



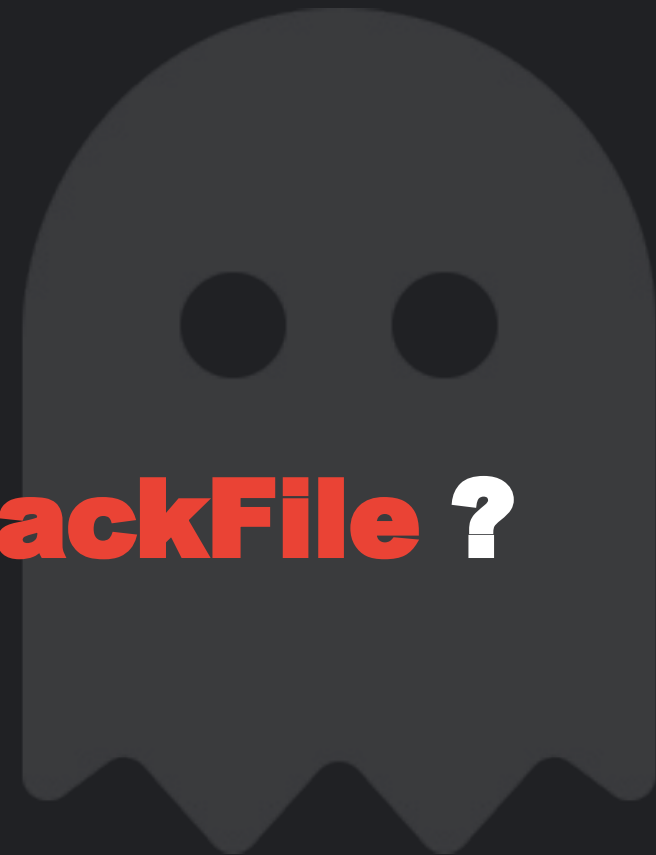
VANISHING ACT

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.



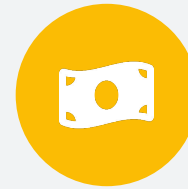
Early 2026

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.

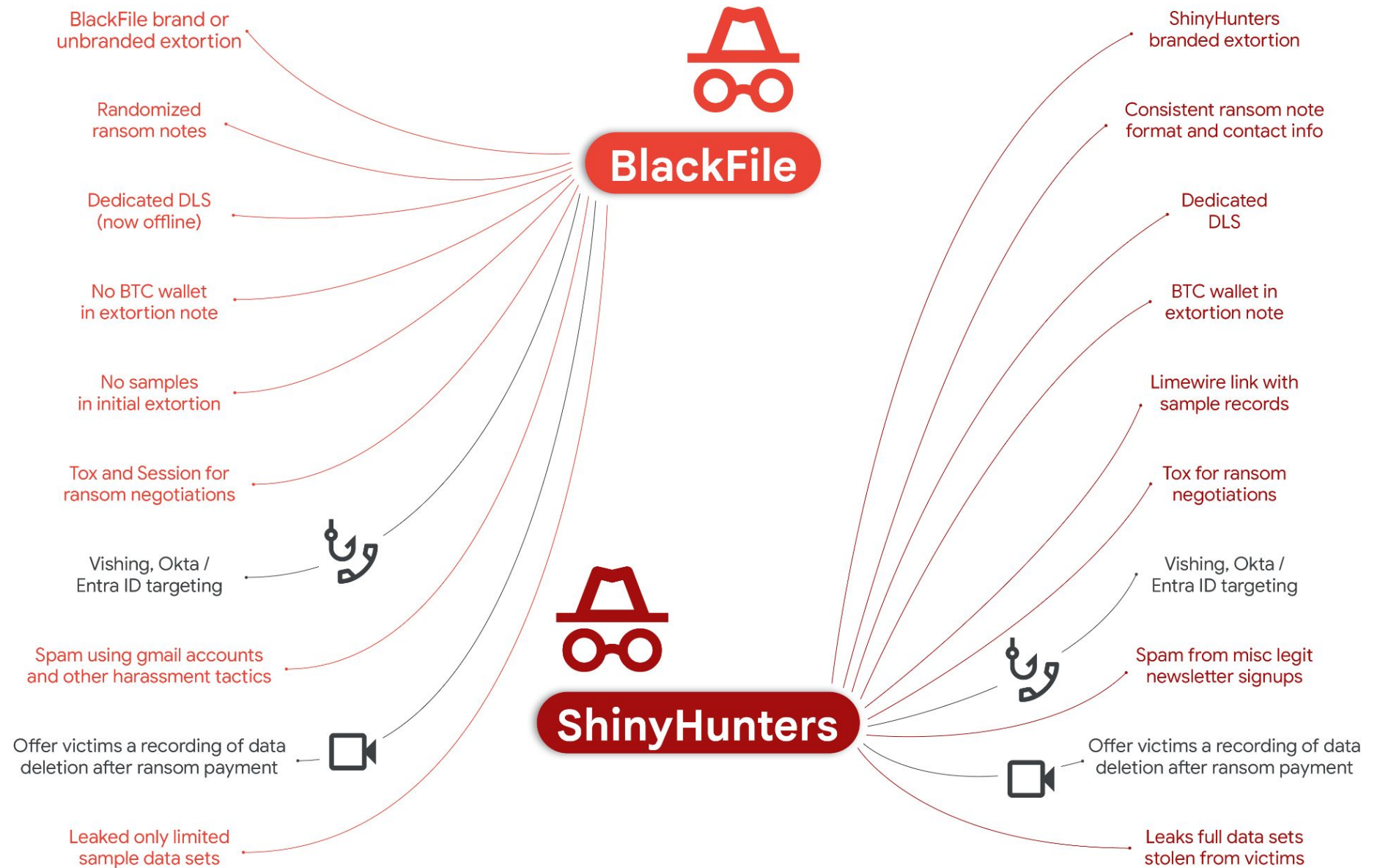
WHAT THEY SHARE Vishing as IT help desk · victim-branded SSO harvesting · live MFA interception · attacker MFA device · PowerShell / scripted SaaS exfiltration · 72-hour extortion deadlines · email spam ·

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



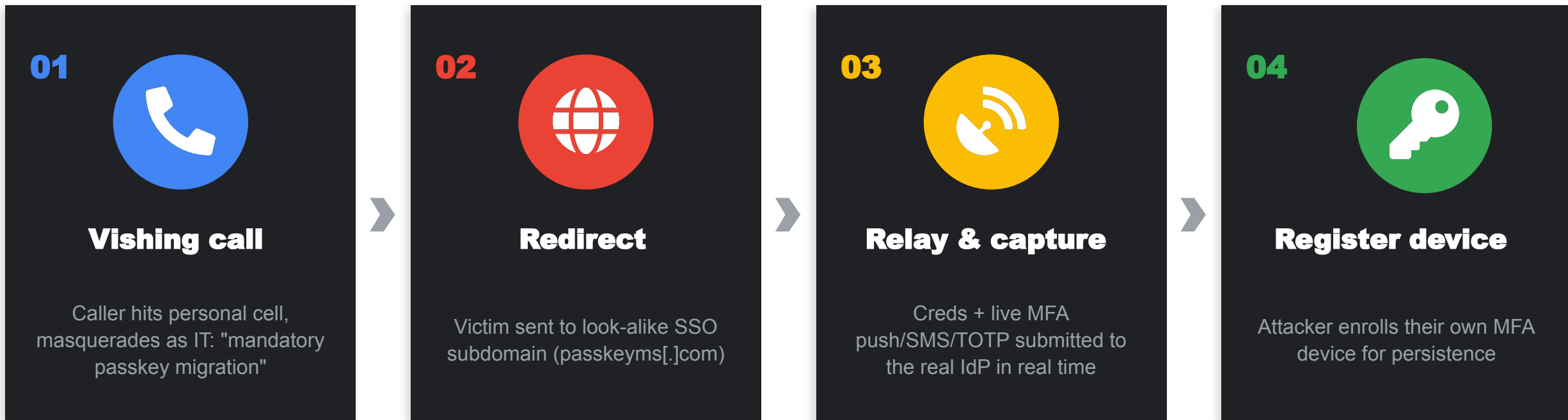
Comparing TTPs





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.



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.

The screenshot shows the homepage of the BlackFile website. At the top, there is a navigation menu with links for 'Homepage', 'Leaks', 'FAQ', 'Deletion', and 'Contact'. The main content area features a large heading 'We are BlackFile' followed by the tagline 'Having poor security comes at a cost.' Below this, a paragraph explains that they are security researchers who identify vulnerabilities in corporate networks and offer companies the chance to protect their data before it is leaked. A link to the 'FAQ' is provided for more information. The footer is divided into three columns: 'WHAT WE DO', 'OUR CODE', and 'TRACK RECORD', each with a brief description of their services and policies.

Homepage Leaks FAQ Deletion Contact

We are BlackFile

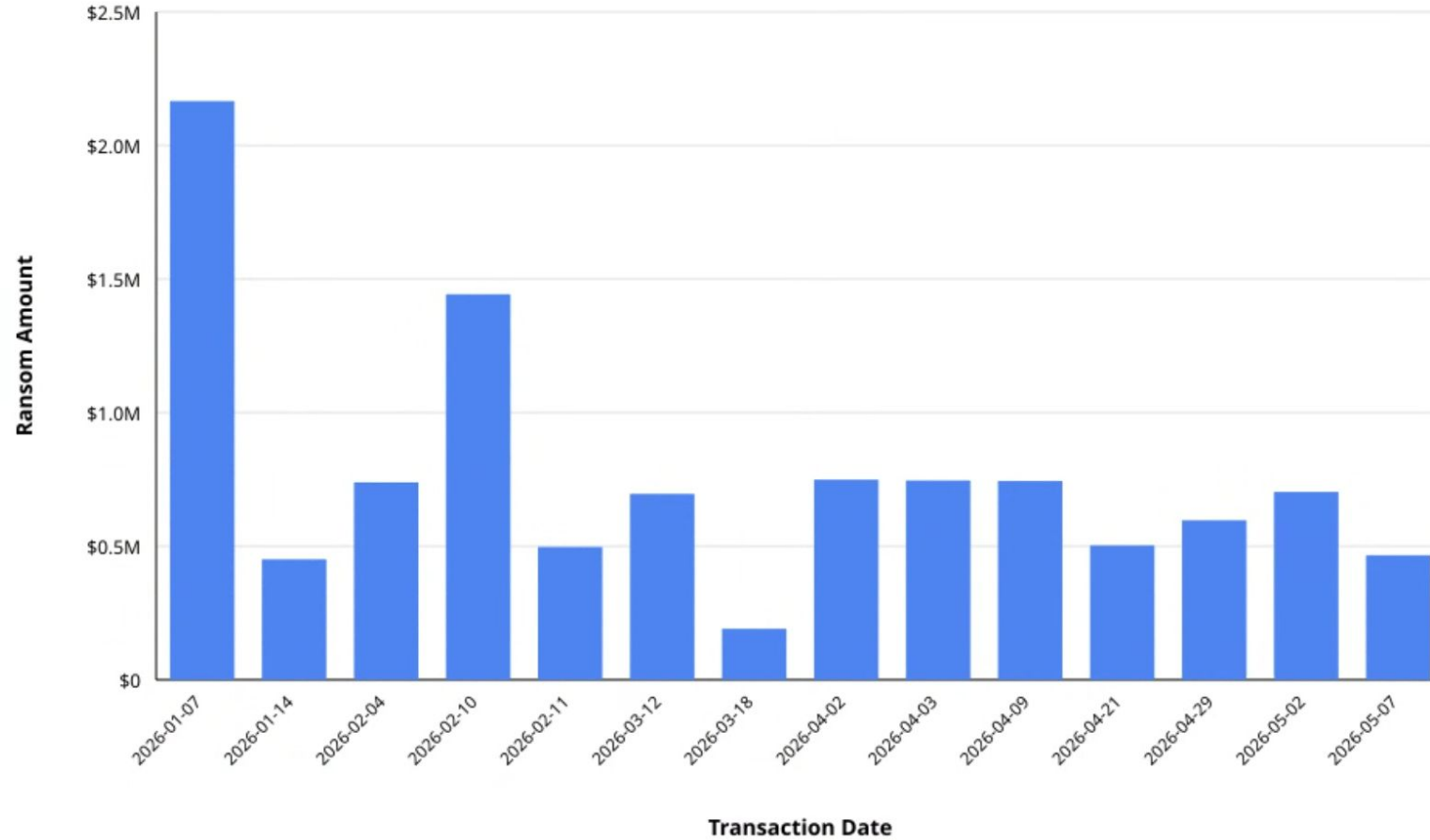
Having poor security comes at a cost.

We are security researchers operating independently. We identify vulnerabilities in corporate networks and give companies the opportunity to protect their data before it becomes public. Read the [FAQ](#) for more information.

- WHAT WE DO
We identify security vulnerabilities in corporate infrastructure. Companies that work with us receive detailed reports. Those that don't have their data published here.
- OUR CODE
We do not do ransomware. We honor all agreements made. All data is permanently deleted once terms are met. We have never broken this promise.
- TRACK RECORD
Every company listed on our blog either ignored us or failed to reach an agreement. We give fair warning and reasonable timelines before publication.




Blackfile Ransom Payments





Blackfile Shuts Down

• FINAL NOTICE




BlackFile is shutting down

OPERATIONS ENDING · THANK YOU

After careful consideration, BlackFile is shutting down. We are no longer operating services, negotiations, or outreach **under this name.**

Our public presence ends and infrastructure will wind down in an orderly way. There were no historical mirrors or archives from this project.

Do not pay anyone who contacts you claiming to represent BlackFile or using our name. We do not endorse payments to third parties and will not ask you for money through unofficial channels.

WHAT THIS MEANS 

CONTACT

This domain or onion endpoint may become unreachable without further notice. Do not expect ongoing support channels.

TIMELINE

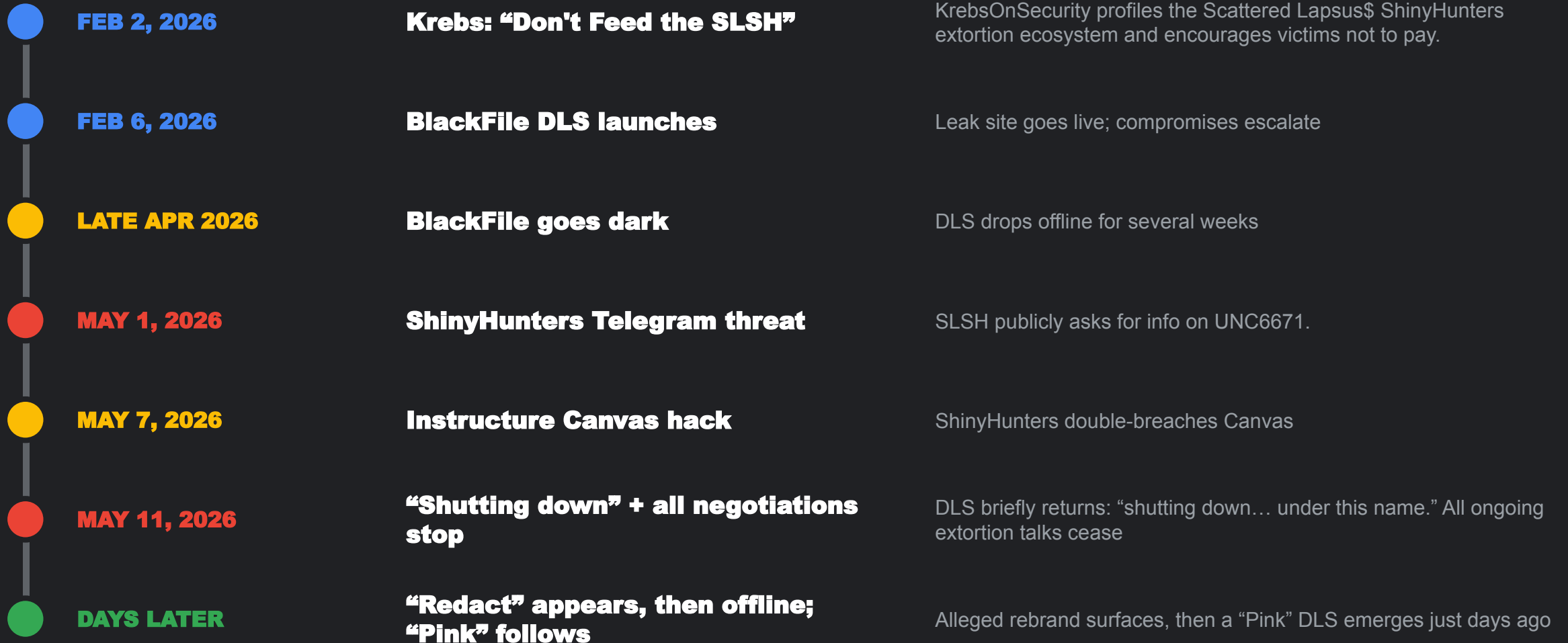
Access may degrade gradually before full discontinuance. Treat any stated date as approximate.

Stay safe.



The Vanishing Act: A Timeline

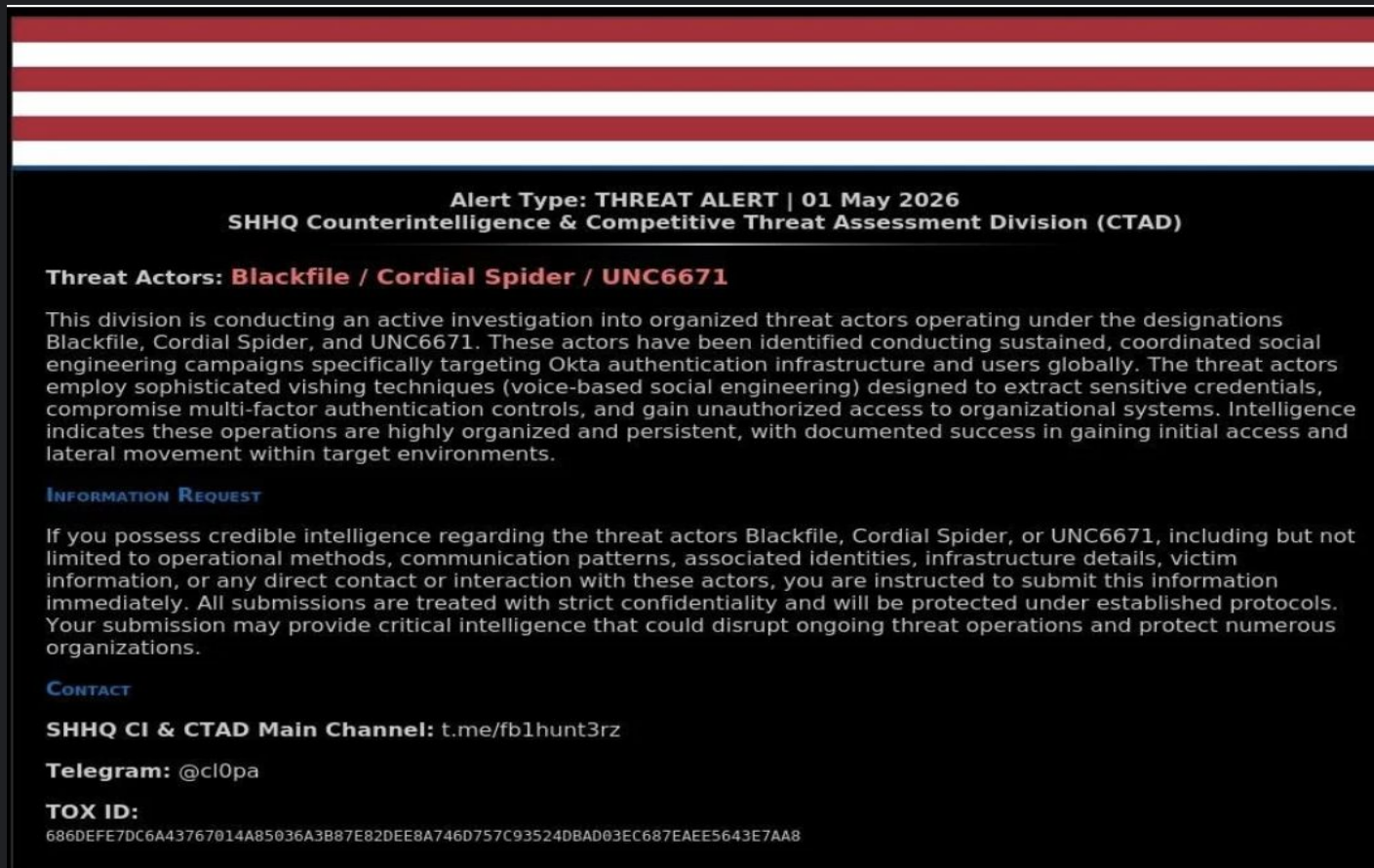
Chaotic disappearance and bizarre resurrection.





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

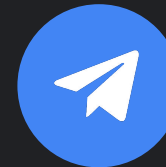
If you possess credible intelligence regarding the threat actors Blackfile, Cordial Spider, or UNC6671, including but not limited to operational methods, communication patterns, associated identities, infrastructure details, victim information, or any direct contact or interaction with these actors, 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:
686DFE7DC6A43767014A85036A3B87E82DEE8A746D757C93524DBAD03EC687EAAE5643E7AA8



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

■ 2026-05-19 04:25 UTC

[REDACT]

> LEAKS [0]

#01 · 2026-05-19 · 81C1B1D2

BLACKFILE OPERATIONAL UPDATE

All operations under the Blackfile name have been officially and permanently ceased as of this post. This is not an exit scam, and all clients who have paid have no need to fear being targeted again by our group under a different name.

We want to make our rebrand known, as we highly value the reputation we have built and aim to be as transparent as possible throughout this change.

All operations will resume under our new name: Redact. We find this name fitting, as we have yet to fully and publicly leak any data belonging to the companies we have targeted who have not paid. Under this rebrand, all collected data will be published.

We will attempt to reach out to each company one last time before their data is uploaded here. For all negotiation firms, our primary Tox address will remain the same, and you can verify it using the PGP key on our profile.



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



THE FEED

What's happening right now.

ANNOUNCEMENTS

Hello, world. My name is Pink.

We've contacted a number of companies whose names are not yet listed here. We believe it is only fair to allow them an opportunity to respond before any further action is taken. We look forward to hearing from those prepared to engage constructively.

Pink is now fully operational.

As of May 31st, 2026, we have decided to operate publicly. If you feel the need to confirm you are actually speaking to us, you are welcome to verify it using the PGP keys listed on our site.

NEW LEAKS

Nothing here yet :(

HEADLINES

Nothing here yet :(