

Dark Web Weekly Intelligence Briefing

Week of 26 October 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
- 2. UK Spam & Social Engineering
- 3. Initial Access Broker (IAB) Watchlist
- 4. Ransomware — UK Victim Monitoring
- 5. Stolen UK Credentials & Data Dumps
- 6. Scam-as-a-Service Offerings
- 7. UK Phishing Infrastructure
- 8. Free Intel Enrichments (OnionClaw+)
- 9. Sources & Methodology

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

Dark Web Intelligence Report

Query: UK spam social engineering phishing scams 2026 general public

Sources: 11 results

Onion Services: 0

Key Findings:

- HIGH SEVERITY: 1 critical threat indicators detected

Threat Assessment:

Hacking services — PDFUK Spam & Social Engineering Weekly Threat Briefing

Exploit trading — PDFUK Spam & Social Engineering Weekly Threat Briefing

Phishing infrastructure — PDFUK Spam & Social Engineering Weekly Threat Briefing

Fraud services — PDFUK Spam & Social Engineering Weekly Threat Briefing

Identity theft — UK social engineering scams jump 62% as fraud tactics shift: BioCatch

Recommendation: IMMEDIATE ACTION: High-severity threats detected. Further investigation recommended. Do not interact with flagged services without proper operat

Search Results

PDFUK Spam & Social Engineering Weekly Threat Briefing

https://cyberawareuk.co.uk/reports/uk-scams/UK_Scams_Weekly_Briefing_20260826.pdf

The widespread adoption of generative AI has dramatically improved the quality and believability of phishing, voice cloning, and deepfake attacks, making them significantly harder for the general public

PDFUK Spam & Social Engineering Weekly Threat Briefing

https://cyberawareuk.co.uk/reports/uk-scams/UK_Scams_Weekly_Briefing_20260715.pdf

Social engineering fraud in the UK has reached record levels in 2025-2026, with a 62% year-on-year increase in attempted attacks. Fraudsters are pivoting away from technical hacking toward psychological m

UK social engineering scams jump 62% as fraud tactics shift: BioCatch

<https://www.biometricupdate.com/202604/uk-social-engineering-scams-jump-62-as-fraud-tactics-shift-biocatch>

While the United States is battling with credit card fraud and identity theft, UK consumers are being targeted by increased attempts at social engineering attacks, behavioral biometrics company BioCatch wa

Phishing Attack Alert 2026: New AI Email Scams in UK

<https://securityjournaluk.com/phishing-attack-alert-2026/>

Explore the latest phishing attack trends affecting UK users in 2026, including AI-driven phishing emails, fake login scams, credential theft tactics, and expert prevention strategies.

Phishing Scams UK 2026: Spot, Report, and Claim Back | Kaeltripton

<https://www.kaeltripton.com/latest/phishing-scams-uk-how-to-spot-and-report/>

Phishing Scams UK 2026: How to Spot Them, Report Them, and Get Your Money Back Phishing is the leading gateway to financial fraud in the UK. FCA and Action Fraud report rising impersonation scam volumes in 202

Phishing Attack Trends 2026: UK & Global Statistics

<https://www.internetsafetystatistics.com/phishing-attack-trends-statistics/>

Explore the latest Phishing Attack Trends for 2026, from AI-generated scams and quishing to UK, Irish and global data, plus how to stay protected.

Email Phishing Scams Statistics 2026: UK Data

<https://www.internetsafetystatistics.com/email-phishing-scams-statistics/>

Email phishing scams statistics for 2026, with UK and Irish breach data, AI-driven scam trends and practical steps to spot a fake message.

Phishing Statistics UK: Attacks, Scam Reports & Fraud Losses

<https://gdprcourse.co.uk/blog/phishing-statistics-uk>

UK phishing statistics: 38% of businesses identified attacks in the 2025/26 survey; NCSC reporting totals, payment-fraud context and current reporting routes.

Money stolen by scammers hijacking UK social media accounts rises 400%

<https://www.theguardian.com/money/2026/oct/05/scammers-hijacking-uk-social-media-accounts>

The total amount stolen by criminals who hack into people's emails and social media accounts and then pretend to be them has risen by more than 400% in a year, official UK data shows.

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

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

How UK businesses stop deepfake scams, voice-clone CEO fraud and AI phishing in 2026— phishing training, verification protocols and insurance that pays.

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 suggests Initial Access Brokers are shifting toward larger enterprises and charging more for higher-privilege footholds. Privilege

How Initial Access Brokers Sell Corporate Network Access | Sinon ...

<https://www.sinonsecurity.com/blog/how-initial-access-brokers-sell-corporate-network-access-sinon-security>

Initial access brokers auction VPN, RDP and domain admin access to ransomware crews. See how IAB listings work, what they cost in 2026, and how to detect exposure early.

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, VPN access surged, challenging RDP access for the top spot (45% VPN vs. 41% RDP). Most Initial Access Broker posts fall within a price range of \$500 to \$2,000 for corporate access, though high-value

Hackers Leverage Telegram for Initial Access to Corporate VPN, RDP, and ...

<https://cybersecuritynews.com/hackers-leverage-telegram-for-initial-access/>

Initial Access Brokers, commonly called IABs, use dedicated channels to advertise stolen credentials and verified entry points into corporate VPN portals, Remote Desktop Protocol sessions, and cloud platforms.

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-based initial access broker channels showed a sustained rise in listings tied to info-stealer logs, including access to corporate VPN

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>

Initial access brokers sell corporate network access for \$500-\$50,000 on dark web forums, letting ransomware groups skip intrusion and focus on extortion.

How initial access brokers price corporate access in 2026: an explainer ...

<https://ransomnews.com/initial-access-brokers-pricing-2026/>

A field guide to the 2026 initial access broker market: how IABs source access, how they price it, who buys, and what the listings look like under the hood.

Initial Access Brokers 2026: ransomware's supply chain

<https://ransomnews.com/initial-access-brokers-2026-ransomware-supply-chain/>

Initial Access Brokers (IABs) are the middlemen of the modern ransomware economy, specialists who break into corporate networks and resell that access to ransomware operators. We break down the marketplaces,

PDF Initial Access Brokers Report - e.cyberint.com

<https://e.cyberint.com/hubfs/IAB%20Report%202025.pdf>

Brokers targeting RDP systems sell access to corporate servers compromised through brute-force attacks on unprotected systems with weak credentials. Finally, brokers exploit known vulnerabilities in network devices.

Initial Access Brokers (IABs): How Hackers Sell Access to Corporate ...

<https://securifyai.co/learnings/initial-access-brokers-how-hackers-sell-access-to-corporate-networks/>

Initial Access Broker activities typically target enterprise infrastructure across multiple environments. Platforms commonly targeted: Corporate VPN portals, Remote Desktop Protocol (RDP) servers, Cloud infrastructure.

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: 1 critical threat indicators detected

Threat Assessment:

Ransomware operations — Ransomware Statistics — 2026

Fraud services — Over 300 UK Firms Hit by Ransomware in a Year

Recommendation: IMMEDIATE ACTION: High-severity threats detected. Further investigation recommended. Do not interact with flagged services without proper operational security.

Leak Sites & Discussions

Ransomware Statistics — 2026

<https://www.ransomware.live/stats/2026>

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

Ransomware statistics 2026: latest UK and global data

<https://aag-it.com/the-latest-ransomware-statistics/>

Theransomwarelandscape has fragmented.Leak-site tracking recorded 7,551 namedvictimsbetween April 2025 and March2026, a 24.9% rise, with 61 newransomwaregroups appearing during the period and 146 acti

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.

Ransomware attacks in 2026: 876 confirmed incidents so far

<https://ransomnews.com/ransomware-attacks/2026/>

Whichransomwaregroups had the most confirmedvictimsin2026The operator is attributed in 700 of the 876 confirmed incidents. Counts are confirmedvictims, notleak-site claims, so they run well below the

Ransomware Tracker: Live Victims & Leak Sites | Ransomnews

<https://ransomnews.com/ransomtracker/>

Liveransomwareleak-site tracker: 29victimslisted in the last 24 hours, 889 this month, 8,916 in2026, 636 operations catalogued. Claims as published, with operator profiles, trends and a country map.

Ransomware.live

<https://www.ransomware.live/stats>

Ransomware.live tracks & monitorsransomwaregroups'victimsand their activity. It was created by Julien Mousqueton, a security researcher. The website provides information onRansomwaregroups,victims, ne

Over 300 UK Firms Hit by Ransomware in a Year

<https://www.infosecurity-magazine.com/news/over-300-uk-firms-hit-ransomware/>

UKorganizations suffered more than 26 successfulransomwareattacks each month last year, with SMEs hit hardest, according to newdatafrom Report Fraud. TheUK'scybercrime and fraud reporting service was

Ransomware Report H1 2026 — 4,472 Victims Analyzed | HookPhish

<https://www.hookphish.com/reports/ransomware-h1-2026/>

Home / Reports /RansomwareH12026Threat ReportRansomwareLandscape Report — H120264,472 organizations were named onransomwareleaksites in the first half of2026— an average of 24.7 every single day, acro

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.

Recent Breaches: Latest Data Breach News & Live Tracker (2026)

<https://recentbreaches.com/>

Recent Breaches tracks the latest data breaches, leaks and ransomware disclosures as they happen — what was exposed, who was affected, the groups behind them, and how to check if your information is out there

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

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 billion stolen credentials in June 2026, one of the largest info-stealer log compilations on record.

UK Domains Private Dump Leaks 33,276 Passwords | HEROIC

<https://heroic.com/darkhive-breaches/uk-domains-private-dump-33276-credentials-exposed/>

What Was Exposed This leak included the following data types: Email addresses tied to UK domains Plaintext passwords URLs linked to each set of credentials Why This Matters With 33,276 UK-focused credentials

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 this dump especially dangerous is its heavy weighting toward fresh info-stealer logs rather than older, recycled breach data. Many of these credentials may still be active, giving attackers real-

Recovering a hacked account | National Cyber Security Centre

<https://www.ncsc.gov.uk/guidance/recovering-a-hacked-account>

Whether it's your email, a social media account, or your online bank, losing access to a digital account can be stressful. This guidance explains what you can do to minimise the damage, and how you can re

24 Billion Stolen Records Data Breach Threats | CyPro

<https://cypro.co.uk/insights/cyber-bulletins/24-billion-stolen-records-found-in-data-dump-what-to-do/>

Given the scale of the 24 billion stolen records data dump, organisations should act quickly to assess and strengthen their security posture. Here are key steps to consider: 1. Check for Exposed Credential

Hacked accounts | National Cyber Security Centre

<https://www.ncsc.gov.uk/section/respond-recover/hacked-accounts>

It's also important to change the password for any accounts where you use the same password. This is important because cyber criminals know people often use the same password for different accounts, and

Huge data leak of 149 million credentials exposed without any ...

<https://www.techradar.com/pro/security/huge-data-leak-of-149-million-credentials-exposed-without-any-protection-98gb-of-unique-usernames-and-passwords-from>

Jeremiah Fowler uncovered a huge database of credentials spanning financial services, banking, social media, and dating apps without password or encryption protection.

Money stolen by scammers hijacking UK social media accounts rises 400% ...

<https://www.theguardian.com/money/2026/oct/05/scammers-hijacking-uk-social-media-accounts>

The total amount stolen by criminals who hack into people's emails and social media accounts and then pretend to be them has risen by more than 400% in a year, official UK data shows.

24B Records Exposed in Massive Leak of Emails, Passwords, and Login Data

<https://www.techrepublic.com/article/news-24-billion-credential-records-exposed-database/>

A massive collection of stolen login credentials containing roughly 24 billion records was briefly exposed online, according to cybersecurity researchers at Cybernews.

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 billion stolen records, including usernames, passwords, and other sensitive account data.

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 andAlphishingin 2026 — vishing training, verification protocols and insurance that pays.

AI Scams in the UK 2026 — Spot and Avoid Them | AI101.uk

<https://www.ai101.uk/blog-ai-scams-uk-2026.html>

AcompleteUKguide toAI-poweredscamsin 2026. Deepfakevoicecalls,Alinvestment fraud, romancescams,phishing— how to spot each one, what to do if you're targeted, and how to protect yourself.

AI Voice Cloning Scams UK 2025-2026: How They Work and How to Stay Safe ...

<https://www.whoiscalling.me.uk/scams/ai-voice-cloning>

Alvoicecloninguses 3 seconds of audio to clone avoicewith 85% accuracy. Find out how thesescamswork in theUKand how to protect yourself.

AI Voice Scam Prevention for UK Firms - mtsservices.co.uk

<https://www.mtsservices.co.uk/blog/vishing-attack-prevention-uk-7-steps-to-stop-ai-voice-cloning-scams/>

StopAlvoicecloningcamswith 7 practical vishing prevention steps forUKbusinesses, from payment checks to staff training.

AI Phishing Attacks on UK Businesses: 2026 Guide

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

The three main types ofAlphishingAlphishingshows up in three main forms: Fake emails, often called business email compromise, that impersonate a boss or supplier.Voicecloning, known as vishing, where

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

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

What anAlvoicecloningcamlooks like Thisscamis a phone call using anAI-generated copy of a real person'svoice— often a family member — claiming an emergency and asking for money urgently.

Voice cloning scams - Police Scotland

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

Voicecloningcamssare when someone uses digital tools likeAlto 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

AI Voice Cloning Fraud: What the UK Government Just Warned, How Much ...

<https://westpiertech.com/ai-voice-cloning-fraud-what-the-uk-government-just-warned-how-much-businesses-are-losing-and-what-to-do-first/>

This is a plain guide to whatvoicecloningis, what the government actually said, what it is costingUKbusinesses, and the order to deal with it. If you are searching for:AlvoicecloningcamscamUKdeepfake CE

Deepfake Vishing Defense: Detect Voice Cloning Attacks

<https://shieldoperations.co.uk/deepfake-vishing-defense-voice-cloning/>

Protect your organisation fromAlvoicecloningattacks. Detection checklist and policy template for executives and HR teams. Stop deepfake vishing now.

AI Voice Cloning Scams Surge in the UK — CyberAware UK

<https://cyberawareuk.co.uk/ai-voice-cloning-surge-2026>

AlVoiceCloningSurge — July 2026 Investigation TL;DR:Alvoicecloningcamscin theUKhave surged 200% since January 2026. Criminals arecloningvoicesfrom 3-second audio clips pulled from TikTok, Instagram,

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.

UK Scam & Phishing Prevention Guide: 2026 Edition

<https://cyberawareuk.co.uk/scam-phishing-prevention-guide-2026>

The plain-EnglishUKscam andphishingprevention guide for2026: how to spotphishingtexts and emails, the top scams targetingUKfamilies, and exactly what to do if you are targeted. Free, human-verified an

UK Scam Alerts: Current Phishing, Fraud and Dark-Web Threats

<https://cyberawareuk.co.uk/uk-scam-alerts>

The scams hitting theUKright now - currentphishing,bank, parcel, crypto and job scams with clear what-to-do guidance. Updated daily from Action Fraud, police, CERTs and dark-web monitoring.

Spoof Text Messages Explained: Spot and Avoid Them in 2026

<https://www.sendhub.com/sms-spoof-text-messages-explained/>

Learn what spoof text messages are, howSMSspoofingworks, real2026examples, warning signs to watch for, and a complete step-by-step guide to reporting them.

UK Scam Texts (2026): Current Campaigns and Free Checker | ONSIM

<https://onsim.uk/scam-texts/>

The scam texts currently circulating in theUK: Royal Mail, Evri, DVLA, HMRC,banks, "Hi Mum" and more. What each looks like, how to tell, and a free AI checker for any message.

13 Free Phishing Email Templates, Ready to Use - Keepnet

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

Thirteen ready-to-usephishingemailtemplates, from BEC and QR code to callback,SMSand deepfake voice, each with a subject line and red flags.

Scam Texts UK (2026) — Spot a Fake Text & Report It Free to 7726 ...

<https://connection-technologies.co.uk/blog/scam-texts-uk-how-to-spot-check-report>

Got a suspicious text? See the scam texts circulating in theUK, check the sender free, and report smishing to 7726 in seconds. Stay ahead of fraudsters.

Bank Scams 2026: Threats, Trends, and Fraud Prevention Strategies for ...

<https://ironvest.com/blog/banking-scams-guide-2026/>

An in-depth2026guide tobankscams and banking fraud types shaping the financial sector. Examine real-world tactics, current solution challenges, and next-gen fraud prevention solutions.

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.

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

<https://hackershut.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

Phishing Attack Alert 2026: New AI Email Scams in UK

<https://securityjournaluk.com/phishing-attack-alert-2026/>

Explore the latestphishingattack trends affectingUKusers in2026, including AI-drivenphishingemails, fake login scams, credential theft tactics, and expert prevention strategies.

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: 26 October 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: 1290
- Search sessions completed: 149
- Unique queries tracked: 6
- Pipeline runs executed: 20

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