VANISHING ACT

What *Really* Happened to BlackFile ?

Austin Larsen
Principal Threat Intelligence Analyst · Google Threat Intelligence Group

UNC6671 · 10-min lightning talk

Who is BlackFile?

An extortion brand (tracked as UNC6671) that became one of 2026's most impactful, and most under-reported, threat actors.

Early 2026

First observed; high operational cadence

Dozens of Victims

Organizations targeted across US, UK & Australia

Millions Extorted

Opening demands, often settling at low six figures

M365 + Okta

Primary identity & SaaS targets

BlackFile vs. ShinyHunters: Cousins, Not Twins

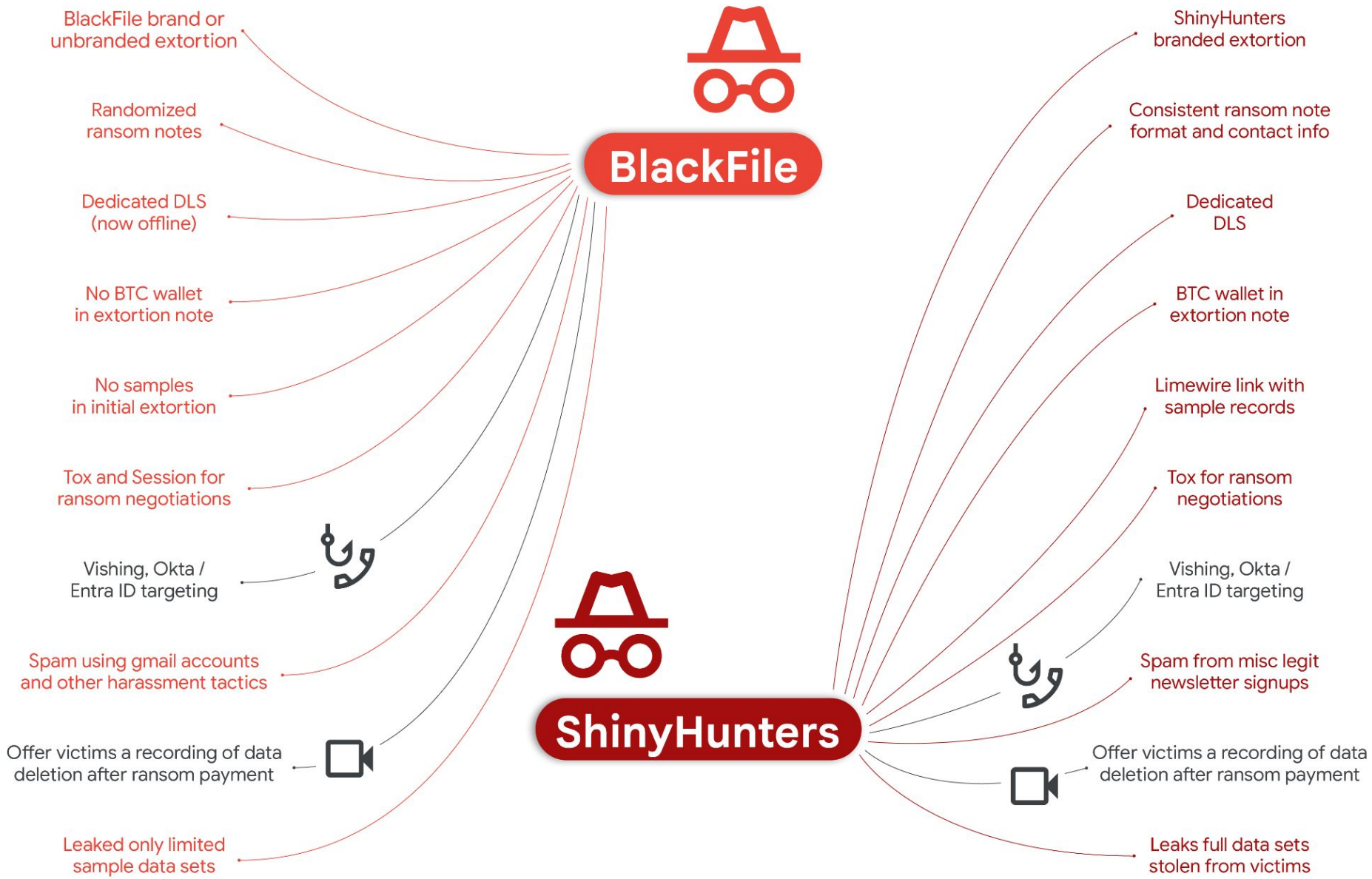
GTIG tracks these as distinct clusters (UNC6671 vs. UNC6240). Same vishing-to-SaaS playbook, but the branding, channels, extortion, and infrastructure diverge.

WHAT THEY SHARE Vishing as IT help desk · victim-branded SSO harvesting · live MFA interception · attacker MFA device · PowerShell / scripted SaaS exfiltration · 72-hour extortion deadlines · email spam ·

BlackFile UNC6671	
BRAND	BlackFile identity & DLS
CHANNEL	Unique Tox IDs, then exclusively Session
REGISTRAR	Tucows; subdomain (passkeyms[.]com)
EXTORTION	Quiet DLS; samples only, no full dumps

ShinyHunters UNC6240	
BRAND	Established ShinyHunters DLS
CHANNEL	Consistent Tox; tutanota / onionmail
REGISTRAR	NICENIC (paired w/ UNC6661)
EXTORTION	Loud: Limewire/Shinywire, DDoS, named victims, media engagement

Comparing TTPs



Live AiTM Vishing: Bypassing MFA

A caller posing as IT help desk walks the victim through a fake passkey enrollment while the attacker relays credentials and MFA prompt to the real portal.

01

Vishing call

Caller hits personal cell, masquerades as IT: "mandatory passkey migration"

02

Redirect

Victim sent to look-alike SSO subdomain (passkeyms[.]com)

03

Relay & capture

Creds + live MFA push/SMS/TOTP submitted to the real IdP in real time

04

Register device

Attacker enrolls their own MFA device for persistence

Result: a foothold established before the SOC can typically spot the anomaly.

Blinding the SOC: "Direct Fetch" Exfiltration

By replaying captured session cookies with python-requests / PowerShell, the actor streams files via direct HTTP GETs, logged as benign FileAccessed, not FileDownloaded.

WHAT SOCs USUALLY WATCH

FileDownloaded
events, treated as the high-signal indicator. FileAccessed is frequently ignored.

```
"UserAgent": "python-requests/2.28.1"
"Operation": "FileDownloaded"
"ApplicationDisplayName": "Microsoft Office"
```

WHAT ACTUALLY HAPPENED

FileAccessed
a direct fetch that mimics a normal web client and blends into routine traffic.

```
"UserAgent": "python-requests/2.28.1"
"Operation": "FileAccessed"
"ApplicationDisplayName": "python-requests"
```

1,000,000+ files pulled from a single victim's SharePoint & OneDrive in one run.

When Victims Don't Pay: Escalation

Notes started unbranded via unique Tox, then identified as "BlackFile" on Session with a typical 72-hour deadline. Silence from victims sometimes triggered aggressive real-world pressure.

Mailbox flooding

Dozens of throwaway Gmail accounts spam employee inboxes until auto-restricted

Executive voicemails

Threatening messages left directly for C-suite

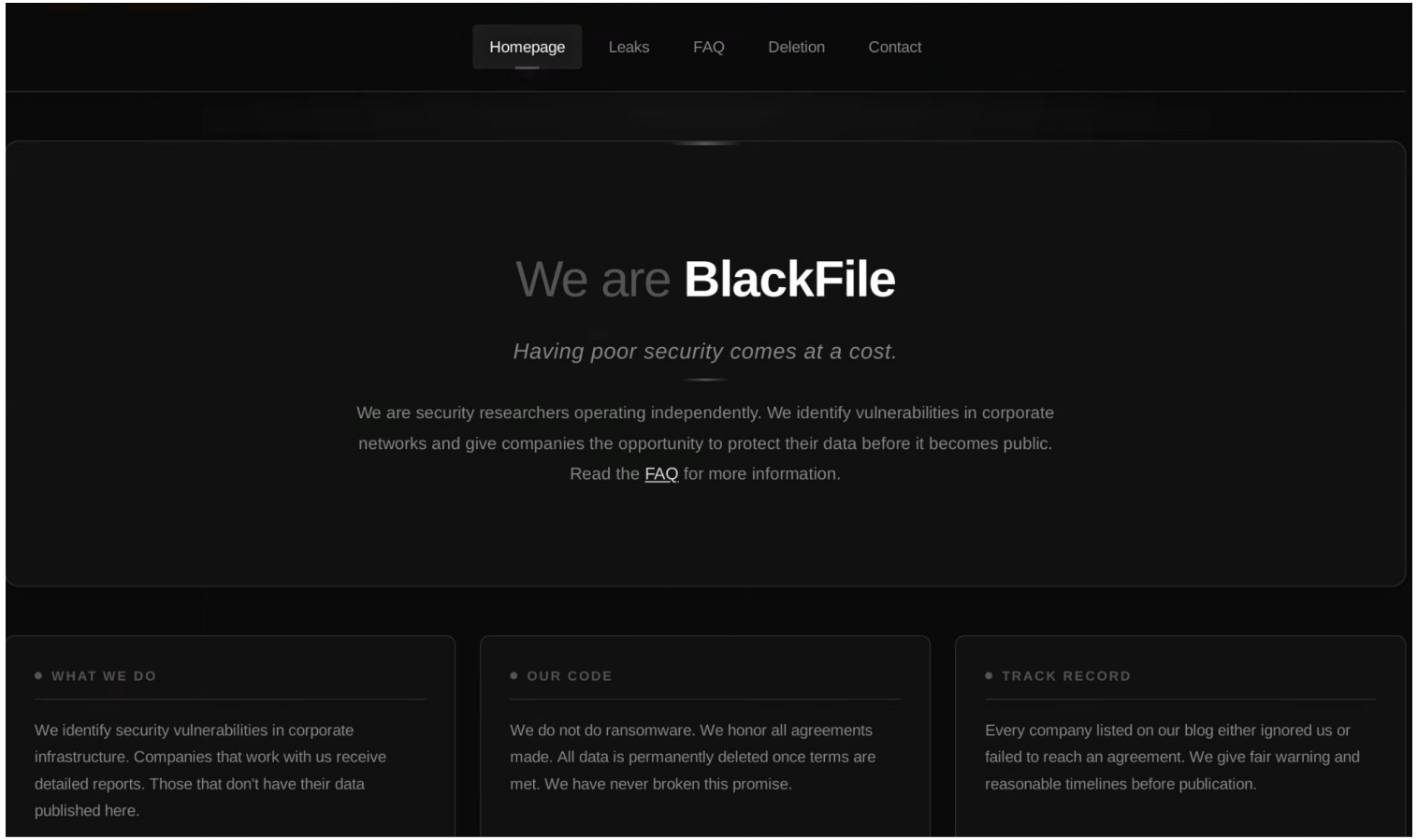
Corporate swatting

False emergency reports weaponized against company personnel

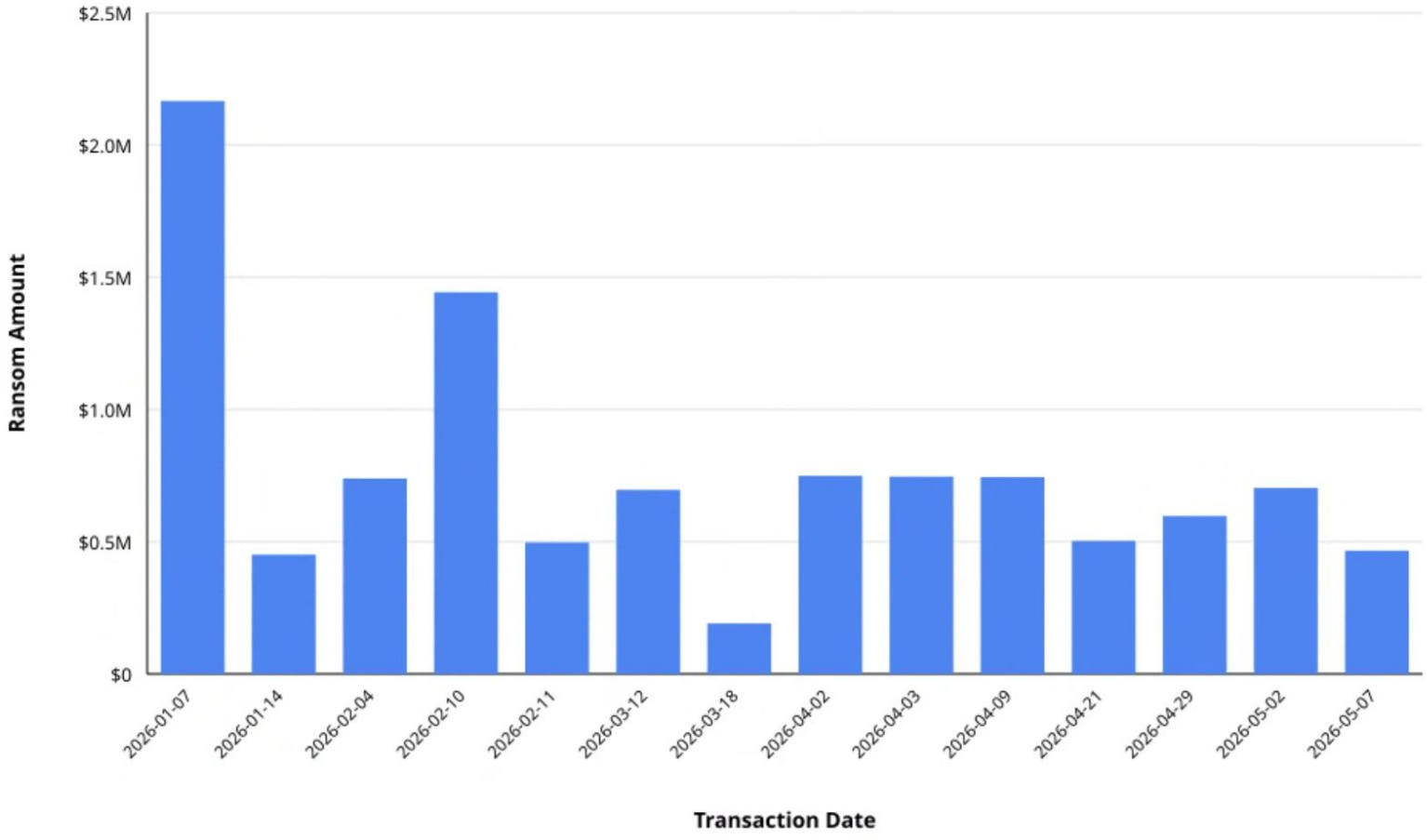
> *“Silence may not always be wise in situations like this. We will not be ignored.”*
>
> Generalized BlackFile ransom note

The BlackFile Data Leak Site

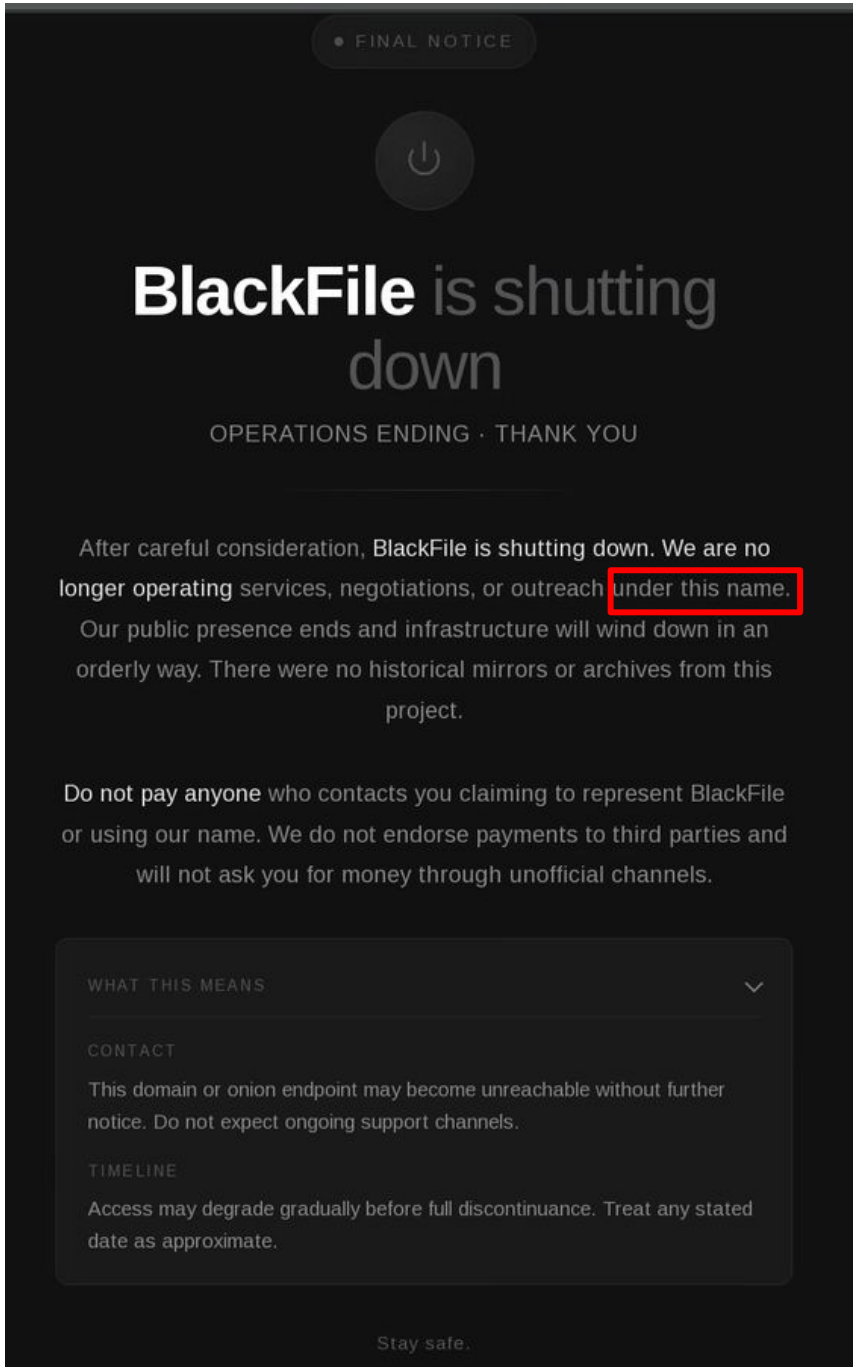
Not really advertised, never indexed, only limited samples ever posted.



Blackfile Ransom Payments



Blackfile Shuts Down



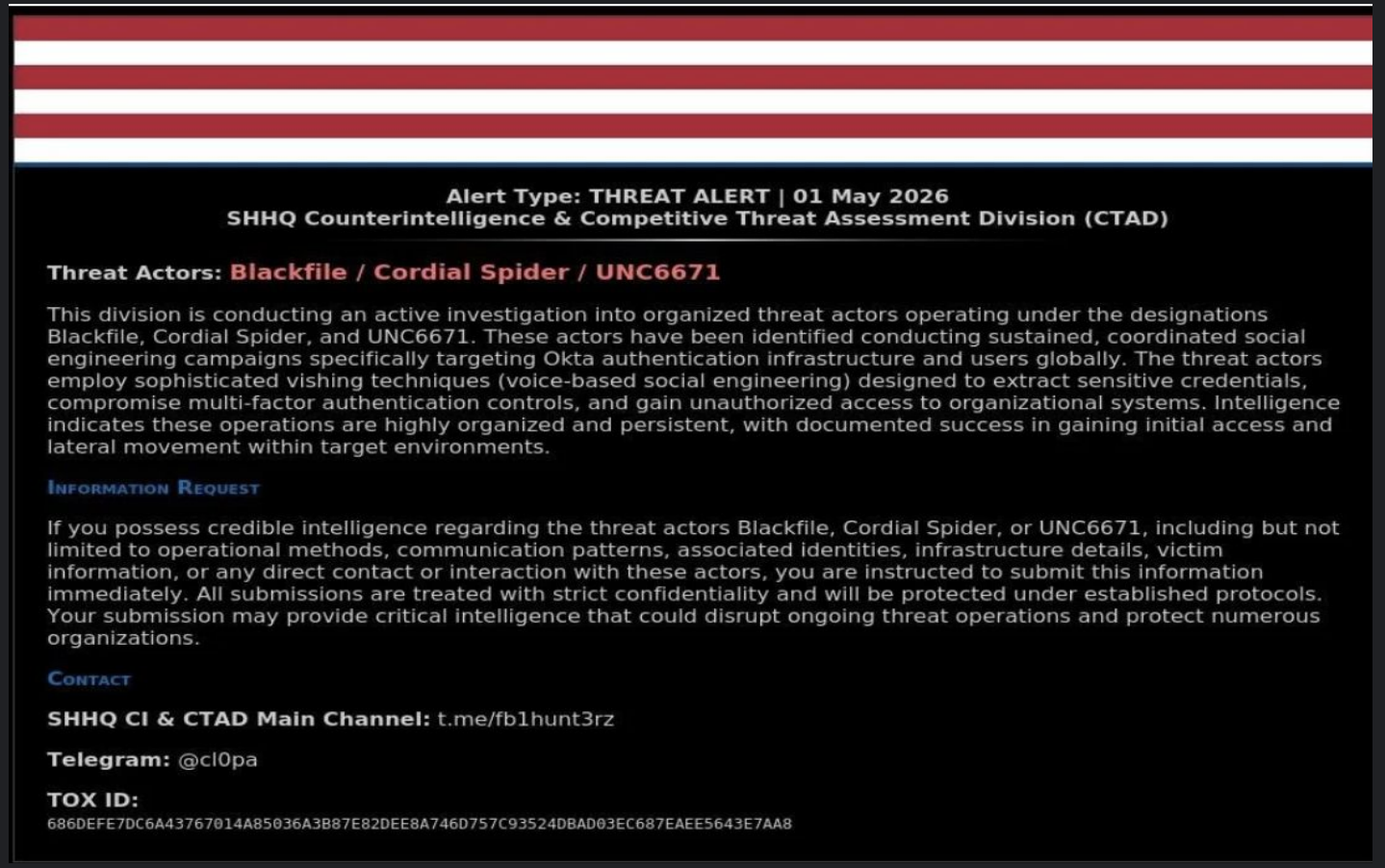
The Vanishing Act: A Timeline

Chaotic disappearance and bizarre resurrection.

FEB 2, 2026	**Krebs: “Don't Feed the SLSH”**	KrebsOnSecurity profiles the Scattered Lapsus$ ShinyHunters extortion ecosystem and encourages victims not to pay.
FEB 6, 2026	**BlackFile DLS launches**	Leak site goes live; compromises escalate
LATE APR 2026	**BlackFile goes dark**	DLS drops offline for several weeks
MAY 1, 2026	**ShinyHunters Telegram threat**	SLSH publicly asks for info on UNC6671.
MAY 7, 2026	**Instructure Canvas hack**	ShinyHunters double-breaches Canvas
MAY 11, 2026	**“Shutting down” + all negotiations stop**	DLS briefly returns: “shutting down… under this name.” All ongoing extortion talks cease
DAYS LATER	**“Redact” appears, then offline; “Pink” follows**	Alleged rebrand surfaces, then a “Pink” DLS emerges just days ago

What Spooked Them Offline?

In early May 2026, the SLSH Telegram channel publicly solicited information on UNC6671. Days later, BlackFile went dark and announced its shutdown.



Alert Type: THREAT ALERT | 01 May 2026
SHHQ Counterintelligence & Competitive Threat Assessment Division (CTAD)

Threat Actors: Blackfile / Cordial Spider / UNC6671

This division is conducting an active investigation into organized threat actors operating under the designations Blackfile, Cordial Spider, and UNC6671. These actors have been identified conducting sustained, coordinated social engineering campaigns specifically targeting Okta authentication infrastructure and users globally. The threat actors employ sophisticated vishing techniques (voice-based social engineering) designed to extract sensitive credentials, compromise multi-factor authentication controls, and gain unauthorized access to organizational systems. Intelligence indicates these operations are highly organized and persistent, with documented success in gaining initial access and lateral movement within target environments.

Information Request

If you possess credible intelligence regarding the threat actors Blackfile, Cordial Spider, or UNC6671, including but not limited to operational methods, communication patterns, associated identities, infrastructure details, victim information, or any direct contact or interaction with these actors, you are instructed to submit this information immediately. All submissions are treated with strict confidentiality and will be protected under established protocols. Your submission may provide critical intelligence that could disrupt ongoing threat operations and protect numerous organizations.

Contact

SHHQ CI & CTAD Main Channel: t.me/fb1hunt3rz

Telegram: @cl0pa

TOX ID:
686DEFE7DC6A43767014A85036A3B87E82DEE8A746D757C93524DBAD03EC687EAEE5643E7AA8

SLSH Affiliated TELEGRAM CHANNEL

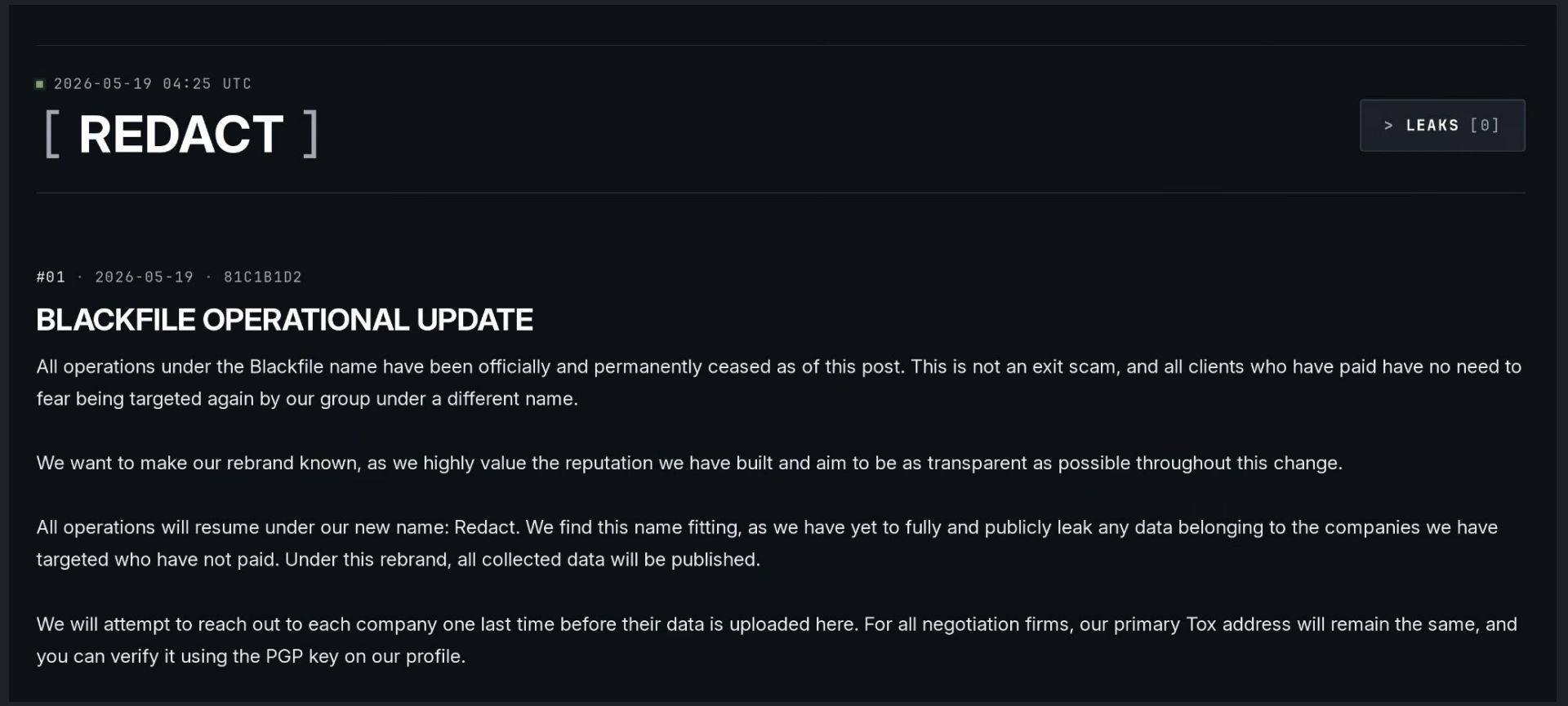
?

The open question

Was a threat from a more established enough to make UNC6671 abandon its brand? Timing is suggestive, not conclusive.

The Redact Data Leak Site

The alleged successor



Red Flags in the Redact Rebrand

A few weird things.

Abandoned protocols

Drops BlackFile's own Tox→Session migration and reverts to advertising a "primary" Tox ID

Borrowed playbook

Mimics ShinyHunters' tradecraft, the very brand BlackFile once impersonated

Courting negotiators

Directly addresses ransom-negotiation firms, a departure from prior behavior

Loud, not quiet

BlackFile never advertised its DLS; this one wants to be seen

The biggest tell: Redact claimed it would contact BlackFile's existing victims to continue negotiations. As far as we know, not a single one has been contacted.

The Redact Data Leak Site

2026-06-04 19:25 UTC

[REDACT]

> LEAKS [0]

#01 · 2026-05-22 · D32687F8

BLACKFILE OPERATIONAL UPDATE

As of this post, all operations under the Blackfile name have been permanently ceased and will not continue. However, our operations are not shutting down. We are continuing under a new name: Redact.

We find this name fitting, as we have yet to publicly leak any data, except for a few instances involving companies that did not pay us. This will change under our rebrand. We have collected data from over 30 companies that have not paid us, and their data will be uploaded here soon. We will attempt to reach out to these companies one more time before uploading their data.

For all clients who have paid us, there is no need to worry. You will not be targeted again. Our code of conduct and business practices will remain unchanged. We highly value the reputation we have built, which is why we wanted to be as transparent as possible about our rebrand.

So... What Really Happened?

Scared into retirement?

Law enforcement or competitor scrutiny may have forced a quiet exit.

A hostile takeover?

Did another actor take over the brand, infrastructure, or victims mid-negotiation?

Just another rebrand?

Extortion crews routinely disperse and reappear under new names to retool.

Defender Takeaways

Phishing-resistant MFA

Move to FIDO2 keys / passkeys: the single most effective control against AiTM vishing

FileAccessed

Treat it as critically as FileDownloaded when the UserAgent is a scripting library

Hunt scripted agents

Alert on python-requests / PowerShell UAs spoofing "Microsoft Office"

Correlate infra

Flag auth from commercial VPNs / hosting providers abnormal for the user

Guard credentials

Password Alert (Workspace) / Defender Credential Protection on submission

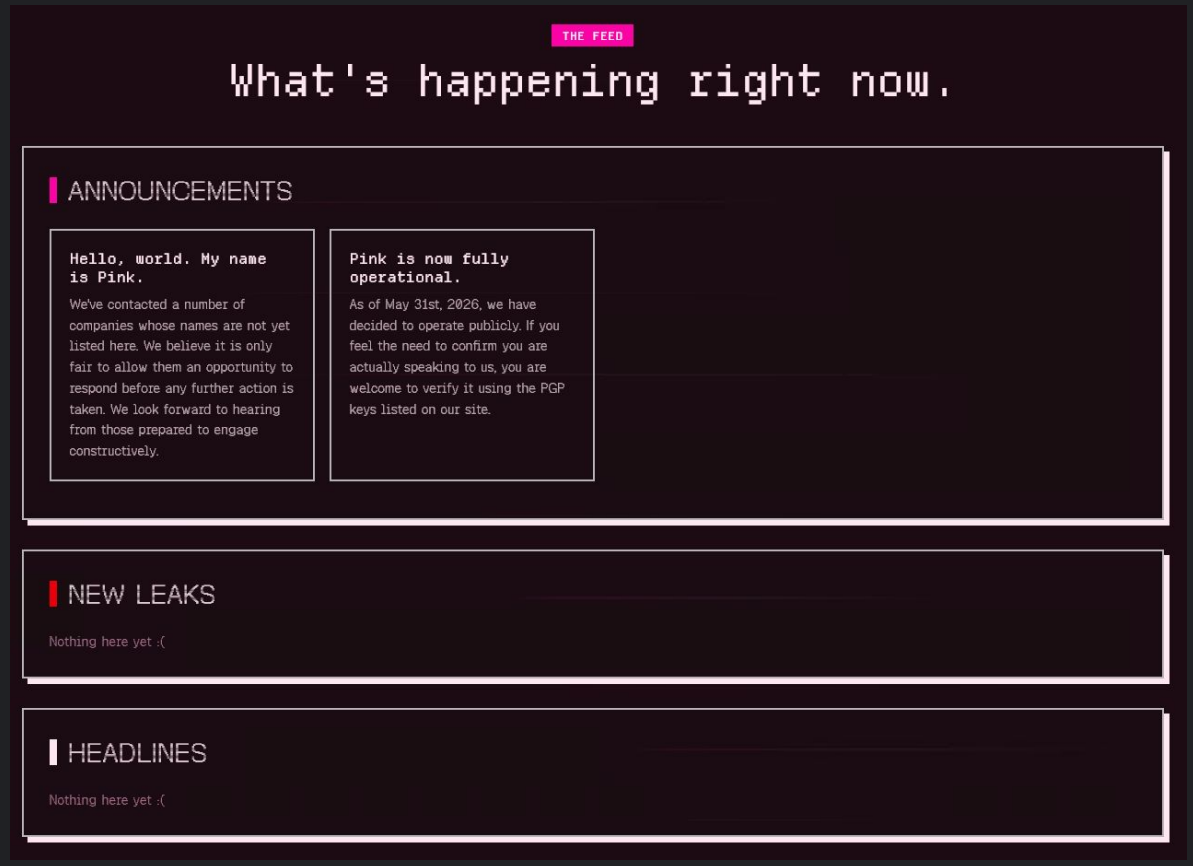
Watch IdP device adds

MFA factor setup right after failed / abandoned challenges = red flag

What's Next?

Even if the BlackFile name is retired, they are not going anywhere. First reported by Unit42 earlier this week, we are now tracking an emerging Pink DLS that looks very similar. We assess this is likely UNC6671.

Same actor? Copycat? We shall see.



x.com/AustinLarsen_

kernelpanic.28