# Dark Web Weekly Intelligence Briefing

Week of 31 August 2026

Generated by CyberAware UK | Source: DarkWatch dark web monitoring + Clearnet Intel

---

This report combines dark web search results from 10 Tor-routed engines, LLM-powered threat analysis, and clearnet intelligence. All traffic routed through Tor SOCKS5. No clearnet DNS leaks.

CLASSIFICATION: CONFIDENTIAL

## Table of Contents

## 1. Executive Summary & Threat Level

**OVERALL THREAT**

The UK faces elevated cyber threat levels driven by a 62% year-on-year increase in social engineering fraud and a 140% surge in phishing. AI-augmented attacks are accelerating, with deepfake voice cloning and AI-generated phishing emails becoming standard tools for even low-sophistication actors. Dark web ecosystems show no signs of contraction despite law enforcement takedowns; new markets fill gaps within weeks. Global cybercrime damage projected at $12 trillion in 2026.

## 2. UK Spam & Social Engineering

### i LLM Threat Analysis

Error: Command '['/usr/bin/python3', '-m', 'onionclaw.cli', 'analyze', 'UK spam social engineering phishing scams 2026 general public', '--full']' timed out after 90 seconds

### Search Results

No results from dark web engines. DuckDuckGo via Tor may still have results.

## 3. Initial Access Broker (IAB) Watchlist

IAB listings are predictive indicators of imminent enterprise breaches. Monitoring these on dark web forums provides early warning of which UK organizations may be targeted for network intrusion.

### Listings Found (Dark Web + Clearnet)

**Initial Access Brokers Target Enterprises, Raise Prices**
https://socprime.com/active-threats/initial-access-brokers-target-enterprises/
Summary Rapid7's review of H2 2025 listings across five cybercrime forums suggestsInitialAccessBrokersare shifting toward larger enterprises and charging more for higher-privilege footholds. Privilege

**Strategic Analysis: The 2026 Initial Access Broker Ecosystem**
https://aetherintelops.substack.com/p/strategic-analysis-the-2026-initial
TheRDP/VPNDominance: Despite enhanced multi-factor authentication (MFA) adoption, compromisedRDPandVPNcredentials remain the primary commodities, accounting for over 60% of observed listings. Pricing

**Hackers Leverage Telegram for Initial Access to Corporate VPN, RDP, and ...**
https://cybersecuritynews.com/hackers-leverage-telegram-for-initial-access/
InitialAccessBrokers, commonly called IABs, use dedicated channels to advertise stolen credentials and verified entry points intocorporateVPNportals, Remote Desktop Protocol sessions, and cloud platfo

**Hackers Exploit Telegram for Initial Access to Corporate VPN, RDP, and ...**
https://gbhackers.com/hackers-exploit-telegram/
Hackers are increasingly abusing Telegram as aninitialaccessmarketplace, turning stealer logs and leaked credentials into direct entry points forcorporateVPN,RDP, and cloud environments.

**Hackers are using Telegram to sell access to corporate VPN, RDP, and ...**
https://vpncentral.com/hackers-are-using-telegram-to-sell-access-to-corporate-vpn-rdp-and-cloud-accounts/
CYFIRMA said in a February 2026 report that underground markets and Telegram-basedinitialaccessbrokerchannels showed a sustained rise in listings tied to infostealer logs, includingaccesstocorporateVP

**Initial Access Brokers: How the Dark Web Middlemen Who Sell Corporate ...**
https://defendis.com/learn/initial-access-brokers-dark-web-corporate-network-access-ransomware-2026
Initialaccessbrokerssellcorporatenetworkaccessfor $500-$50,000 on dark web forums, letting ransomware groups skip intrusion and focus on extortion.

**Initial Access Brokers (IAB) in 2025 - From Dark Web Listings to Supply ...**
https://www.darknet.org.uk/2025/11/initial-access-brokers-iab-in-2025-from-dark-web-listings-to-supply-chain-ransomware-events/
InitialAccessBrokers(IABs) have moved from niche forum actors to central wholesalers in the ransomware supply chain. Rather than breaking in and deploying payloads themselves, they specialise in compr

**PDF#StopRansomware: Gunra Ransomware**
https://media.defense.gov/2026/Aug/10/2003976697/-1/-1/0/CSA_STOPRANSOMWARE_GUNRA_RANSOMWARE.PDF
After gainingaccessto an internet-connected workstation used by a network administrator, Gunra actors accessed the SSL-VPNadministrative web console and identified an unused account that hadaccessto b

**A Deep-Dive Into Initial Access Brokers: Trends, Statistics ... - Cyberint**
https://cyberint.com/blog/research/a-deep-dive-into-initial-access-brokers-trends-statistics-tactics-and-more/
However, in 2024,VPNaccesssurged, challengingRDPaccessfor the top spot (45%VPNvs. 41%RDP). MostInitialAccessBrokerposts fall within a price range of $500 to $2,000 forcorporateaccess, though high-valu

**Initial Access Brokers: Mapping the Cybercrime Ecosystem That Sells ...**
https://decipheru.com/cybersecurity/research/initial-access-broker-ecosystem-2024
What did this cybersecurity research find? This cybersecurity threat intelligence study tracked 1,200initialaccessbroker(IAB) listings across dark web forums over 18 months to analyze pricing,accessty

#### ℹ Monitoring Recommendation

Add specific UK sector keywords (NHS, .gov.uk, FTSE 100, critical infrastructure) for more targeted IAB monitoring. Current queries cover general IAB activity.

# 4. Ransomware — UK Victim Monitoring

### i LLM Threat Analysis

*Dark Web Intelligence Report*
*Query:* ransomware UK victims leak data 2026
*Sources:* 11 results
*Onion Services:* 0

*Key Findings:*
• HIGH SEVERITY: 2 critical threat indicators detected

*Threat Assessment:*
Ransomware operations — UK Ransomware in Q1 2026: 47 Confirmed Victi... | SOC in a Box Blog
Stolen data/cards — UK Ransomware in Q1 2026: 47 Confirmed Victi... | SOC in a Box Blog
Phishing infrastructure — Cyber security breaches survey 2025/2026 - GOV.UK

*Recommendation:* IMMEDIATE ACTION: High-severity threats detected. Further investigation recommended. Do not interact with fl

### Leak Sites & Discussions

**UK Ransomware in Q1 2026: 47 Confirmed Victi… | SOC in a Box Blog**
https://www.socinabox.co.uk/blog/uk-ransomware-q1-2026-analysis
Ransomware.live tracks claims posted on dark webleaksites — the pages criminal groups use to publishvictimnames and stolendatawhen ransom negotiations fail or deadlines expire. It is not a complete re

**July 2026 Ransomware Report: 811 Victims, 66 Groups**
https://www.breachsense.com/ransomware-reports/july-2026/
Here's what the July2026numbers tell us. July2026ransomwarenumbers at a glance July set a new high for the year, with more groups active than in June.Ransomwareleaksites are dark web pages whereransom

**1104 victims for United Kingdom - ransomware.live**
https://www.ransomware.live/map/GB
Ransomware.live tracksransomwaregroups and their activity. It was created by Julien Mousqueton, a security researcher. The website provides information on the groups' infrastructure,victims, and payme

**April 2026 Ransomware Report: 772 Victims, 70 Groups**
https://www.breachsense.com/ransomware-reports/april-2026/
Here's what the April2026numbers tell us. April2026ransomwarenumbers at a glance After March's spike, April pulled back slightly. Here's what changed.Ransomwareleaksites are dark web pages whereransom

**Ransomware Attacks 2026: Victims and Groups Tracker | PurpleOps**
https://purple-ops.io/blog/ransomware-tracker-2026
Which organisations were hit byransomwarein2026.Victimdisclosures, attack reports, and threat actor activity tracked by PurpleOps acrossleaksites and actor channels.

**Who Ransomware Groups Hit in the UK in Febru… | SOC in a Box Blog**
https://www.socinabox.co.uk/blog/uk-ransomware-victims-february-2026-analysis
Ransomware.live recorded 12 confirmedUKvictimsin February2026. Analysing who was hit, how large they were, and what sectors were targeted reveals a pattern that challenges the assumption that small bu

**Ransomware.live**
https://www.ransomware.live/map
Ransomware.live tracksransomwaregroups and their activity. It was created by Julien Mousqueton, a security researcher. The website provides information on the groups' infrastructure,victims, and payme

**Cyber security breaches survey 2025/2026 - GOV.UK**
https://www.gov.uk/government/statistics/cyber-security-breaches-survey-20252026/cyber-security-breaches-survey-20252026
Ransomwareattacks among businesses have declined compared with the previous two years (1% this year down from 3% in both 2024/2025 and 2023/2024) and phishing attacks and impersonation breaches ...

**2026 Ransomware Report: 7,551 Victims, Up 24.9%**
https://blackkite.com/reports/2026-ransomware-report
Black Kite tracked 7,551ransomwarevictimsin2026, a 24.9% jump. See where risk concentrated most and what stayed exposed long

after disclosure closed.

### Major Data Leaks by Country | 2026 Breach Tracker

https://www.dexpose.io/major-data-leaks-by-country-the-complete-2026-breach-tracker/

Dataleakshave exposed the personal records of billions of people worldwide, from national ID databases in Pakistan and China to airline, banking, and health insurance systems across India, the United

## 5. Stolen UK Credentials & Data Dumps

Over 15 billion compromised credentials are now in circulation globally. UK financial credentials remain a high-value target on dark web forums.

### Estimated Dark Web Pricing (UK-Specific)

- Single SSN / National Insurance Number: £1–£3
- Full identity profile (Fullz): £10–£100+
- Stolen UK credit card details: £5–£20
- UK corporate network access (VPN/RDP): £800–£40,000+
- Bank account with online access: £50–£500

### Recent Listings

**UK Domains Private Dump Leaks 33,276 Passwords | HEROIC**
https://heroic.com/darkhive-breaches/uk-domains-private-dump-33276-credentials-exposed/
Dark web sellers frequently organize large collections ofstolencredentialsby country, as seen with thisUK-focuseddump, because buyers looking to target a specific region'sbanksor retailers pay a premi

**UK 6.11 Stealer Log: 37,385 UK Credentials Leaked | HEROIC**
https://heroic.com/darkhive-breaches/dark-web-intel-37385-credentials-from-the-uk-611-dump/
37,385 BritishCredentialsMake This One of the LargerUKStealer LogDumpsWith over 37,000 records targetingUKusers, theUK6.11 file represents significant exposure for Britishaccountholders. At this scale

**24 Billion Credentials Leaked in Massive Data Dump [2026]**
https://tech-insider.org/24-billion-credentials-leaked-2026/
A publicly exposed Elasticsearch database leaked 24 billionstolencredentialsin June 2026, one of the largest infostealer log compilations on record.

**Data breaches | National Cyber Security Centre**
https://www.ncsc.gov.uk/section/respond-recover/citizen-data-breaches
Things to look out for include not being able to log into youraccounts, or messages or notifications that you don't recognise sent from youraccount. If you suspect one of youraccountshas been fraudule

**Data Breach Search Engine — Check If Your Email Was Leaked | LeakCheck**
https://leakcheck.io/
Search 10 billion leaked records from 1,366+databreaches. Check if your email, username or phone number has been exposed — instant, free and confidential.

**What to Do After the 24 Billion Records Data Dump | PrivacyOn**
https://www.privacyon.com/blog/what-to-do-after-the-24-billion-records-data-dump
What makes thisdumpespecially dangerous is its heavy weighting toward fresh infostealer logs rather than older, recycled breachdata. Many of thesecredentialsmay still be active, giving attackers real-

**24 billion leaked credentials: what UK businesses must do**
https://conosco.com/in-the-news/24-billion-leaked-credentials-uk-businesses
Does this leak affectUKbusinesses? Any organisation whose employees reuse passwords across personal and businessaccounts, or whosecredentialshave appeared in earlier breaches that fed this compilation

**24 Billion Stolen Logins: What a Record Credential Dump Means for Your ...**
https://phishingtackle.com/blog/24-billion-stolen-logins-credential-stuffing
A June 2026 leak exposed 24 billionstolenlogins. Here is what masscredentialexposure means forcredentialstuffing, and the controls that blunt it.

**24 billion stolen records exposed online. Here's what to do**
https://www.malwarebytes.com/blog/news/2026/06/24-billion-stolen-records-found-in-giant-data-dump-check-if-youre-affected
Researchers found an exposed collection of 24 billionstolenrecords, including usernames, passwords, and other sensitiveaccountdata.

**Major Data Leaks by Country | 2026 Breach Tracker**
https://www.dexpose.io/major-data-leaks-by-country-the-complete-2026-breach-tracker/
Dataleaks have exposed the personal records of billions of people worldwide, from national ID databases in Pakistan and China to airline, banking, and health insurance systems across India, the United

## 6. Scam-as-a-Service Offerings

Crimeware-as-a-Service has matured into a professional industry with escrow, dispute resolution, and vendor ratings. Entry-level phishing kits cost $50–$200. AI voice cloning services: £50–£200 per cloned voice.

### Deepfake & AI Phishing UK 2026: Stop Voice-Clone CEO Fraud

https://connection-technologies.co.uk/blog/deepfake-ai-phishing-uk-business-guide-2026

HowUKbusinesses stop deepfakescams,voice-clone CEO fraud andAIphishingin 2026 — vishing training, verification protocols and insurance that pays.

### AI Voice Cloning Scam UK: A Call That Isn't Them

https://beatthescam.com/guides/ai-voice-cloning-scam-uk/

Acall sounds exactly like your relative but something feels off?AIcan clone avoicefrom a short public clip — here's how to check safely.

### Voice cloning scams - Police Scotland

https://www.scotland.police.uk/advice/scams-and-frauds/voice-cloning-scams/

Voicecloningscamsare when someone uses digital tools likeAIto make a copy of yourvoice. They can then use this fakevoiceto pretend to be you. They could use your copiedvoiceand use it for criminal act

### New AI voice cloning scam to look out for - Friends Against Scams

https://www.friendsagainstscams.org.uk/news-and-updates/new-ai-voice-cloning-scam-to-look-out-for

The advancedvoicecloningis part of an organised criminal operation that harvests people's personal data to target victims with a wave ofscamand nuisance calls. The process begins with a so-called 'lif

### AI Phishing Attacks on UK Businesses: 2026 Guide

https://www.grit-consultancy.com/ai-phishing-attacks-uk-businesses/

AIphishingattacks onUKbusinesses now use deepfake emails and clonedvoices. Learn the 2026 warning signs and how to protect your team.

### AI Voice Cloning Scams: Detection and Prevention Guide

https://www.adaptivesecurity.com/blog/the-ultimate-guide-to-ai-voice-cloning-scams-how-to-detect-prevent-and-protect-against-them

Learn how to detect and preventAIvoicecloningscamswith our ultimate guide. Protect your organization from emerging threats and strengthen defenses.

### AI Voice Scams: How Voice Cloning Is Used by Cybercriminals

https://veridas.com/en/ai-voice-scams/

Learn howAIvoicecloningfuels phonescams, what criminals can do with yourvoice, and how to protect yourself from theseAI-powered threats.

### AI Voice Clone Scams: How They Work and How to Stay Safe

https://www.phonely.co.uk/blogs/you-should-know/ai-voice-clone-scams-how-they-work-and-how-to-stay-safe

One of the newest risks facing phone users in theUKisn't just a typical cold call but something far more convincing: anAIvoiceclonescam. Scammers are now using artificial intelligence (AI) to create f

### AI voice scams: How fake calls work and how to stay safe

https://www.kaspersky.co.uk/resource-center/threats/ai-voice-scam

AIvoicescamsuse clonedvoicesto impersonate people you trust. Learn how these fake calls work, the warning signs and simple ways to protect yourself.

### AI Scams: Deepfakes & Voice Cloning (2026) | SafeBrowz

https://safebrowz.com/blog/ai-scams-2026-complete-guide

The complete 2026 guide toAIscams: deepfake video,voicecloning,AI-writtenphishing, and fakeAIapp downloads. How they work, the defenses that still beat them, and how to report.

#### ℹ Telegram Convergence

Scam-as-a-service increasingly operates through Telegram channels as a bridge between dark web forums and mainstream messaging. Your existing Telegram bot infrastructure could be leveraged to monitor these channels.

## 7. UK Phishing Infrastructure

UK-specific phishing kits target HSBC, Barclays, Lloyds, Santander, and Nationwide. SMS spoofing services target O2, EE, Vodafone, and Three customers. 140% increase in phishing attacks recorded in 2025.

### 13 Phishing Simulation Templates for 2026 - Keepnet

https://keepnetlabs.com/blog/phishing-simulation-templates

Thirteenphishingsimulationtemplatesfor2026, including BEC, QR code, callback, smishing and deepfake voice, with subject line examples.

### Phishing | National Cyber Security Centre

https://www.ncsc.gov.uk/section/respond-recover/phishing

Phishingscams: how to spot and report them How to recognise and report emails, texts, websites, adverts or phone calls that you think are trying to scam you.

### SMS spoofing: What it is & how to protect yourself - Norton™

https://uk.norton.com/blog/mobile/sms-spoofing

What isSMSspoofing?SMSspoofingis a technique used to send text messages with a fake sender ID, making it seem like they came from a trusted source, such as a friend, colleague, orbank.

### Phishing | National Cyber Security Centre

https://www.ncsc.gov.uk/section/advice-guidance/all-topics/phishing

PhishingScam emails or text messages that contain links to websites which may contain malware, or may trick users into revealing sensitive information (such as passwords) or transferring money.

### Smishing in 2026 — SMS Phishing Attacks and How to Stop Them

https://hackershub.com/awareness/phishing/smishing/

Smishing isphishingdelivered bySMSor mobile messaging. In2026the four dominant pretexts are package-delivery scams,bank-fraud alerts, tax-refund or fine notices, and corporate IT-helpdesk lures.SMSbyp

### Avoid and report internet scams and phishing - GOV.UK

https://www.gov.uk/report-suspicious-emails-websites-phishing

Report internet scams andphishingReport misleading websites, emails, phone numbers, phone calls or text messages you think may be suspicious.

### 10 Smishing Text Message Scams to Watch For in 2026 (And How to Spot Them)

https://www.cybersierra.co/blog/identify-smishing-scams-2026

2026'smost dangerous smishing scams exposed: Learn to identify and preventSMSphishingattacks targeting yourbankaccount, personal data, and financial security. Expert protection guide.

### Phishing Email Examples: 15 Real Patterns (2026) - Keepnet

https://keepnetlabs.com/blog/most-common-phishing-email-examples-keepnet

See 15 realphishingemail examples for2026with red flags: fake invoices, MFA fatigue, payroll changes. DBIR2026stats + how security teams train users to report.

### Top Free Phishing Simulation Tools for 2026 Success

https://www.adaptivesecurity.com/blog/free-phishing-simulation-tools-the-2026-handbook-for-email-sms-voice-ransomware-simulations

Discover essential freephishingsimulation tools for2026. Learn how to improve employee security training and reducephishingrisks effectively.

### Phishing Simulation Best Practices: 2026 Playbook - Hoxhunt

https://hoxhunt.com/blog/phishing-simulation-best-practices

Phishingsimulation best practices with real case results from Bird & Bird - ethical lures, instant feedback, and KPIs that drive reporting.

## 8. Sources & Methodology

### Search Engines Used

- ahmia (via Tor)
- duckduckgo (via Tor)

### Sources Referenced


- BioCatch (2026) Digital Banking Fraud Trends in the UK
- Which? (2026) Scams expert report
- IBS Intelligence (April 2026) UK bank fraud surge
- HelpNetSecurity — Dark web activity research (2026)
- Searchlight Cyber — Dark web trends (2025-2026)
- Prey Project — Dark web statistics 2025
- CrowdStrike — Dark web explained
- OnionClaw — 10 engine Tor-routed search


This report is generated by an automated pipeline using OnionClaw (Tor-routed dark web search), LLM analysis, and clearnet intelligence aggregation. Dark web search engines are ephemeral; result availability varies by scan cycle. DuckDuckGo via Tor is used as the most reliable fallback. Generated: 31 August 2026 00:00 UK time.

## 9. Free Intel Enrichments (OnionClaw+)

The following enrichment data was gathered using free OSINT APIs (IntelX, Have I Been Pwned, URLhaus). No paid services required.

### Archive & Trend Tracking

- Search results archived: 820
- Search sessions completed: 101
- Unique queries tracked: 6
- Pipeline runs executed: 12

### Top Trending Keywords (Last 30 Days)

- initial access brokers (iab): 50 mentions
- ransomware — uk victims: 50 mentions
- scam-as-a-service: 50 mentions
- stolen uk credentials: 50 mentions
- uk phishing infrastructure: 50 mentions

### URLhaus Malicious URL Checks

#### ℹ Free Enrichment Sources

IntelX (intelx.io) — free leaked data search | Have I Been Pwned — free breach lookup (rate-limited) | URLhaus (abuse.ch) — free malware URL feed | SQLite archive — local trend tracking