufacturing, ordering, and shipments; systems restoration required; ~80,000 devices reportedly wiped	Operational + destructive	HIGH
Kash Patel	External (not in TW mirror but linked campaign)	Emails, personal data	Public exposure of personal emails and documents; reputational and counterintelligence risk	Exposure / reputational	HIGH
Hebrew University of Jerusalem	Late (parallel campaign)	40–48 TB wiped, 23 TB exfil (claimed)	Claimed destructive attack; partial reporting, no strong independent confirmation of full scale	Operational (claimed)	MEDIUM
Verifone	Mid–late (external claim)	Payment system compromise (claimed)	Company denied breach; no confirmed disruption	Reputational only	LOW
VahidOnline	Mid (T5)	~180,000 users + phone numbers	Doxxing and exposure of identities; intimidation risk to dissident network	Identity exposure / intimidation	MEDIUM-HIGH
Sima Shine	Mid (T4)	~100,000 emails (claimed)	Public leak claims; reputational and intelligence exposure; no confirmed operational disruption	Exposure / reputational	MEDIUM
Ilan Steiner	Early–Mid (T3)	~50,000 emails (claimed)	Public leak claims; financial/internal exposure narrative; no confirmed secondary impact	Exposure / reputational	MEDIUM
Deborah Oppenheimer	Early (T2)	Private communications (claimed)	Public exposure claims; limited external corroboration of downstream effects	Exposure / reputational	LOW-MEDIUM

Victim	Leak (Relative Timeline)	Claimed Data	Confirmed Adverse Event	Impact Type	Confidence
Eran Ortal	Early (T1)	Strategic documents (claimed)	Narrative exposure of military planning; no confirmed operational consequence	Exposure / narrative	LOW-MEDIUM
Israeli Security Institutions (aggregate)	Mid–Late (T7)	~50,000+ emails (claimed)	Systemic compromise narrative; no confirmed service disruption or institutional failure	Exposure / perception	MEDIUM
Mossad-linked "Treasury"	Mid–Late (T6)	Financial/internal documents (claimed)	Corruption/financial exposure narrative; no confirmed operational impact	Narrative / reputational	LOW-MEDIUM
Israeli Water Infrastructure	Late (T8)	Target database (claimed)	No confirmed breach; deterrence signaling only	Strategic signaling	LOW
Israeli Energy Grid	Late (T9)	Target database (claimed)	No confirmed breach; deterrence messaging	Strategic signaling	LOW
Lockheed Martin engineers (Israel)	External campaign	Personal data (dox)	Doxing + threats; intimidation campaign; limited validation of dataset accuracy	Physical intimidation	MEDIUM