LeakNet Extortion: ClickFix and Deno Runtime Loader TTPs

How Self-Execution Social Engineering and Legitimate Runtime Abuse Enable Data Extortion Campaigns

Unofficial AI-assisted Research

Cloud Security Alliance AI Safety Initiative

2026-03-17

Key Takeaways

The threat actor landscape surrounding data extortion campaigns has converged on two complementary techniques that together represent a structural shift in initial access and payload delivery—one that defeats both network-layer and endpoint controls simultaneously: ClickFix social engineering and abuse of the Deno JavaScript runtime as a fileless loader. LeakNet, a data extortion group identified in August 2025, exemplifies the profile of threat actors operating in this space—exfiltrating bulk data and leveraging victim-shaming infrastructure to pressure ransom payments without necessarily deploying file-encrypting ransomware [1][2]. The attack chain associated with this class of actor begins with ClickFix, a self-execution technique that induces victims to paste and run malicious commands directly, bypassing web security controls entirely [3]. Once execution is achieved, Deno—a legitimate, digitally signed JavaScript runtime—functions as a loader, executing obfuscated payloads while evading endpoint detection tools that whitelist trusted runtimes [4][5].

The significance of this combination extends beyond any single threat actor. ClickFix surged dramatically through 2025: ESET Research documented a 517% increase in observed attacks during the first half of that year [6], and the Microsoft 2025 Digital Defense Report separately identified ClickFix as the leading single initial access method observed by Microsoft Defender Experts, accounting for 47% of such notifications [18]. Separately, ThreatDown documented the first known weaponization of Deno in the CastleRAT campaign, a fileless attack chain that delivered ransomware after using Deno to execute steganographically concealed payloads extracted from JPEG images [4]. Iran's MuddyWater (Seedworm), assessed with high confidence to operate on behalf of the Ministry of Intelligence and Security, subsequently deployed the Dindoor backdoor using Deno as its execution engine in a March 2026 campaign targeting a U.S. bank, an airport, a nonprofit, and a defense-sector software supplier [5] [7]. The convergence of these techniques signals that Deno-as-loader has moved from novelty to operational tradecraft—and that defenders must update detection postures accordingly.

Background

LeakNet and the Data Extortion Model

LeakNet was first identified by Searchlight Cyber analysts on August 18, 2025, when the group posted proof of a claimed intrusion at SWAN General Limited, a financial and insurance firm in Mauritius [1]. The exfiltrated material described in the posting included customer identification documents, passports, financial records, and internal email correspondence—a data mix consistent with bulk credential and records harvesting rather than targeted surgical extraction. SOCRadar's dark web monitoring subsequently identified at least one additional victim, Banco Vimenca, posted to LeakNet's Tor-hosted leak site [2].

LeakNet's operational model is consistent with what security researchers classify as pure double extortion: data is stolen and held as leverage, with public posting on a victim-shaming site used to intensify ransom pressure. Critically, no confirmed encryption-based ransomware payload has been attributed to LeakNet in public reporting; the group's documented activity focuses on data exfiltration and extortion rather than file encryption [1][2]. This distinction matters operationally. It means that traditional ransomware defenses focused on backup integrity and encryption detection may not surface a LeakNet intrusion until the exfiltration phase is already complete and the actor has already published proof. Detection must therefore focus on the access and exfiltration phases rather than the detonation event.

Initial access vectors for LeakNet have not been definitively confirmed in public reporting as of the date of this analysis. While ClickFix has not been confirmed as a LeakNet initial access vector, organizations investigating an unexplained extortion intrusion during a period when ClickFix accounted for a high proportion of initial access activity should include ClickFix scenarios in their investigation scope alongside other common vectors such as phishing, credential stuffing, and VPN exploitation.

The ClickFix Technique

ClickFix emerged in early 2024 as a social engineering mechanism exploiting the gap between browser-based security controls and direct operating system command execution. In its canonical form, a victim visiting a malicious or compromised webpage encounters a fake browser error dialog, a broken CAPTCHA, or a verification prompt. JavaScript running behind the page silently injects an obfuscated command—typically a Base64-encoded PowerShell invocation—into the user's clipboard. The page

instructs the victim to press Win+R to open the Windows Run dialog, paste the contents of the clipboard, and press Enter. The victim executes the attacker's command directly, without any browser security layer, content filter, or email gateway examining the payload [3][8].

The technique's effectiveness derives from this bypass architecture. Web proxies and secure email gateways cannot inspect a command that travels through the user's clipboard and executes through the operating system's native run facility. The lure is both simple and credible—years of experience with legitimate browser prompts that request action to resolve apparent errors have made the instruction to paste a command feel consistent with expected browser behavior—and the execution path requires no exploit, no vulnerability, and no privilege escalation at the point of delivery. CISA, the FBI, HHS, and MS-ISAC issued a joint advisory in July 2025 (AA25-203A) documenting ClickFix as the primary initial access mechanism in Interlock ransomware campaigns, formalizing the technique's status as a significant operational threat [9]. Microsoft Security published a detailed analysis of ClickFix variants in August 2025, including documentation of state-sponsored actors from Iran, North Korea, and Russia incorporating the technique into their intrusion playbooks [8][17].

ClickFix has continued to evolve technically. Modern variants have been adapted for macOS and Linux targets. A successor technique, FileFix, was observed in testing in July 2025 and extends the self-execution model to file-based lures [10]. A DNS-based variant exploiting Microsoft's nslookup utility was disclosed in February 2026, demonstrating that the underlying social engineering framework continues to find new execution pathways [11].

Deno as a Malware Loader

Deno is an open-source JavaScript and TypeScript runtime developed by Ryan Dahl, the original creator of Node.js. Released as stable in 2020 and widely used in legitimate software development, Deno is distributed as a digitally signed binary, supports native TypeScript execution, and can run cross-platform scripts with minimal dependencies. These same properties make it attractive as an attacker-controlled execution environment: antivirus and endpoint detection and response (EDR) tools that apply trust based on digital signature and binary reputation typically do not flag Deno as malicious, and its use in legitimate enterprise environments makes behavioral anomalies harder to distinguish from normal activity [4].

ThreatDown (Malwarebytes) documented the first known weaponization of Deno in the CastleRAT campaign, attributed to the GrayBravo threat cluster (also tracked as TAG-150) [12][16]. In that attack chain, a ClickFix lure delivers an initial command that silently downloads and installs Deno. Deno then executes an obfuscated JavaScript payload that fetches a JPEG image from attacker infrastructure. The image contains an encrypted payload embedded via steganography; a PyArmor-protected Python script decodes it and loads CastleRAT through reflective PE injection, a fileless technique in which the

executable is loaded directly into memory without writing to disk [4]. CastleRAT proceeds to perform keystroke logging, clipboard theft, system fingerprinting, and command-and-control beaconing. Recorded Future's Insikt Group subsequently documented multiple distinct threat clusters—attributed to GrayBravo affiliates—using the same CastleLoader infrastructure as a precursor to CastleRAT deployment [12][13]. The Velvet Tempest affiliate cluster has been documented using this chain as a delivery path for Termite ransomware [14].

Iran's MuddyWater represents the most recent and highest-profile adoption of the Deno loader technique. Active campaign infrastructure was identified in March 2026 targeting organizations across the U.S. financial, aviation, nonprofit, and defense-adjacent software sectors [5][7]. The Dindoor backdoor deployed in this campaign uses Deno as its execution runtime and was signed with a certificate issued to "Amy Cherne," a convention consistent with prior MuddyWater certificate infrastructure [5][7]. Companion malware Fakeset, a Python-based implant, was deployed alongside Dindoor at the airport and nonprofit victim sites. Data exfiltration from compromised hosts was routed through Rclone, directed to Wasabi cloud storage—a cloud exfiltration pattern that leverages the same trusted-service bypass logic that makes Deno effective as a loader [7].

Security Analysis

Why the ClickFix-Deno Chain Is Structurally Difficult to Detect

The ClickFix-to-Deno attack chain exploits two distinct gaps in conventional security architectures simultaneously. ClickFix defeats network-layer controls by moving execution to the endpoint and routing the initial command through the clipboard and the operating system run facility rather than through a browser download or email attachment. Deno defeats endpoint controls by using a trusted, signed binary as the execution container for malicious JavaScript, sidestepping application allowlisting policies and AV heuristics that identify malware by binary characteristics rather than behavioral patterns.

The combination is compounding: defenders must detect the ClickFix lure at the user interaction layer before the run dialog opens (difficult, because the technique bypasses browser controls), or they must detect the anomalous invocation of Deno during the execution phase (challenging in environments where Deno is legitimately installed), or they must detect the downstream payload behavior after CastleRAT or a similar implant has already loaded into memory. The narrowest detection window with the highest signal-to-noise ratio is the behavioral layer: an unexpected process spawning Deno with network connectivity and subsequent memory injection activity is anomalous regardless of whether Deno itself is trusted.

The steganographic JPEG component of the CastleRAT chain adds a third layer of evasion. Network-layer inspection of the Deno JavaScript's outbound fetch request encounters a valid JPEG image file—a format that content inspection tools typically pass without deep analysis. Detecting the steganographic payload requires either behavioral detection of the subsequent decryption and memory injection sequence, or network behavioral analytics capable of flagging anomalous outbound connections from Deno processes [4].

Threat Actor Convergence on Deno

The documented adoption of Deno as a loader by both financially motivated cybercriminal clusters and a state-sponsored Iranian APT within a short operational window indicates that Deno abuse is in an active expansion phase. The short interval between GrayBravo's documented Deno abuse and MuddyWater's subsequent adoption suggests that awareness of the technique spread rapidly—possibly through underground forums, observed operational success of the criminal clusters, or the intelligence-sharing relationships between Iranian MOIS actors and criminal infrastructure that Check Point Research has documented [15]. While the specific communication pathway is not confirmed, the pattern warrants treating Deno as an actively diffusing technique rather than an isolated finding.

The GrayBravo/TAG-150 cluster's modular delivery architecture—CastleLoader staging CastleRAT, which in turn delivers ransomware or enables extortion—makes it particularly significant as a case study for enterprise defenders. Recorded Future's documentation of multiple distinct threat clusters adopting the same CastleLoader infrastructure suggests that GrayBravo is functioning as a loader-as-a-service intermediary: providing initial access and staging capability to multiple downstream operators, each running their own final-stage payloads [12][13]. This is a pattern analogous to the loader-as-a-service role Emotet and TrickBot fulfilled for ransomware affiliates—removing the downstream ransomware payload does not eliminate the initial access capability, which remains available to be reloaded by the infrastructure operator.

Implications for Cloud and Hybrid Environments

Data extortion groups targeting cloud-connected environments gain additional leverage from the exfiltration phase because cloud storage can be accessed and exfiltrated without requiring the attacker to maintain continuous network connectivity to on-premises infrastructure. The MuddyWater campaign's use of Rclone pointed at Wasabi cloud storage exemplifies this pattern: a single Rclone execution can exfiltrate hundreds of gigabytes through an HTTPS connection that bypasses destination-based network controls, as the traffic is structurally identical to legitimate cloud sync. Behavioral analytics capable of flagging anomalous transfer volumes, unusual cloud endpoint registration, or Rclone process provenance may surface this activity, but such controls are not universally deployed [7]. LeakNet's

documented exfiltration at SWAN General—characterized as "hundreds of gigabytes" including identity documents and financial records, as alleged by the threat actor in their leak site posting—is consistent with cloud storage-assisted bulk exfiltration, though the specific exfiltration method has not been publicly confirmed [1].

Cloud environments also expand the data extortion surface in ways that traditional ransomware response plans may not account for. An extortion actor targeting a cloud-connected organization can threaten to expose data stored in S3 buckets, SharePoint sites, or cloud email archives as well as data on local endpoints. Security teams designing response playbooks for extortion scenarios should map their full data inventory across both on-premises and cloud storage and ensure that incident response plans address containment of cloud credentials as part of the initial compromise scope, not only after a breach is confirmed.

Recommendations

Immediate Actions

Security teams should implement user-level behavioral controls targeting the ClickFix execution path. The Windows Run dialog (Win+R) is rarely required for standard end-user workflows in managed enterprise environments—though IT administrators and developers may have legitimate uses—making it a practical candidate for restricted or monitored execution in end-user workstation policy. Group Policy and endpoint management tooling can be used to restrict or log Win+R invocations from non-administrative users; flagging PowerShell or cmd.exe processes spawned from the Run dialog as high-priority alerts provides a detection signal that carries low false-positive rates in environments where standard end-users have no legitimate need to invoke those shells through the Run dialog. Environments with administrative or developer populations should baseline legitimate behavior before setting alert priority. Similarly, monitoring for the installation of Deno or similar lightweight JavaScript runtimes (Node.js, Bun) through unsigned or non-software-catalog installation events can surface early stages of the CastleRAT-style attack chain before payload execution.

Endpoint detection rules should specifically target processes that invoke Deno with outbound network connections. A Deno process that fetches a remote file and subsequently spawns a memory injection or PE loading sequence represents a high-fidelity behavioral indicator of the described attack chain. Many EDR platforms support custom behavioral rules that can surface this pattern without requiring prior knowledge of specific file hashes or command signatures—an important capability given that the described chains are designed specifically to evade hash-based detection.

Short-Term Mitigations

Organizations should review and audit application allowlisting policies to ensure that Deno, Bun, and similar JavaScript runtimes—even if legitimately used in development environments—are not permitted to execute in end-user workstation contexts where their presence cannot be explained by documented business need. Where Deno is legitimately required, restrict its network access through host-based firewall rules to the minimum set of permitted endpoints.

Security awareness programs should be updated to include ClickFix scenarios specifically. Users who understand that a legitimate web page or browser security dialog will never ask them to open the Windows Run dialog and paste a command are significantly less susceptible to the technique, regardless of how the lure is presented. Simulated phishing programs should incorporate ClickFix-style lures to test and reinforce this awareness. CISA's July 2025 joint advisory on Interlock ransomware (AA25-203A) provides indicator sets and detection guidance that can be adapted for enterprise detection rule development [9].

Cloud storage permissions should be audited for the presence of overly permissive credentials or tokens that could enable bulk exfiltration. Rclone and similar tools should be restricted in endpoint management policies unless specifically required, and egress monitoring should be configured to alert on unusually large outbound data transfers to cloud storage endpoints regardless of the transfer method. Organizations holding sensitive bulk data—financial records, identity documents, healthcare records—are specifically targeted by extortion groups like LeakNet and should apply proportionate controls to data at rest and in transit.

Strategic Considerations

The convergence of ClickFix and Deno abuse across both criminal and state-sponsored threat actor ecosystems suggests that these techniques will remain operationally active for an extended period. The underlying evasion logic exploits two structural properties of conventional security controls—reliance on user interaction layer trust and binary reputation as a proxy for benign behavior—that cannot be addressed through patch management alone. Defenders should treat the detection and mitigation work described above as long-term capability development rather than a one-time response to a specific campaign.

Organizations operating in sectors targeted by LeakNet and related extortion actors—financial services, insurance, critical infrastructure—should evaluate their data discovery and classification maturity. Extortion groups derive leverage from the breadth and sensitivity of exfiltrated data; organizations that do not know where their most sensitive data resides cannot effectively contain an actor who is actively

staging it. A data inventory program that maps sensitive data to specific systems and access controls provides the baseline visibility needed to both reduce extortion leverage through access restriction and identify exfiltration events through anomalous access patterns.

CSA Resource Alignment

This threat pattern intersects with multiple Cloud Security Alliance frameworks and guidance documents.

The MAESTRO framework for AI threat modeling (Layer 4: Agent Trust Boundaries; Layer 6: Ecosystem Integration) is relevant to the Deno loader technique. As AI-assisted development tooling increasingly relies on JavaScript runtimes including Deno and Node.js for agentic task execution, the same signed-binary trust relationship that makes Deno effective as a malware loader applies to AI agent execution environments. Defenders building agentic AI pipelines should assess runtime execution contexts as part of their MAESTRO threat model rather than extending implicit trust to runtimes based solely on digital signature.

The Cloud Controls Matrix (CCM) provides applicable controls across several domains. CCM domain TVM (Threat and Vulnerability Management) addresses detection capability for emerging attack techniques. CCM domain IAM (Identity and Access Management) applies to the credential access phases of the described intrusion chain, including the post-ClickFix harvesting of credentials that precedes lateral movement and data staging. CCM domain DSP (Data Security and Privacy) covers the data classification, access control, and exfiltration monitoring practices most directly relevant to defeating extortion actors like LeakNet.

CSA's Zero Trust guidance is directly applicable to the cloud exfiltration pathway documented in the MuddyWater Dindoor campaign and consistent with LeakNet's operational model. A zero trust posture that requires continuous verification for cloud storage access and applies egress data transfer monitoring at the workload level provides meaningful defense-in-depth against the cloud exfiltration phase of this attack chain—particularly when behavioral analytics are configured to flag anomalous data transfer volumes from otherwise-verified sessions. However, zero trust controls do not prevent the initial ClickFix execution or detect Deno-based payload staging on a compromised endpoint, because ClickFix operates through valid user credentials and sessions that pass posture checks in most ZT implementations. Workload behavioral monitoring and user awareness training remain necessary complements to ZT controls for this attack pattern.

CSA's AI Organizational Responsibilities framework should prompt security teams to assess whether AI coding assistants, developer toolchains, and automated build environments in their organizations use Deno or similar runtimes in ways that could create legitimate cover for malicious Deno process execution—a consideration relevant to establishing baseline behavioral expectations for Deno-enabled processes.

References

[1] Searchlight Cyber, "LeakNet Ransomware Group – SWAN General Limited Breach," Mine2.io, August 18, 2025. https://www.mine2.io/blog/2025-08-18-leaknet-ransomware-swan-general-breach/

[2] SOCRadar, "Banco Vimenca and Wired Government Data Leaks," SOCRadar Blog, 2025. https://socradar.io/blog/banco-vimenca-wired-government-data-leaks/

[3] Unit 42 / Palo Alto Networks, "Fix the Click: Preventing the ClickFix Attack Vector," Palo Alto Networks, 2025. https://unit42.paloaltonetworks.com/preventing-clickfix-attack-vector/

[4] ThreatDown / Malwarebytes, "CastleRAT: The First Cyberattack to Abuse the Deno JavaScript Runtime to Evade Enterprise Security," ThreatDown Blog, 2025. https://www.threatdown.com/blog/castlerat-cyber-attack-is-the-first-to-abuse-deno-javascript-runtime-to-evade-enterprise-security/

[5] The Hacker News, "Iran-Linked MuddyWater Hackers Target U.S. Networks with Dindoor Backdoor," The Hacker News, March 2026. https://thehackernews.com/2026/03/iran-linked-muddywater-hackers-target.html

[6] Infosecurity Magazine, "ClickFix Attacks Surge 517% in First Half of 2025," Infosecurity Magazine, June 26, 2025. https://www.infosecurity-magazine.com/news/clickfix-attacks-surge-2025/

[7] The Register, "Iran's MOIS Backdoored a US Bank, Airport Networks and More," The Register, March 5, 2026. https://www.theregister.com/2026/03/05/mudywater_backdoor_us_networks/

[8] Microsoft Security, "Think Before You Click(Fix): Analyzing the ClickFix Social Engineering Technique," Microsoft Security Blog, August 21, 2025. https://www.microsoft.com/en-us/security/blog/2025/08/21/think-before-you-clickfix-analyzing-the-clickfix-social-engineering-technique/

[9] CISA, FBI, HHS, MS-ISAC, "#StopRansomware: Interlock Ransomware," Joint Cybersecurity Advisory AA25-203A, July 22, 2025. https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-203a

[10] Check Point Research, "FileFix: The New Social Engineering Attack Building on ClickFix, Tested in the Wild," Check Point Blog, July 2025. https://blog.checkpoint.com/research/filefix-the-new-social-engineering-attack-building-on-clickfix-tested-in-the-wild/

[11] The Hacker News, "Microsoft Discloses DNS-Based ClickFix Variant via Nslookup," The Hacker News, February 2026. https://thehackernews.com/2026/02/microsoft-discloses-dns-based-clickfix.html

[12] Recorded Future / Insikt Group, "GrayBravo's CastleLoader Activity Clusters Target Multiple Industries," Recorded Future, 2025. https://www.recordedfuture.com/research/graybravos-castleloader-activity-clusters-target-multiple-industries

[13] The Hacker News, "Four Threat Clusters Using CastleLoader as GrayBravo Expands," The Hacker News, December 9, 2025. https://thehackernews.com/2025/12/four-threat-clusters-using-castleloader.html

[14] BleepingComputer, "Termite Ransomware Breaches Linked to ClickFix and CastleRAT Attacks," BleepingComputer, 2025. https://www.bleepingcomputer.com/news/security/termite-ransomware-breaches-linked-to-clickfix-castlerat-attacks/

[15] Check Point Research, "Iranian MOIS Actors: The Cybercrime Connection," Check Point Research, March 10, 2026. https://research.checkpoint.com/2026/iranian-mois-actors-the-cyber-crime-connection/

[16] Darktrace, "CastleLoader and CastleRAT: Behind TAG-150's Modular Malware Delivery System," Darktrace Blog, November 26, 2025. https://www.darktrace.com/blog/castleloader-castlerat-behind-tag150s-modular-malware-delivery-system

[17] Proofpoint, "Around the World in 90 Days: State-Sponsored Actors Try ClickFix," Proofpoint Threat Insight, April 17, 2025. https://www.proofpoint.com/us/blog/threat-insight/around-world-90-days-state-sponsored-actors-try-clickfix

[18] Microsoft, "Microsoft Digital Defense Report 2025," Microsoft Security, October 2025. https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2025