10Alytics
data & strategy

2026

Cyber Threat Intelligence Report

Analyst
Olumide Solanke

Reported on
24 January, 2026

10Alytics
data & strategy

2026

OSINT-Based Threat Intelligence Assessment

Target Organization: TikTok (Primary domain: tiktok.com)

Parent organisation: ByteDance (bytedance.com

Industry Sector: Technology
- Social Media
- Digital Advertising
- E-Commerce Enablement

Confidentiality Notice
This report contains defensive cyber threat intelligence derived exclusively from publicly available open-source information (OSINT). It is prepared strictly for educational and analytical purposes and does not include exploitation, intrusion, or unauthorized access activities.

↘ Executive Summary

Selected organization and industry

This OSINT-based assessment focuses on TikTok (tiktok.com) and its parent company ByteDance (bytedance.com) operating in the Technology / Social Media sector with global users, advertisers, creators, and business partners. TikTok's platform footprint includes web portals, mobile applications, developer services, and business/advertising portals.

Key threats identified

Based on passive OSINT collection and analysis, the most relevant threats are:

- **Phishing & brand impersonation risk (Primary):**

Publicly discoverable login portals and well-known brand identity increase the likelihood of cloned login pages, credential-harvesting, and user/employee impersonation.

- **Email enumeration and spear-phishing enablement:**

Public OSINT sources (e.g., email discovery platforms) indicate substantial availability of employee email patterns and addresses, enabling targeted phishing and business email compromise (BEC) attempts.

- **Attack surface complexity (subdomain sprawl):**

Large numbers of subdomains and service endpoints (including developer and business-related infrastructure) widen the overall exposure footprint and increase opportunities for misconfiguration or third-party abuse—though no direct exploitation was attempted.

- **Reputation & infrastructure posture (Strength):**

Domain reputation checks indicate clean/low-malicious reputation, with significant use of CDN/edge protection, suggesting strong baseline controls.

Overall risk level

Overall Risk Level: Medium

- Technical exposure: Low to Moderate (strong edge protection observed; no obvious exposed services surfaced in this passive review)
- Human-layer/social engineering exposure: Moderate (brand popularity + identifiable email patterns elevate spear-phishing risk)

Business impact

If abused by attackers, likely impacts include:

- Reputational: Loss of trust from users/creators/advertisers due to phishing campaigns impersonating TikTok portals.
- Operational: Account compromise leading to abuse of business portals, ad accounts, creator monetization and support workflows.
- Financial: Fraud losses, advertising account theft, chargebacks, incident response costs.
- Regulatory: Privacy/security incident reporting exposure depending on geography and impacted user data.

Key recommendations (management-ready)

- Implement/validate robust DMARC (enforce), SPF and DKIM across domains; monitor for spoofing attempts.
- Strengthen brand monitoring & takedown capability for look-alike domains and cloned login pages.
- Expand phishing-resistant authentication (FIDO2/WebAuthn) for privileged accounts and employees.
- Continuously monitor certificate transparency and newly registered domains resembling TikTok/ByteDance.
- Run targeted security awareness campaigns focused on credential-harvesting and impersonation threats.

2

Organization Profile

2.1 Organization Overview

- Organization name: TikTok (TikTok Inc. / regional entities), parent: ByteDance
- Industry sector: Technology – Social media, advertising, creator economy, business services
- Geographic presence: Global (consumer and business services with multiple regional portals)
- Core digital services:
  - Public website and content delivery (tiktok.com)
  - Business portals (advertising, merchant/seller, partner tooling)
  - Developer services and APIs (developer portals)
  - Mobile applications (iOS/Android)
  - Support/help center and operational portals

2.2 Digital Footprint Summary

Publicly visible digital assets identified through OSINT methods include:

- Primary domains: tiktok.com, bytedance.com
- Subdomains: High-volume subdomains observed (including developer/business/service endpoints)
- Email infrastructure: Mail exchange records visible via OSINT platforms (no intrusive validation performed)
- Public-facing services: Login portals, business and developer endpoints, content delivery presence
- Social media presence: Strong and globally recognizable brand presence; increases impersonation attractiveness

3

Intelligence Requirements & Scope ↘

3.1 Intelligence Objectives

This assessment aimed to answer:

- Are there OSINT indicators suggesting **phishing or brand impersonation risk** against TikTok/ByteDance?
- Are there publicly discoverable **assets/endpoints** that could support attacker reconnaissance?
- Are there indicators of **data leakage** (e.g., exposed documents, leaked emails—not credentials)?
- What is the **overall risk posture** based on passive OSINT validation?

3.2 Scope & Limitations

- **Passive OSINT only:** No exploitation, intrusion, credential testing, or active scanning.
- **Public sources only:** Search engines, OSINT platforms, public archives, reputation tools.
- **Ethical boundary adherence:** Findings are contextual and defensive; raw sensitive lists are not reproduced.

Methodology & Tools Used

4.1 OSINT Methodology

A standard CTI workflow was applied:

1. Planning & Direction: Define objectives and threat questions (phishing, exposure, leakage).
2. Collection: Gather relevant OSINT from search engines, OSINT platforms, and reputation services.
3. Processing: De-duplicate, categorize, and prioritise signals (identity, infrastructure, reputation, history).
4. Analysis: Assess attacker usability, likelihood, and potential impact; identify defensive gaps.
5. Dissemination: Produce actionable findings, risk ratings, and recommendations.

4.2 Tools Utilized

Google Dorks

- Discovery of indexed login/admin/API strings and exposed file types (PDF, etc.).

theHarvester

- Passive enumeration of hosts/subdomains and associated infrastructure signals.

Hunter.io

- Email pattern discovery and organisational email exposure indicators (high-level only).

VirusTotal

- Domain reputation, DNS relations, passive associations, and vendor consensus.

Shodan

- Visibility of internet-facing services and certificate-based signals (passive review).

Wayback Machine

- Historical snapshots to identify legacy exposure and content evolution.

OSINT Framework

Structured selection of OSINT categories and tooling paths.

5

OSINT Collection Summary

This section describes **what was collected** (relevance-focused), not raw dumps:

Domains & key portals

Primary domains and publicly indexed authentication-related pages.

Subdomain footprint

Large-scale subdomain listings indicating extensive service segmentation.

Email exposure indicators

Publicly accessible evidence of corporate email patterns and employee email availability (not reproduced in bulk).

Reputation & trust signals

Vendor detection consensus and popularity rankings for primary domains.

Historical web evidence

Archived snapshots providing baseline comparison of older site content.

DNS and hosting patterns

CDN/edge protection signals and DNS relationships visible via OSINT platforms.

6

Key Findings & Exposures

6.1 Phishing & Brand Impersonation

Finding 6.1.1 — Publicly discoverable login portals increase cloning risk

- Observation

Search results show multiple **login-related URLs and portals** associated with TikTok services.

- Why this matters

High-traffic login pages are frequently cloned by adversaries for credential harvesting. Even without evidence of a specific active phishing campaign in this dataset, **discoverability + brand strength** increases likelihood of impersonation at scale.

- Risk rating: Medium

Finding 6.1.2 — Email pattern exposure supports spear-phishing

- Observation

OSINT sources indicate large volumes of **employee email addresses** and consistent formatting patterns for TikTok/ByteDance domains.

- Why this matters

Attackers can craft convincing spear-phishing and BEC attempts using real employee identities, titles, and address formats—especially against finance, HR, PR, policy, or vendor management.

- Risk rating: Medium

Key Findings & Exposures

6.2 Infrastructure Exposure

Finding 6.2.1 — Large subdomain footprint increases attack surface complexity

- Observation

Passive enumeration indicates **very high subdomain counts** across tiktok.com and bytedance.com, including developer/service naming conventions.

- Why this matters

Large distributed service landscapes are harder to govern; attackers benefit from increased chance of misconfiguration, orphaned endpoints, or third-party integration weaknesses.

- Risk rating: Medium

Finding 6.2.2 — Strong edge/CDN posture observed (positive control)

- Observation

OSINT strongly suggests extensive use of CDN/edge protection (e.g., Akamai/edge networks) and generally non-exposed direct origin services.

- Why this matters

Edge protection reduces direct exposure, mitigates some volumetric threats, and limits attacker visibility into origin infrastructure.

- Risk rating: Low (protective factor)

Key Findings & Exposures

6.3 Data Leakage Indicators

Finding 6.3.1 — Public PDFs exist (not necessarily sensitive)

- Observation

Public PDF documents related to TikTok/ByteDance are indexed and accessible.

- Why this matters

While many PDFs are legitimate marketing/policy documents, document exposure can occasionally lead to inadvertent metadata leakage (names, internal references, tooling identifiers).

- Risk rating: Low

Finding 6.3.2 — No confirmed credential leak evidence in this dataset

- Observation

- This passive review did not confirm leaked passwords or credential dumps attributable to the target (no breach dataset validation conducted beyond passive indication).

- Why this matters

Reinforces that the key risk here is **social engineering enablement**, not proven credential compromise from this collection.

- Risk rating: Low

7

Threat Analysis & Risk Assessment

7.1 Threat Actor Perspective

From an attacker's viewpoint, the highest-value exploitation path is **human-layer compromise:**

- **Likely attack paths:**

→ 1) Identify legitimate TikTok login/business portals → 2) Clone portal/look-alike pages → 3) Send spear-phishing using real employee identities or branded lures → 4) Capture credentials/session tokens → 5) Abuse compromised accounts (ads, support, creator payouts, admin tooling).

- **Common attacker techniques (MITRE ATT&CK-aligned):**
  - **T1593** Search Open Websites/Domains (discover portals and documents)
  - **T1589** Gather Victim Identity Information (employee identity/email pattern)
  - **T1590** Gather Victim Network Information (subdomains/infrastructure mapping)
  - **T1566** Phishing (delivery mechanism for credential theft / impersonation)

7.1 Threat Actor Perspective

From an attacker's viewpoint, the highest-value exploitation path is **human-layer compromise:**

- **Likely attack paths:**

→ 1) Identify legitimate TikTok login/business portals → 2) Clone portal/look-alike pages → 3) Send spear-phishing using real employee identities or branded lures → 4) Capture credentials/session tokens → 5) Abuse compromised accounts (ads, support, creator payouts, admin tooling).

- **Common attacker techniques (MITRE ATT&CK-aligned):**
  - **T1593** Search Open Websites/Domains (discover portals and documents)
  - **T1589** Gather Victim Identity Information (employee identity/email pattern)
  - **T1590** Gather Victim Network Information (subdomains/infrastructure mapping)
  - **T1566** Phishing (delivery mechanism for credential theft / impersonation)

Threat Analysis & Risk Assessment

7.2 Business Risk Impact

Risk is rated per confirmed finding:

Finding	Risk	Financial	Reputational	Operational	Regulatory
6.1.1 Login portal cloning risk	Medium	Medium	High	Medium	Medium
6.1.2 Email-based spear-phishing enablement	Medium	Medium	Medium	Medium	Medium
6.2.1 Subdomain sprawl complexity	Medium	Medium	Medium	Medium	Low–Medium
6.2.2 Strong edge/CDN posture	Low (positive)	Low	Low	Low	Low
6.3.1 Public PDFs	Low	Low	Low–Medium	Low	Low
6.3.2 No credential leak observed	Low	Low	Low	Low	Low

Overall assessment:

- **Technical posture:** generally strong (edge protection, clean domain reputation).
- **Primary risk:** phishing/impersonation at scale and spear-phishing against staff/partners.

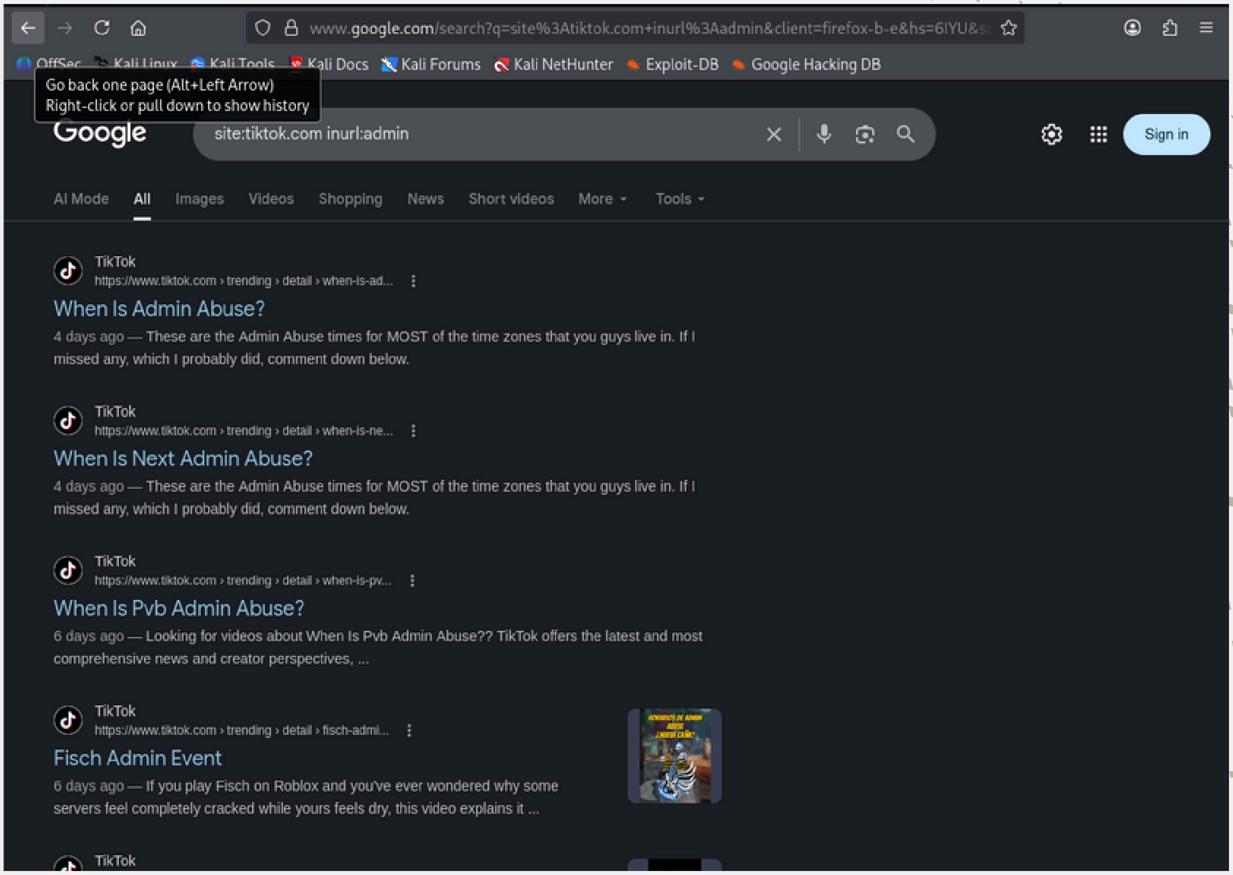
Evidence Log

8

(Screenshots/URLs clearly labeled. No exploitation evidence.)
Note: Evidence items below reference the provided screenshots captured during collection.

Evidence ID	Tool / Source	What it supports	Evidence file (provided)	Timestamp (Capture date)
E1	Google Dorks	Indexed “admin/login/api” search results	T1_GoogleDorks_tiktok_com_inurl_admin_2026-01-23.png	Jan 23, 2026
E2	Google Dorks	Indexed API discovery results	T1_GoogleDorks_tiktok_com_inurl_api_2026-01-23.png	Jan 23, 2026
E3	Google Dorks	Indexed login discovery results	T1_GoogleDorks_tiktok_com_inurl_login_2026-01-23.png	Jan 23, 2026
E4	Google Dorks	Public PDF discovery (tiktok.com/bytedance.com)	T1_GoogleDorks_tiktok_com_filetype_pdf_2026-01-23.png.png / T1_GoogleDorks_bytedance_com_filetype_pdf_2026-01-23.png	Jan 23, 2026
E5	theHarvester	TikTok/ByteDance hosts/subdomains output	T2_theHarvester_tiktok_com_b_all_terminal_subdomains_2026-01-23.png / T2_theHarvester_bytedance_com_b_all_terminal_2026-01-23.png	Jan 23, 2026
E6	Hunter.io	Email exposure indicators + patterns	T4_hunter_io_tiktok_com_domain_search_2026-01-23.png / T4_hunter_io_bytedance_com_domain_search_2026-01-23.png	Jan 23, 2026
E7	Wayback Machine	Historical snapshot for comparison	T5_wayback_machine_tiktok_com_2019_2026-01-24.png	Jan 24, 2026
E8	VirusTotal	Domain reputation/details (clean consensus)	T6_virus_total_tiktok_com_detection_2026_01_24.png / T6_virus_total_tiktok_com_details_2026_01_24.png	Jan 24, 2026
E9	VirusTotal	DNS relations + subdomain relations	T6_virus_total_tiktok_com_relations_dns_2026_01_24.png / T6_virus_total_tiktok_com_relations_subdomain_2026_01_24.png	Jan 24, 2026
E10	OSINT Framework	Method selection rationale	T7_OSINTframework_tiktok_com_domain_category_2026_01_24.png / T7_OSINTframework_tiktok_com_email_category_2026_01_24.png / T7_OSINTframework_tiktok_com_network_category_2026_01_24.png	Jan 24, 2026

Evidence Log


www.google.com/search?q=site%3Atiktok.com+inurl%3Aadmin&client=firefox-b-e&hs=6IYU&s
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Go back one page (Alt+Left Arrow)
Right-click or pull down to show history
Google
site:tiktok.com inurl:admin
Sign in
AI Mode
All
Images
Videos
Shopping
News
Short videos
More
Tools

TikTok
https://www.tiktok.com › trending › detail › when-is-ad...

When Is Admin Abuse?

4 days ago — These are the Admin Abuse times for MOST of the time zones that you guys live in. If I missed any, which I probably did, comment down below.

TikTok
https://www.tiktok.com › trending › detail › when-is-ne...

When Is Next Admin Abuse?

4 days ago — These are the Admin Abuse times for MOST of the time zones that you guys live in. If I missed any, which I probably did, comment down below.

TikTok
https://www.tiktok.com › trending › detail › when-is-pv...

When Is Pvb Admin Abuse?

6 days ago — Looking for videos about When Is Pvb Admin Abuse?? TikTok offers the latest and most comprehensive news and creator perspectives, ...

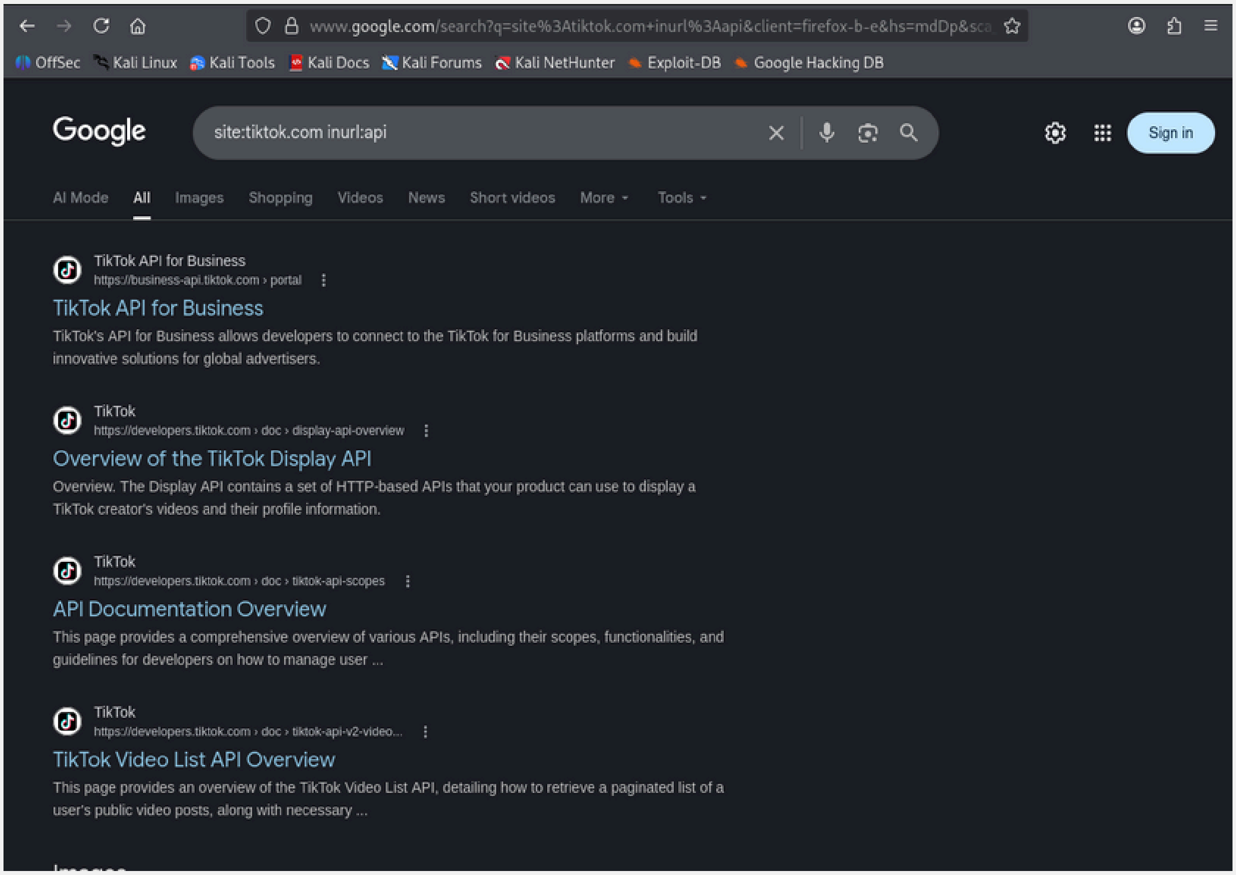
TikTok
https://www.tiktok.com › trending › detail › fisch-admi...

Fisch Admin Event

6 days ago — If you play Fisch on Roblox and you've ever wondered why some servers feel completely cracked while yours feels dry, this video explains it ...

TikTok

E1 - Google Dorks Indexed “admin/login/api” search results



TikTok API for Business
https://business-api.tiktok.com › portal

TikTok API for Business

TikTok's API for Business allows developers to connect to the TikTok for Business platforms and build innovative solutions for global advertisers.

TikTok
https://developers.tiktok.com › doc › display-api-overview

Overview of the TikTok Display API

Overview. The Display API contains a set of HTTP-based APIs that your product can use to display a TikTok creator's videos and their profile information.

TikTok
https://developers.tiktok.com › doc › tiktok-api-scopes

API Documentation Overview

This page provides a comprehensive overview of various APIs, including their scopes, functionalities, and guidelines for developers on how to manage user ...

TikTok
https://developers.tiktok.com › doc › tiktok-api-v2-video...

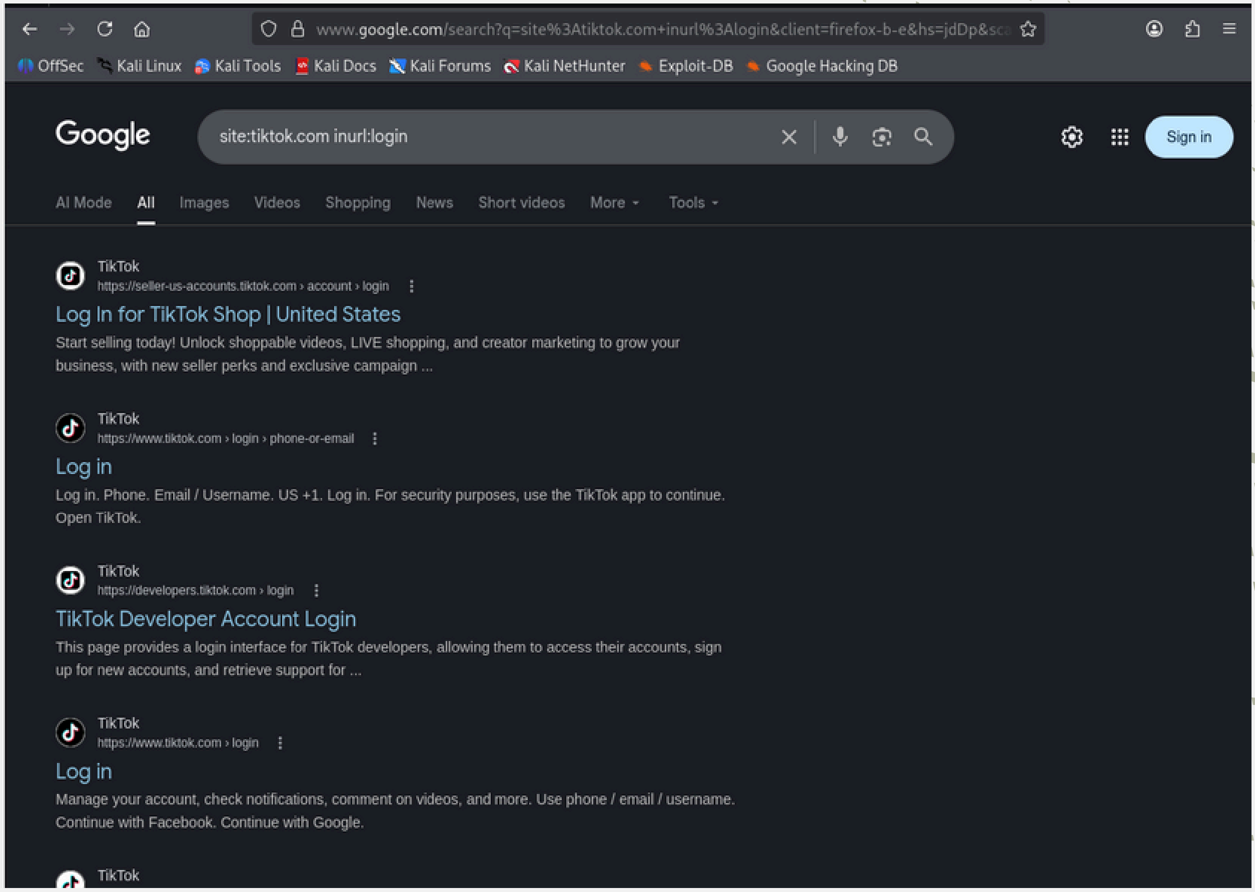
TikTok Video List API Overview

This page provides an overview of the TikTok Video List API, detailing how to retrieve a paginated list of a user's public video posts, along with necessary ...

Images

E2 - Google Dorks Indexed API discovery results

Evidence Log



www.google.com/search?q=site%3Atiktok.com+inurl%3Alogin&client=firefox-b-e&hs=jdDp&sca

site:tiktok.com inurl:login

TikTok
https://seller-us-accounts.tiktok.com › account › login
Log In for TikTok Shop | United States
Start selling today! Unlock shoppable videos, LIVE shopping, and creator marketing to grow your business, with new seller perks and exclusive campaign ...

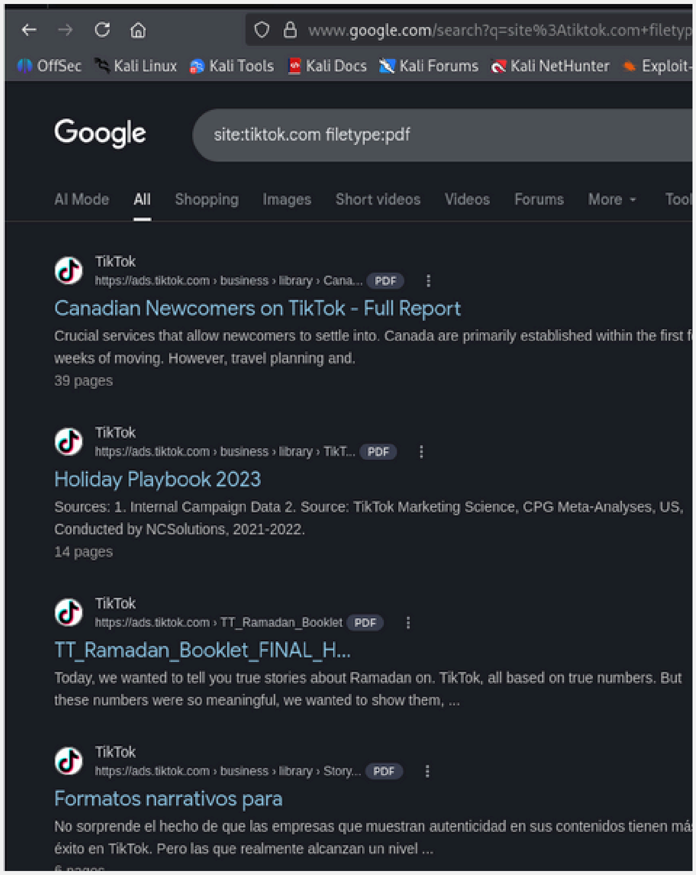
TikTok
https://www.tiktok.com › login › phone-or-email
Log in
Log in. Phone. Email / Username. US +1. Log in. For security purposes, use the TikTok app to continue. Open TikTok.

TikTok
https://developers.tiktok.com › login
TikTok Developer Account Login
This page provides a login interface for TikTok developers, allowing them to access their accounts, sign up for new accounts, and retrieve support for ...

TikTok
https://www.tiktok.com › login
Log in
Manage your account, check notifications, comment on videos, and more. Use phone / email / username. Continue with Facebook. Continue with Google.

TikTok

E3 – Google Dorks Indexed login discovery results



www.google.com/search?q=site%3Atiktok.com+filetyp

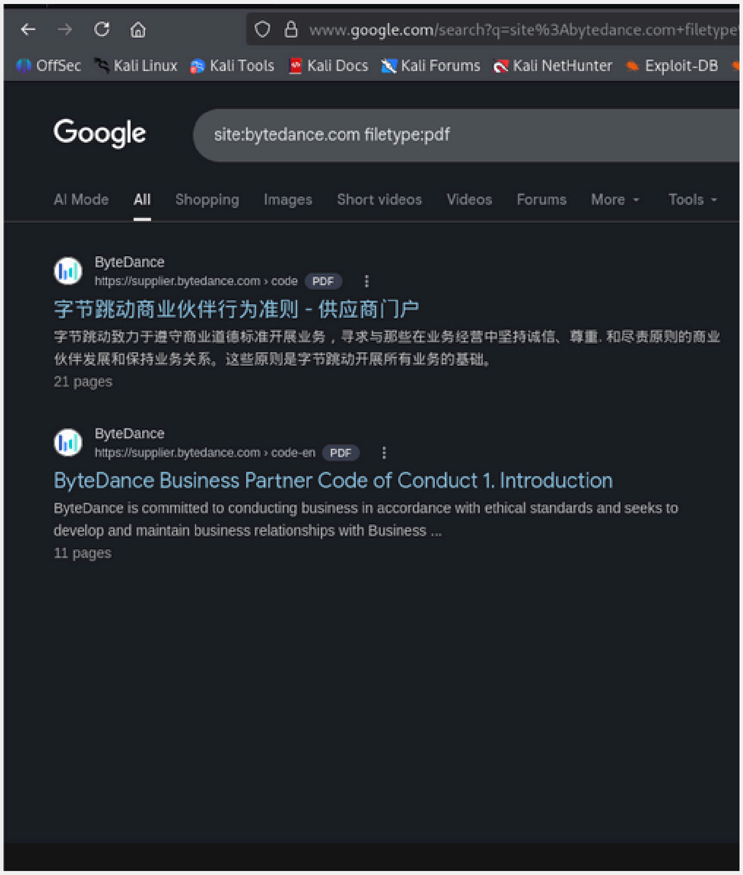
site:tiktok.com filetype:pdf

TikTok
https://ads.tiktok.com › business › library › Cana... PDF
Canadian Newcomers on TikTok - Full Report
Crucial services that allow newcomers to settle into. Canada are primarily established within the first f weeks of moving. However, travel planning and.
39 pages

TikTok
https://ads.tiktok.com › business › library › TikT... PDF
Holiday Playbook 2023
Sources: 1. Internal Campaign Data 2. Source: TikTok Marketing Science, CPG Meta-Analyses, US, Conducted by NCSolutions, 2021-2022.
14 pages

TikTok
https://ads.tiktok.com › TT_Ramadan_Booklet PDF
TT_Ramadan_Booklet_FINAL_H...
Today, we wanted to tell you true stories about Ramadan on. TikTok, all based on true numbers. But these numbers were so meaningful, we wanted to show them, ...

TikTok
https://ads.tiktok.com › business › library › Story... PDF
Formatos narrativos para
No sorprende el hecho de que las empresas que muestran autenticidad en sus contenidos tienen má éxito en TikTok. Pero las que realmente alcanzan un nivel ...
6 pages



www.google.com/search?q=site%3Abytedance.com+filetype

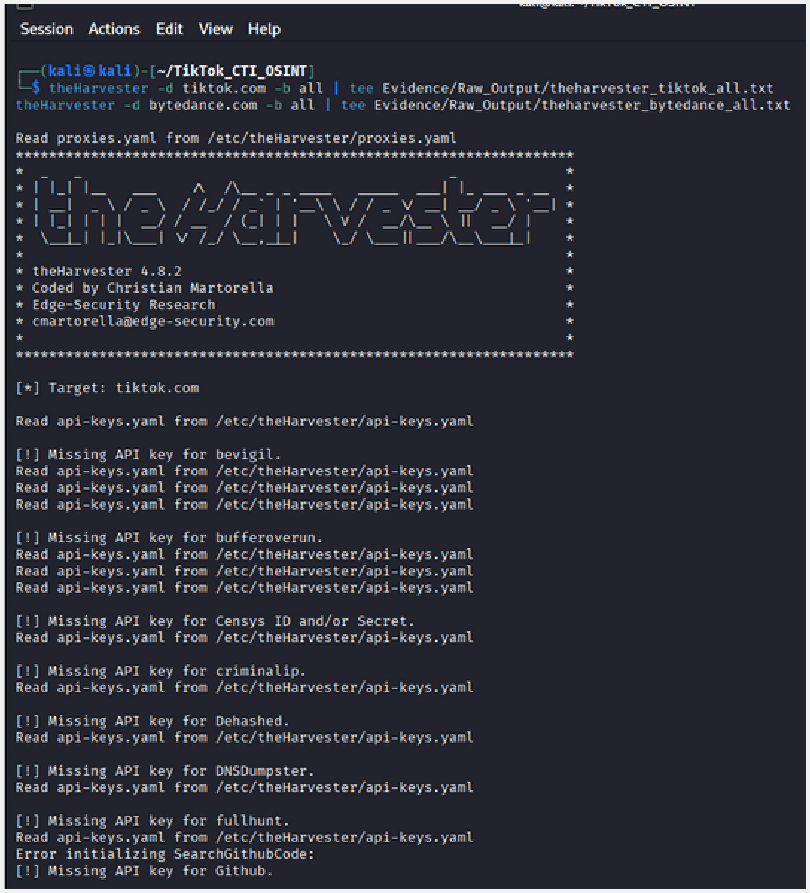
site:bytedance.com filetype:pdf

ByteDance
https://supplier.bytedance.com › code PDF
字节跳动商业伙伴行为准则 - 供应商门户
字节跳动致力于遵守商业道德标准开展业务，寻求与那些在业务经营中坚持诚信、尊重. 和尽责原则的商业伙伴发展和保持业务关系。这些原则是字节跳动开展所有业务的基础。
21 pages

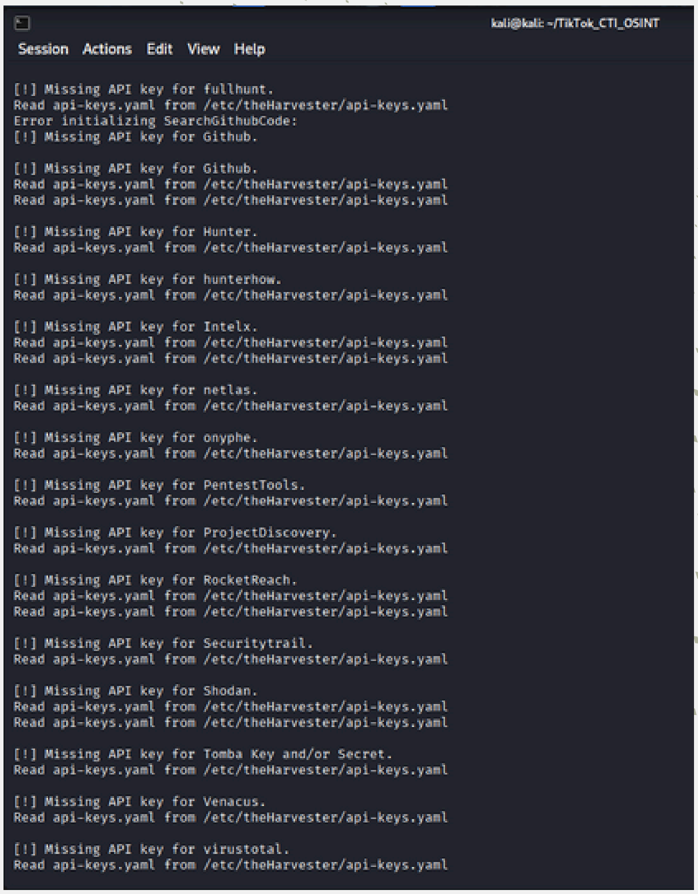
ByteDance
https://supplier.bytedance.com › code-en PDF
ByteDance Business Partner Code of Conduct 1. Introduction
ByteDance is committed to conducting business in accordance with ethical standards and seeks to develop and maintain business relationships with Business ...
11 pages

E4 – Google Dorks Public PDF discovery (tiktok.com/bytedance.com)

Evidence Log

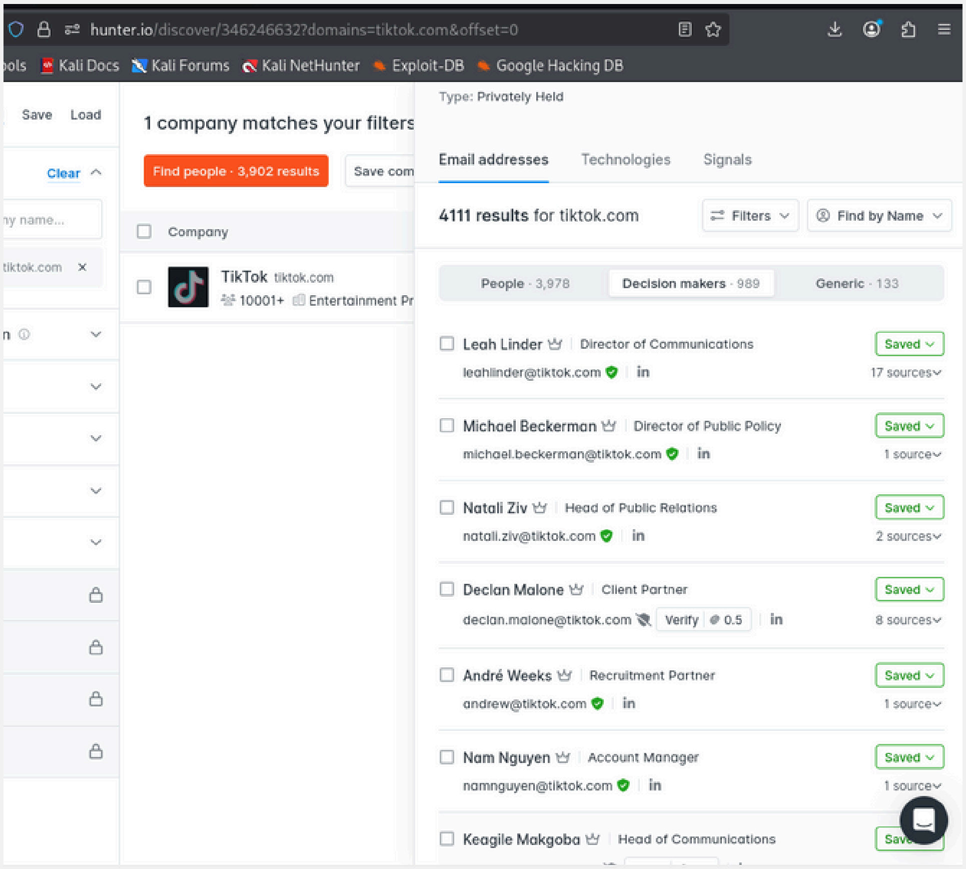


```
┌──(kali㉿kali)-[~/TikTok_CTI_OSINT]
└─$ theHarvester -d tiktok.com -b all | tee Evidence/Raw_Output/theharvester_tiktok_all.txt
theHarvester -d bytedance.com -b all | tee Evidence/Raw_Output/theharvester_bytedance_all.txt

Read proxies.yaml from /etc/theHarvester/proxies.yaml
*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 4.8.2                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************

[*] Target: tiktok.com

Read api-keys.yaml from /etc/theHarvester/api-keys.yaml

[!] Missing API key for bevigil.
Read api-keys.yaml from /etc/theHarvester/api-keys.yaml
Read api-keys.yaml from /etc/theHarvester/api-keys.yaml
Read api-keys.yaml from /etc/theHarvester/api-keys.yaml

[!] Missing API key for bufferoverun.
Read api-keys.yaml from /etc/theHarvester/api-keys.yaml
Read api-keys.yaml from /etc/theHarvester/api-keys.yaml
Read api-keys.yaml from /etc/theHarvester/api-keys.yaml

[!] Missing API key for Censys ID and/or Secret.
Read api-keys.yaml from /etc/theHarvester/api-keys.yaml

[!] Missing API key for criminalip.
Read api-keys.yaml from /etc/theHarvester/api-keys.yaml

[!] Missing API key for Dehashed.
Read api-keys.yaml from /etc/theHarvester/api-keys.yaml

[!] Missing API key for DNSDumpster.
Read api-keys.yaml from /etc/theHarvester/api-keys.yaml

[!] Missing API key for fullhunt.
Read api-keys.yaml from /etc/theHarvester/api-keys.yaml
Error initializing SearchGithubCode:
[!] Missing API key for Github.
```



```
[!] Missing API key for fullhunt.
Read api-keys.yaml from /etc/theHarvester/api-keys.yaml
Error initializing SearchGithubCode:
[!] Missing API key for Github.

[!] Missing API key for Github.
Read api-keys.yaml from /etc/theHarvester/api-keys.yaml
Read api-keys.yaml from /etc/theHarvester/api-keys.yaml

[!] Missing API key for Hunter.
Read api-keys.yaml from /etc/theHarvester/api-keys.yaml

[!] Missing API key for hunterhow.
Read api-keys.yaml from /etc/theHarvester/api-keys.yaml

[!] Missing API key for Intelx.
Read api-keys.yaml from /etc/theHarvester/api-keys.yaml
Read api-keys.yaml from /etc/theHarvester/api-keys.yaml

[!] Missing API key for netlas.
Read api-keys.yaml from /etc/theHarvester/api-keys.yaml

[!] Missing API key for onyphe.
Read api-keys.yaml from /etc/theHarvester/api-keys.yaml

[!] Missing API key for PentestTools.
Read api-keys.yaml from /etc/theHarvester/api-keys.yaml

[!] Missing API key for ProjectDiscovery.
Read api-keys.yaml from /etc/theHarvester/api-keys.yaml

[!] Missing API key for RocketReach.
Read api-keys.yaml from /etc/theHarvester/api-keys.yaml
Read api-keys.yaml from /etc/theHarvester/api-keys.yaml

[!] Missing API key for Securitytrail.
Read api-keys.yaml from /etc/theHarvester/api-keys.yaml

[!] Missing API key for Shodan.
Read api-keys.yaml from /etc/theHarvester/api-keys.yaml
Read api-keys.yaml from /etc/theHarvester/api-keys.yaml

[!] Missing API key for Tomba Key and/or Secret.
Read api-keys.yaml from /etc/theHarvester/api-keys.yaml

[!] Missing API key for Venacus.
Read api-keys.yaml from /etc/theHarvester/api-keys.yaml

[!] Missing API key for virustotal.
Read api-keys.yaml from /etc/theHarvester/api-keys.yaml
```

E5 – theHarvester TikTok/ByteDance hosts/subdomains output



1 company matches your filters

□ TikTok tiktok.com
10001+ Entertainment Pr

Type: Privately Held

4111 results for tiktok.com

People · 3,978 | Decision makers · 989 | Generic · 133

□ Leah Linder | Director of Communications — Saved
leahlinder@tiktok.com | in — 17 sources

□ Michael Beckerman | Director of Public Policy — Saved
michael.beckerman@tiktok.com | in — 1 source

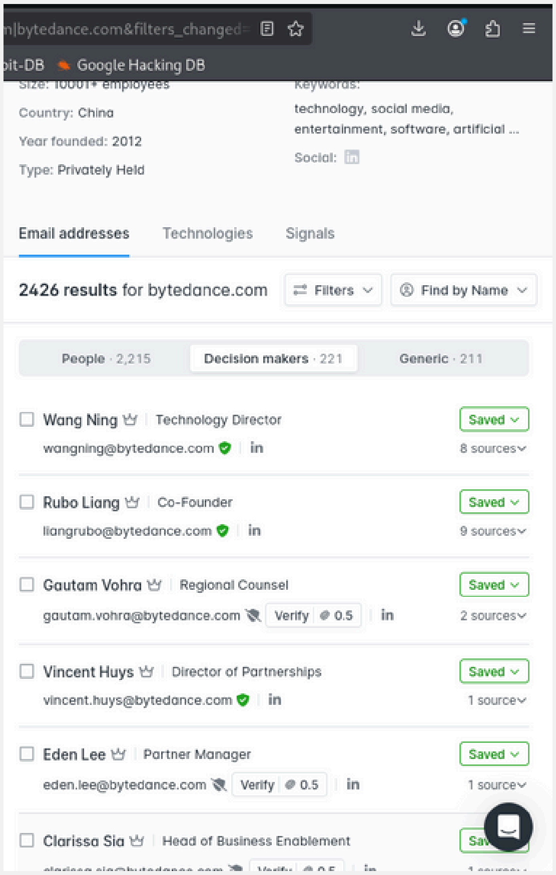
□ Natali Ziv | Head of Public Relations — Saved
natali.ziv@tiktok.com | in — 2 sources

□ Declan Malone | Client Partner — Saved
declan.malone@tiktok.com Verify 0.5 | in — 8 sources

□ André Weeks | Recruitment Partner — Saved
andrew@tiktok.com | in — 1 source

□ Nam Nguyen | Account Manager — Saved
namnguyen@tiktok.com | in — 1 source

□ Keagile Makgoba | Head of Communications — Save



Size: 10001+ employees
Country: China
Year founded: 2012
Type: Privately Held

Keywords:
technology, social media, entertainment, software, artificial ...
Social:

2426 results for bytedance.com

People · 2,215 | Decision makers · 221 | Generic · 211

□ Wang Ning | Technology Director — Saved
wangning@bytedance.com | in — 8 sources

□ Rubo Liang | Co-Founder — Saved
liangrubo@bytedance.com | in — 9 sources

□ Gautam Vohra | Regional Counsel — Saved
gautam.vohra@bytedance.com Verify 0.5 | in — 2 sources

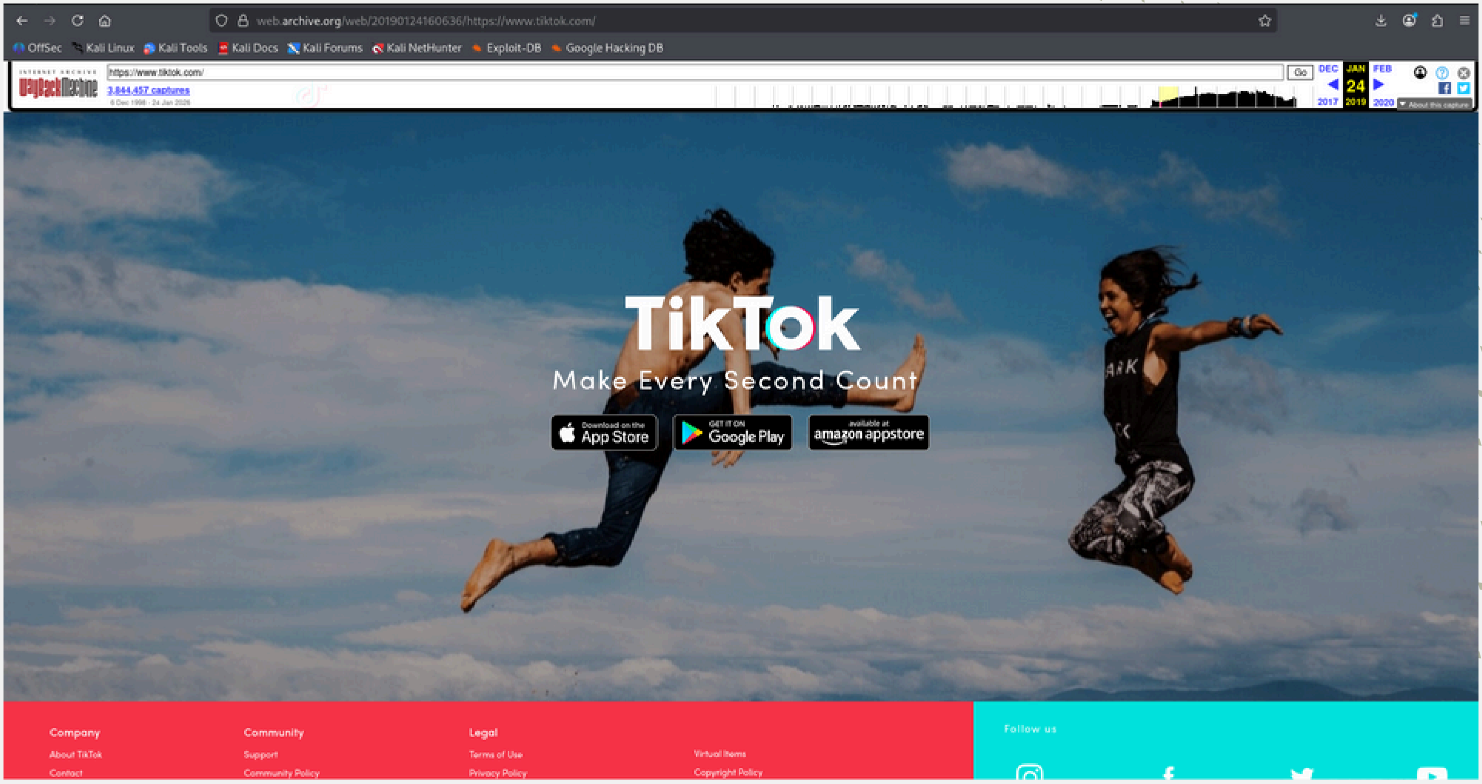
□ Vincent Huys | Director of Partnerships — Saved
vincent.huys@bytedance.com | in — 1 source

□ Eden Lee | Partner Manager — Saved
eden.lee@bytedance.com Verify 0.5 | in — 1 source

□ Clarissa Sia | Head of Business Enablement — Sav

E6 – Hunter.io Email exposure indicators + patterns

Evidence Log



web.archive.org/web/20190124160636/https://www.tiktok.com/

Company
About TikTok
Contact

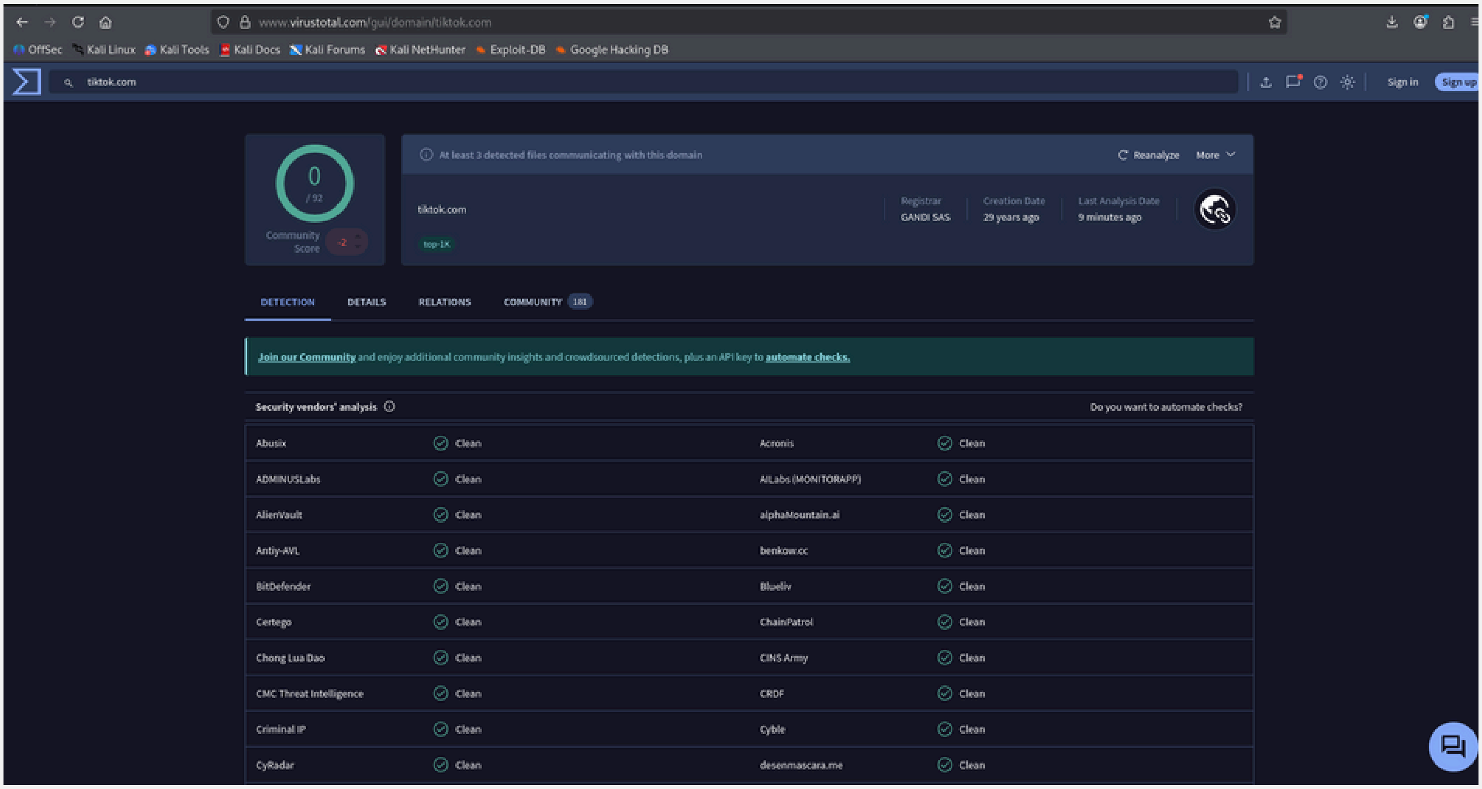
Community
Support
Community Policy

Legal
Terms of Use
Privacy Policy

Virtual Items
Copyright Policy

Follow us

E7 - Wayback Machine Historical snapshot for comparison



www.virustotal.com/gui/domain/tiktok.com

0 / 92

Community Score -2

At least 3 detected files communicating with this domain

tiktok.com

top-1K

Registrar: GANDI SAS

Creation Date: 29 years ago

Last Analysis Date: 9 minutes ago

DETECTION DETAILS RELATIONS COMMUNITY 181

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

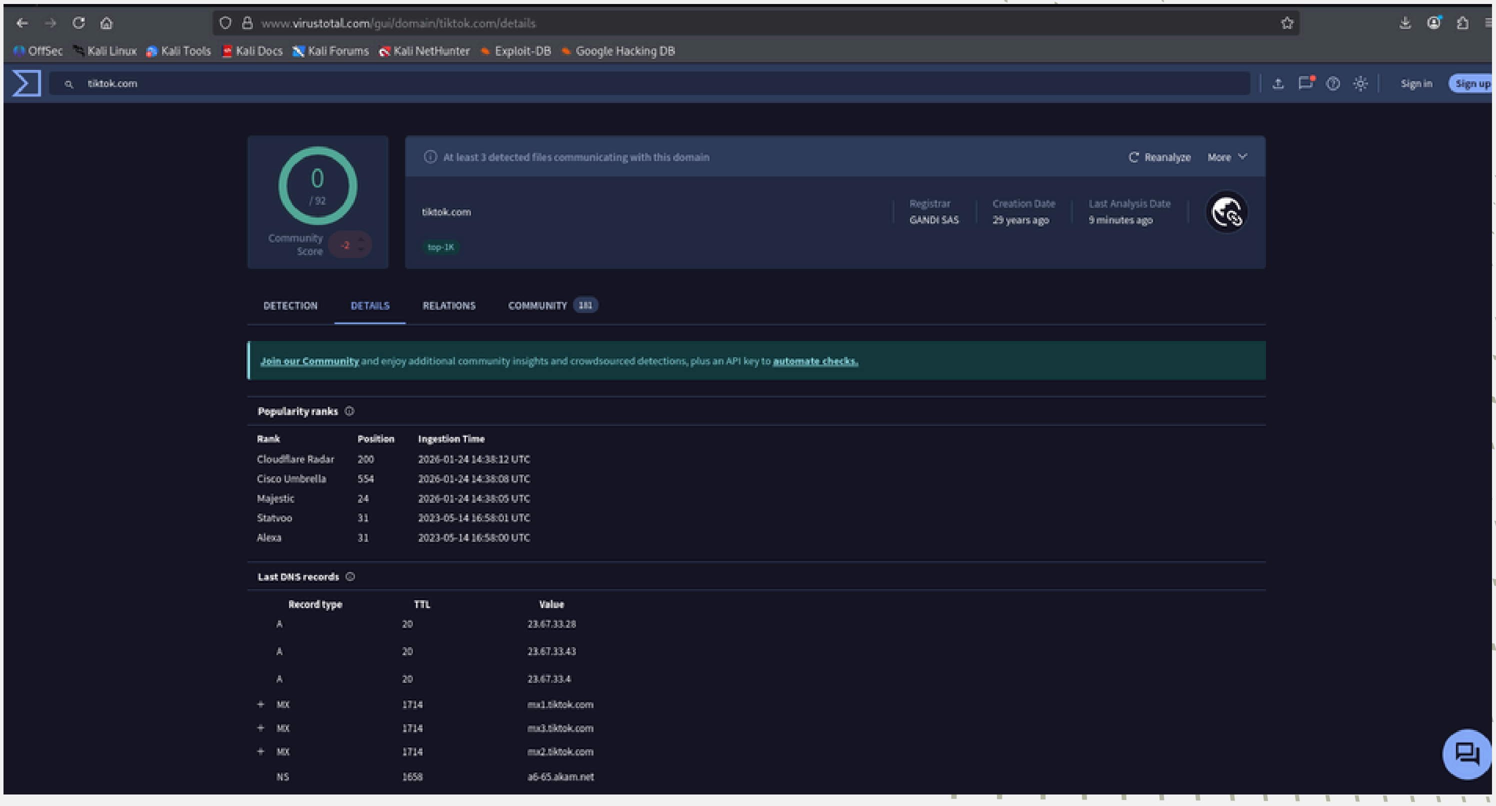
Security vendors' analysis

Do you want to automate checks?

Abusix	✓ Clean	Acronis	✓ Clean
ADMINUSLabs	✓ Clean	AILabs (MONITORAPP)	✓ Clean
AlienVault	✓ Clean	alphaMountain.ai	✓ Clean
Antiy-AVL	✓ Clean	benkow.cc	✓ Clean
BitDefender	✓ Clean	Blueliv	✓ Clean
Certego	✓ Clean	ChainPatrol	✓ Clean
Chong Lua Dao	✓ Clean	CINS Army	✓ Clean
CMC Threat Intelligence	✓ Clean	CRDF	✓ Clean
Criminal IP	✓ Clean	Cyble	✓ Clean
CyRadar	✓ Clean	desenmascara.me	✓ Clean

E8 - VirusTotal Domain reputation/details (clean consensus)

Evidence Log



At least 3 detected files communicating with this domain

tiktok.com

top-1K

Registrar	Creation Date	Last Analysis Date
GANDI SAS	29 years ago	9 minutes ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

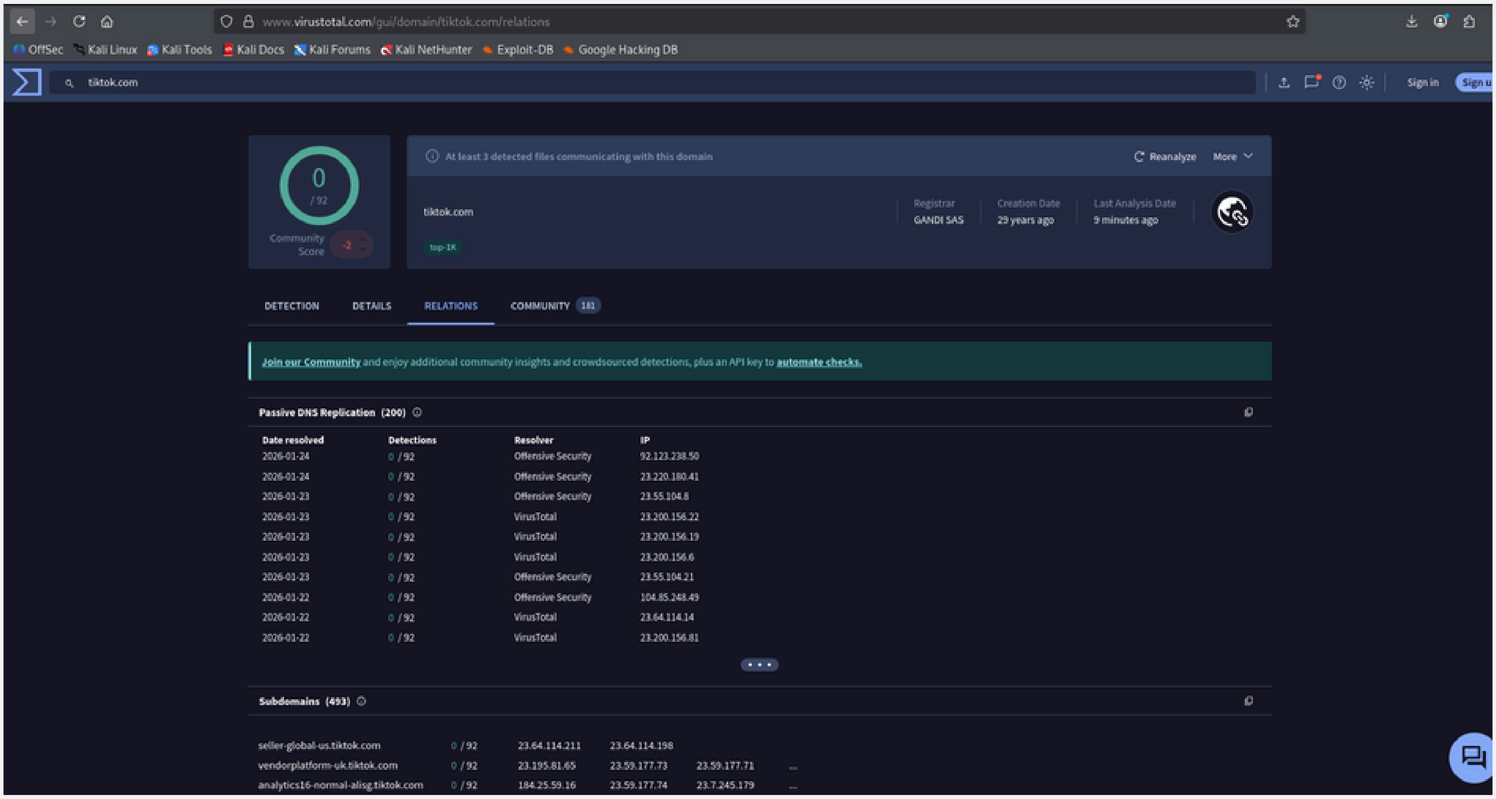
Popularity ranks

Rank	Position	Ingestion Time
Cloudflare Radar	200	2026-01-24 14:38:12 UTC
Cisco Umbrella	554	2026-01-24 14:38:08 UTC
Majestic	24	2026-01-24 14:38:05 UTC
Statvoo	31	2023-05-14 16:58:01 UTC
Alexa	31	2023-05-14 16:58:00 UTC

Last DNS records

	Record type	TTL	Value
	A	20	23.67.33.28
	A	20	23.67.33.43
	A	20	23.67.33.4
+	MX	1714	mx1.tiktok.com
+	MX	1714	mx3.tiktok.com
+	MX	1714	mx2.tiktok.com
	NS	1658	a6-65.akam.net

E8 – VirusTotal Domain reputation/details (clean consensus)



At least 3 detected files communicating with this domain

tiktok.com

top-1K

Registrar	Creation Date	Last Analysis Date
GANDI SAS	29 years ago	9 minutes ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Passive DNS Replication (200)

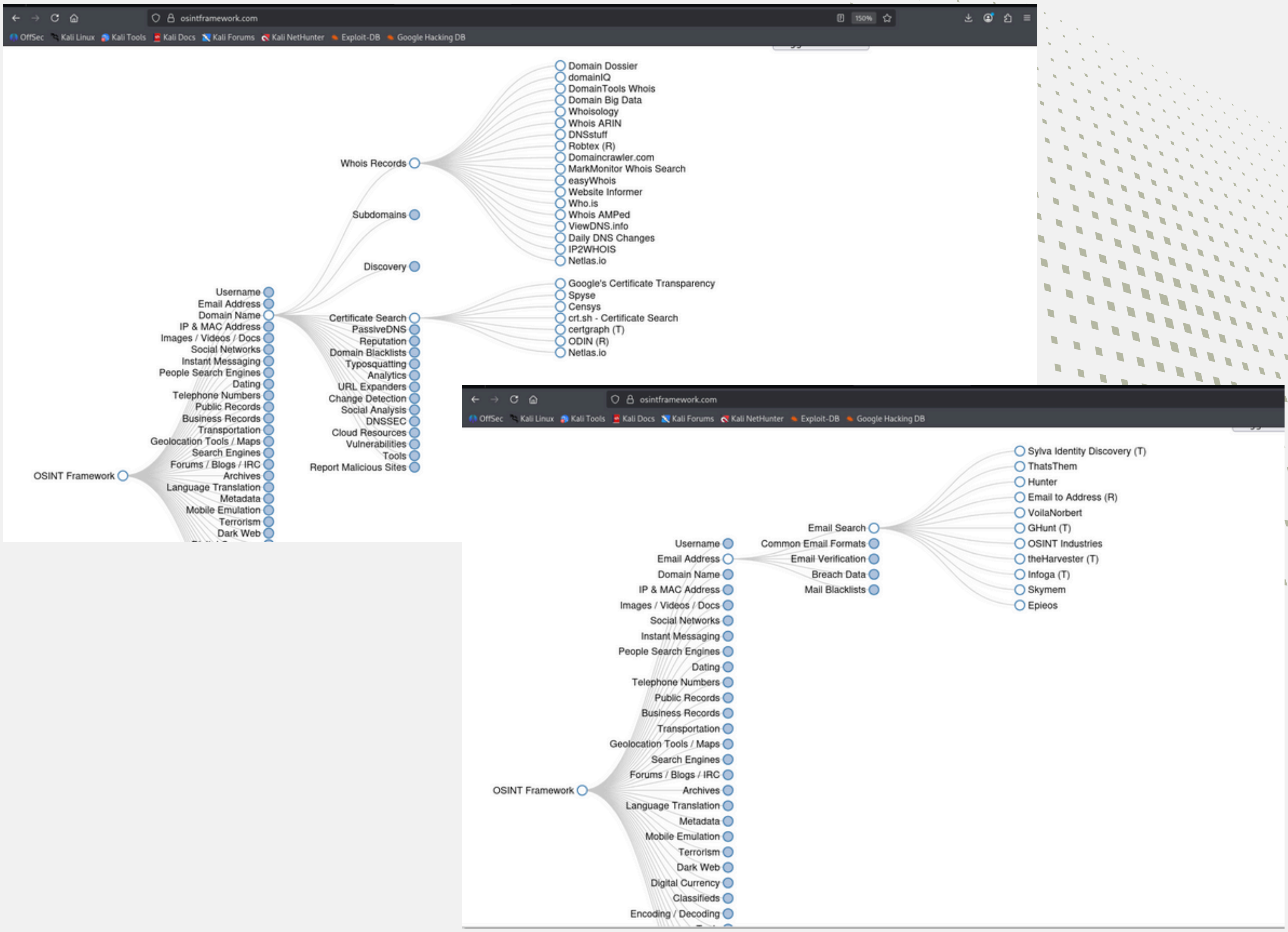
Date resolved	Detections	Resolver	IP
2026-01-24	0 / 92	Offensive Security	92.123.238.50
2026-01-24	0 / 92	Offensive Security	23.220.180.41
2026-01-23	0 / 92	Offensive Security	23.55.104.8
2026-01-23	0 / 92	VirusTotal	23.200.156.22
2026-01-23	0 / 92	VirusTotal	23.200.156.19
2026-01-23	0 / 92	VirusTotal	23.200.156.6
2026-01-23	0 / 92	Offensive Security	23.55.104.21
2026-01-22	0 / 92	Offensive Security	104.85.248.49
2026-01-22	0 / 92	VirusTotal	23.64.114.14
2026-01-22	0 / 92	VirusTotal	23.200.156.81

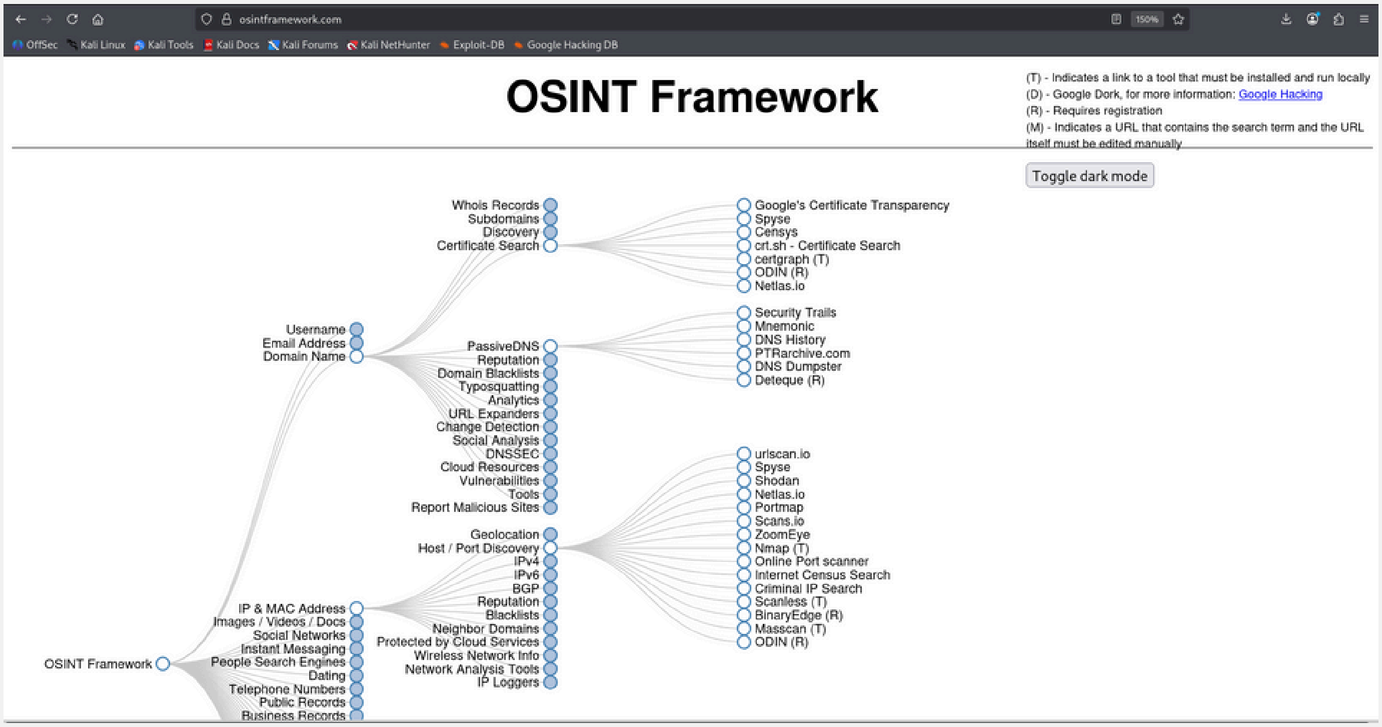
Subdomains (493)

seller-global-us.tiktok.com	0 / 92	23.64.114.211	23.64.114.198		
vendorplatform-uk.tiktok.com	0 / 92	23.195.81.65	23.59.177.73	23.59.177.71	...
analytics16-normal-alisg.tiktok.com	0 / 92	184.25.59.16	23.59.177.74	23.7.245.179	...

E9 – VirusTotal DNS relations + subdomain relations

Evidence Log





OSINT Framework

(T) - Indicates a link to a tool that must be installed and run locally
(D) - Google Dork, for more information: Google Hacking
(R) - Requires registration
(M) - Indicates a URL that contains the search term and the URL itself must be edited manually

E10 – OSINT Framework

Method selection rationale

Mitigation & Recommendations

9

(Actionable guidance mapped to findings.)

For 6.1 Phishing & Impersonation

- Enforce DMARC with a strong policy (move toward p=reject where feasible) and monitor reports.
- Maintain strict SPF/DKIM hygiene across TikTok and ByteDance mail domains and subdomains.
- Deploy/expand brand protection monitoring (look-alike domains, CT logs, app store impersonation).
- Provide a clear and public "official domains & login URLs" page to reduce user confusion.

For 6.2 Attack Surface Complexity

- Maintain rigorous subdomain governance: ownership, lifecycle, TLS policy, and decommissioning controls.
- Continuously monitor for orphaned endpoints, misconfigured cloud resources, and stale DNS entries.
- Use certificate transparency monitoring to detect rogue/typosquat certificates early.
- For 6.3 Document Exposure & Metadata
- Apply document publication controls: metadata scrubbing, classification checks, and content review.
- Implement automated checks to detect sensitive strings in published documents (internal hostnames, email lists, tooling).
- Continuous Monitoring (Strategic)
- Adopt routine OSINT monitoring for:
- Newly registered look-alike domains
- Phishing kits/cloned portals
- Employee impersonation campaigns
- Reputation changes (domain/IP associations)

For 6.3 Document Exposure & Metadata

- Apply document publication controls: metadata scrubbing, classification checks, and content review.
- Implement automated checks to detect sensitive strings in published documents (internal hostnames, email lists, tooling).
- Continuous Monitoring (Strategic)
- Adopt routine OSINT monitoring for:
- Newly registered look-alike domains
- Phishing kits/cloned portals
- Employee impersonation campaigns
- Reputation changes (domain/IP associations)

10

Conclusion

This OSINT-driven assessment indicates TikTok/ByteDance maintain a generally strong external security posture, supported by widespread edge/CDN protections and clean domain reputation consensus from OSINT reputation sources. However, the organisation's global brand prominence and public discoverability of login endpoints and employee identity signals create a persistent medium-level risk centered on phishing, impersonation, and targeted social engineering.

Proactive, continuous OSINT monitoring—combined with strong email authentication enforcement and brand takedown readiness—remains critical to reducing real-world exploitation likelihood

Ethical Considerations & Disclaimer

11

- All data collected was publicly accessible through OSINT sources.
- No active scanning, exploitation, credential testing, or unauthorised access occurred.
- This report is produced for educational and defensive CTI purposes only.

References

12

Tools / Platforms

- Google Search (advanced operators / dorking)
- theHarvester
- Hunter.io
- VirusTotal
- OSINT Framework
- Shodan
- Internet Archive (Wayback Machine)
- MITRE ATT&CK Framework

Thank you!

Thank you for taking the time to read this report. If you have any questions or would like to discuss our findings further, please don't hesitate to reach out

📍 ON, CA.
☎ +1 437 8988 983
✉ lummiee@gmail.com