

Dark Web Weekly Intelligence Briefing

Week of 20 July 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:

Phishing infrastructure — Phishing Attack Alert 2026: New AI Email Scams in UK

Fraud services — Scam Statistics in UK 2026 | Types, Losses & Key Consumer Facts

Ransomware operations — AI-Powered Phishing & Deepfake Scams in 2026: How Social Engineering Is ...

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

Search Results

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.

Top internet scams in United Kingdom 2025-2026 - wonconnect.org.uk

<https://www.wonconnect.org.uk/top-internet-scams-in-united-kingdom-2025-2026/>

Top internet scams in United Kingdom 2025-2026. Over the next two years, you will face evolving online schemes across the United Kingdom; this guide shows how you can spot phishing, AI-generated deepfake

Phishing Statistics [2026]: Latest Attack Data & Trends

<https://app.stationx.net/articles/phishing-statistics>

Discover 2026 phishing statistics from 40+ sources — email volumes, AI-generated attacks, click rates, BEC losses, and industry targeting.

Social Engineering 2026: The Hidden Breach Behind Every Breach

<https://threatscene.com/blog-update/social-engineering-2025-the-hidden-breach-behind-every-breach/>

Introduction For years, phishing emails drove most social engineering attacks. That has changed. According to Mandiant's M-Trends 2026 report, based on over 500,000 hours of incident response work, voicephishing

Scam Statistics in UK 2026 | Types, Losses & Key Consumer Facts

<https://theworlddata.com/scam-statistics-in-uk/>

Scam in United Kingdom 2026 The scam landscape in the United Kingdom has reached an alarming new threshold in 2026, with official data from multiple government bodies and fraud prevention agencies confirming

I'm a scams expert and these are the scams that will be big in 2026

<https://www.which.co.uk/news/article/im-a-scams-expert-and-these-are-the-scams-that-will-be-big-in-2026-aT2MR9t7Dev9>

Each year in my work as a scam expert, I see variations of the same old tricks. But with further technological innovations, such as artificial intelligence (AI), and the introduction of new regulations

Social Engineering Attacks in the Age of Generative AI

<https://www.eccu.edu/blog/social-engineering-attacks-generative-ai-2026/>

Explore how generative AI is transforming social engineering attacks in 2026, from deepfake scam to AI-powered phishing, and learn how organizations can defend against them.

The most convincing scams of 2026 so far - Which?

<https://www.which.co.uk/news/article/the-most-convincing-scams-of-2026-so-far-allCo4W8L4Q1>

Avoid clicking paid ads on search engines and social media. If in doubt, break off contact and use trusted contact details (such as those from a bill or statement) to verify the request. If you've given

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—vishing training, verification protocols and insurance that pays.

AI-Powered Phishing & Deepfake Scams in 2026: How Social Engineering Is ...

<https://www.linkedin.com/pulse/ai-powered-phishing-deepfake-scams-2026-how-social-engineering-8529c>

Payroll fraud, credential theft, ransomware delivery, and financial wire transfers are all increasingly initiated through AI-enhanced social engineering.

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)

Strategic Analysis: The 2026 Initial Access Broker Ecosystem

<https://aetherintelops.substack.com/p/strategic-analysis-the-2026-initial>

The RDP/VPN dominance: Despite enhanced multi-factor authentication (MFA) adoption, compromised RDP and VPN credentials remain the primary commodities, accounting for over 60% of observed listings. Pricing

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 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.

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

Initial Access Brokers have Shifted to High-Value Targets and ... - Rapid7

<https://www.rapid7.com/blog/post/tr-initial-access-broker-shift-high-value-targets-premium-pricing/>

Initial Access Brokers (IABs) are a key component of the cybercrime ecosystem, offering hassle-free building blocks for ransomware, data theft, and extortion. Rapid7's analysis of H2 2025 activity highli

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

<https://securifyai.co/blog/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 infras

PDF Initial Access Brokers Report - e.cyberint.com

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

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

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

Initial Access Brokers: How Threat Actors Breach Enterprise Perimeters ...

<https://ismalicious.com/posts/initial-access-brokers-attack-vectors-2026>

A deep dive into initial access brokers (IABs)—the cybercrime specialists who sell footholds into corporate networks—covering their techniques, pricing, detection signals, and how to defend against the top

The Price of Secrets: How Initial Access Brokers Value Corporate Access ...

<https://abnormal.ai/blog/initial-access-brokers-value-corporate-access-credentials>

Explore the ways in which corporate network access is valued by initial access brokers (IABs) according to access type, company revenue, and country tier.

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

Identity theft — The State of Ransomware 2026: Payments Drop as Encryption Climbs

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

Recommendation: IMMEDIATE ACTION: High-severity threa

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

Ransomware.live

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

This page displays the 100 most recentvictimdisclosures attributed toransomwaregroups, as detected byRansomware.live. Our platform continuously monitors and scrapesransomwaregroupleaksites to identify

1039 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

June 2026 Ransomware Report: 707 Victims, 63 Groups

<https://www.breachsense.com/ransomware-reports/june-2026/>

Here's what the June2026numbers tell us. June2026ransomwarenumbers at a glance June's numbers bounced back. Morevictims, more groups, more countries. But the real shift was in the rankings.Ransomware!

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

PDF2026 Ransomwareand Cyber Threat Report

<https://www.guidepointsecurity.com/wp-content/uploads/2026/01/GRIT-2026-Ransomware-and-Cyber-Threat-Report.pdf>

victimsonransomwaredataleaksites. The numbers tell a stark story where legal industryransomwarevictimsmore than doubl d YoY from 196 in 2024 to 455 in 202

The State of Ransomware - Q1 2026 - Check Point Research

<https://research.checkpoint.com/2026/the-state-of-ransomware-q1-2026/>

Key FindingsRansomwarein Q12026: Consolidation at Scale During the first quarter of2026, we monitored more than 70 activedataleaksites (DLS) that collectively listed 2,122 newvictims. This figure repr

UK Cybersecurity Statistics 2026 - cybersecstats.com

<https://www.cybersecstats.com/uk-cybersecurity-statistics-2026/>

ComprehensiveUKcyber security statistics coveringransomware, fraud, SME vulnerabilities, and budget trends. 300+datapoints from the latest2026data.

Ransomware Statistics 2026: Attacks, Costs & Trends -Complete Guide

<https://axis-intelligence.com/ransomware-statistics/>

44% of breaches involve ransomware. Our2026datahub covers attack volume, costs, top groups, and sector breakdowns — sourced from FBI IC3, IBM, Verizon, and Sophos.Ransomwarestatistics2026complete guide

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

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

Pwned Passwords - Have I Been Pwned

<https://haveibeenpwned.com/Passwords>

Why check for pwned passwords? Password reuse is extremely common and puts your accounts at risk. When credentials are exposed in data breaches, attackers can use these known email and password combinations

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 your accounts, or messages or notifications that you don't recognise sent from your account. If you suspect one of your accounts has been fraudulent

16 billion passwords exposed in colossal data breach | Cybernews

<https://cybernews.com/security/billions-credentials-exposed-in-fostealers-data-leak/>

HOME / SECURITY / 16 billion passwords exposed in record-breaking data breach: what does it mean for you? The Cybernews research team, in collaboration with security researcher Bob Diachenko, has uncovered

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 Credentials

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.

16 Billion Credentials Leak: A Closer Look at the Hype and Reality ...

<https://www.infostealers.com/article/16-billion-credentials-leak-a-closer-look-at-the-hype-and-reality-behind-the-massive-data-dump/>

Lack of Focus: Unlike targeted breaches, such as the Nobitex hack where infostealers exposed specific employee credentials, this leak is a disorganised data dump with little strategic value. Infostealers:

UK's Home for Reporting Cyber Crime & Fraud - Report Fraud

<https://www.reportfraud.police.uk/>

Bank account fraud has occurred if transactions you haven't made show up on your bank statement.

BreachDirectory - Check If Your Email or Username was Compromised

<https://breachdirectory.org/>

BreachDirectory allows you to search through all public data breaches to make sure your emails, usernames, passwords, and domains haven't been compromised.

What steps should I take if I have experienced a data breach?

<https://ico.org.uk/for-the-public/i-m-worried-about-how-an-organisation-has-handled-my-information/what-steps-should-i-take-if-i-have-experienced-a-data-breach/>

Report details of lost or stolen documents, such as passports, driving licences, credit cards and cheque books to the organisation that issued them. Inform your bank, building society and credit card company

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>

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

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

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

AI voice cloning uses 3 seconds of audio to clone a voice with 85% accuracy. Find out how these scams work in the UK and how to protect yourself.

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 advanced voice cloning is part of an organised criminal operation that harvests people's personal data to target victims with a wave of scam and nuisance calls. The process begins with a so-called 'lif

Voice cloning scams - Police Scotland

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

Voice cloning scams are when someone uses digital tools like AI to make a copy of your voice. They can then use this fake voice to pretend to be you. They could use your copied voice and use it for criminal act

AI Phishing Attacks on UK Businesses: 2026 Guide

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

The three main types of AI phishing shows up in three main forms: Fake emails, often called business email compromise, that impersonate a boss or supplier. Voice cloning, known as vishing, where

AI Phishing Examples: Deepfakes, Voice & Email Fraud

<https://www.adaptivesecurity.com/blog/ai-phishing-examples-real-world-deepfake-video-scams-voice-cloning-attacks-and-llm-generated>

Real-world AI phishing examples: deepfake video scams, voice cloning attacks, and LLM-generated email fraud, plus how to recognize and defend against them.

How to guard against voice cloning and deepfake scams - ICAEW

<https://www.icaew.com/insights/viewpoints-on-the-news/2025/jan-2025/how-to-guard-against-voice-cloning-and-deepfake-scams>

A new frontier opened up for financial crime in 2019. In what is considered the first case of its kind, fraudsters used an artificial intelligence (AI) voice clone of a German energy boss to scam the head

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 prevent AI voice cloning scams with our ultimate guide. Protect your organization from emerging threats and strengthen defenses.

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

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

AI voice scams use cloned voices to impersonate people you trust. Learn how these fake calls work, the warning signs and simple ways to protect yourself.

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 the UK isn't just a typical cold call but something far more convincing: an AI voice clone scam. Scammers are now using artificial intelligence (AI) to create f

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.

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

<https://hackershuh.com/awareness/phishing/smishing/>

Smishing is phishing delivered by SMS or mobile messaging. In 2026 the four dominant pretexts are package-delivery scams, bank-fraud alerts, tax-refund or fine notices, and corporate IT-helpdesk lures. SMS by

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>

Scam texts — also called smishing (SMS phishing) — are now one of the most common ways fraudsters reach UK consumers. They imitate banks, delivery firms, HMRC and even your own family to make you tap a li

How to spot & report phishing scams | National Cyber Security Centre

<https://www.ncsc.gov.uk/collection/phishing-scams>

Phishing scams: 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>

SMS spoofing is 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, or bank. Cybercriminals spoof SMS texts to sp

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

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

2026's most dangerous smishing scams exposed: Learn to identify and prevent SMS phishing attacks targeting your bank account, personal data, and financial security. Expert protection guide.

Banking and online account scams | FCA

<https://www.fca.org.uk/consumers/banking-online-account-scams>

Online banking scams Phishing scams Phishing is when fraudsters email or text you pretending to be from your bank. These messages will often ask you to verify information about yourself, including online b

11 Phishing Simulation Templates You Can Try in 2026

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

Explore 11 phishing simulation templates you can try in 2026 to strengthen your employees' cybersecurity skills and protect sensitive information.

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 Trends Report (Updated for 2026) - Hoxhunt

<https://hoxhunt.com/guide/phishing-trends-report>

Stay ahead of cyber threats with our 2026 phishing trends report. Featuring insights from 4M user clicks across 50M phishing simulations and real attacks.

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, how SMS spoofing works, real 2026 examples, warning signs to watch for, and a complete step-by-step guide to reporting them.

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: 20 July 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: 470
- Search sessions completed: 65
- Unique queries tracked: 6
- Pipeline runs executed: 6

Top Trending Keywords (Last 30 Days)

- initial access brokers (iab): 40 mentions
- ransomware — uk victims: 40 mentions
- scam-as-a-service: 40 mentions
- stolen uk credentials: 40 mentions
- uk phishing infrastructure: 40 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