Dark Web Weekly Intelligence Briefing

Week of 27 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

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

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 loginscams, credential theft tactics, and expert prevention strategies.

Scam Statistics in UK 2026 | Types, Losses & Key Consumer Facts
https://theworlddata.com/scam-statistics-in-uk/
Scamin United Kingdom2026Thescamlandscape in the United Kingdom has reached an alarming new threshold in2026, with official data from multiple government bodies and fraud prevention agencies confirmin

Phishing Statistics [2026]: Latest Attack Data & Trends
https://app.stationx.net/articles/phishing-statistics
Discover2026phishingstatistics 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,phishingemails drove mostsocialengineeringattacks. That has changed. According to Mandiant's M-Trends2026report, based on over 500,000 hours of incident response work, voicephis

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,UKconsumers are being targeted by increased attempts atsocialengineeringattacks, behavioral biometrics company BioCatch wa

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 internetscamsin 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 spotphishing, AI-generated deepfake

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 transformingsocialengineeringattacks in2026, from deepfakescamsto AI-poweredphishing, and learn how organizations can defend against them.

January 2026: Recent Threats & Social Engineering Trends
https://www.phishingbox.com/news/post/january-2026-recent-threats-social-engineering-trends
A breakdown of2026'stopsocialengineeringthreats, includingphishing, vishing, AiTM attacks, and credential exposure—and how to reduce risk.

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 transferscamsare all increasingly initiated through AI-enhancedsocialengineering.

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 and AIphishingin2026— vishing 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)

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

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

Initial Access Brokers (IABs): How Hackers Sell Access to Corporate ...
https://securifyai.co/blog/intial-access-brokers-how-hackers-sell-access-to-corporate-networks/
InitialAccessBrokeractivities typically target enterprise infrastructure across multiple environments. Platforms commonly targetedCorporateVPNportals Remote Desktop Protocol (RDP) servers Cloud infras

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

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

How initial access brokers price corporate access in 2026: an explainer ...
https://ransomnews.com/initial-access-brokers-pricing-2026/
A field guide to the 2026initial-access-brokermarket — how IABs sourceaccess, how they price it, who buys, and what the listings look like under the hood.

Initial Access Brokers: The Underground Market Selling Access to Your ...
https://lorikeetsecurity.com/blog/initial-access-brokers-corporate-risk
An IAB's core competency is getting intocorporateenvironments. They invest in expertise around exploiting exposedRDPendpoints, unpatchedVPNappliances (Fortinet, Pulse, Citrix, SonicWall, and Ivanti ha

Understanding initial access brokers and their impact on cyber security
https://zensec.co.uk/blog/understanding-initial-access-brokers-and-their-impact-on-cyber-security/
How doinitialaccessbrokersgainaccessto networks?Initialaccessbrokersuse a range of strategies to target networks, includingRDP,VPN, and phishing messages. Remote desktop protocolRDPis the most common

The Underground Economy of Access: How IABs Operate
https://www.darklake.global/blog/underground-economy-access-brokers
They buyaccess.InitialAccessBrokers(IABs) specialize in breachingcorporatenetworks and selling thataccessto the highest bidder. Types ofAccessIABs sell various forms of entry, including:RDP/VPNAccess:

IAB cybercriminals sell dark web access | WatchGuard Blog
https://www.watchguard.com/wgrd-news/blog/five-cybercriminal-entities-sell-access-2300-corporate-networks
Theseinitialaccessbrokersprovide details of stolenVPNand remote desktop protocol (RDP) accounts, as well as other credentials that criminals can use to break into the networks of more than 2,300 organ

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
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 service

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

1043 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

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

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

March 2026 Ransomware Report: 808 Victims, 65 Groups
https://www.breachsense.com/ransomware-reports/march-2026/
Here's what the March2026numbers tell us. March2026ransomwarenumbers at a glance March was the busiest month of2026so far. Here's what it means for you.Ransomwareleaksites are dark web pages whererans

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

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

2026 Data Breaches: Cybersecurity Incidents - PKWARE®

https://www.pkware.com/blog/2026-data-breaches

June was dominated bydata-theft extortion rather thanransomware. Researchers now describe ShinyHunters, the month's principal actor, as a durable cybercrime brand rather than a single crew; it ran a p

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 Users Targeted: 19,975 Passwords Leaked | HEROIC
https://heroic.com/darkhive-breaches/uk-users-targeted-19975-passwords-combolist-dump/
The file contained 19,975 compromisedcredentialsspecifically targeting United Kingdom-basedaccounts. Each record includes an email address, a plaintext password, and the URL of the service where thecr

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 mediaaccount, or your onlinebank, losing access to a digitalaccountcan be stressful. This guidance explains what you can do to minimise the damage, and how you can re

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.

DataBreach.com | Check If Your Information Was Exposed
https://databreach.com/
Find out if your personal information was compromised indatabreaches. Search your email on DataBreach.com to see where yourdatawas leaked and learn how to protect yourself.

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-fr
Jeremiah Fowler uncovered a huge database ofcredentialsspanning financial services, banking, social media, and dating apps without password or encryption protection.

16 billion passwords exposed in colossal data breach | Cybernews
https://cybernews.com/security/billions-credentials-exposed-infostealers-data-leak/
HOME / SECURITY / 16 billion passwords exposed in record-breakingdatabreach: what does it mean for you? The Cybernews research team, in collaboration with security researcher Bob Diachenko, has uncove

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

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 billionstolenrecordsdatadump, organisations should act quickly to assess and strengthen their security posture. Here are key steps to consider: 1. Check for ExposedCredential

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-breac
Report details of lost orstolendocuments, such as passports, driving licences, credit cards and cheque books to the organisation that issued them. Inform yourbank, building society and credit card com

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 employeecredentials, this leak is a disorganizeddatadumpwith little strategic value. Infostealers:

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

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

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

Voice cloning scams - Police Scotland

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

WhatvoicecloningscamsareVoicecloningscamsare 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

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 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 Phishing Attacks on UK Businesses: 2026 Guide

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

AIphishingattacks onUKbusinesses now work exactly like this. Criminals use artificial intelligence to clonevoices, fake video calls, and write flawlessscamemails.

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.

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

Anew frontier opened up for financial crime in 2019. In what is considered the first case of its kind, fraudsters used an artificial intelligence (AI)voiceclone of a German energy boss toscamthe head

AI voice-cloning scams could target millions of people, Starling Bank ...

https://www.cnn.com/2024/09/18/tech/ai-voice-cloning-scam-warning/

"Millions" of people could fall victim toscamsusing artificial intelligence to clone theirvoices,aUKbank has warned.

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.

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 (SMSphishing) — are now one of the most common ways fraudsters reachUKconsumers. They imitatebanks, delivery firms, HMRC and even your own family to make you tap a li

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

New rules to thwart text message scammers and protect consumers ... - Ofcom

https://www.ofcom.org.uk/phones-and-broadband/scam-calls-and-messages/new-rules-to-thwart-text-message-scammers-and-protect-consumers-and-businesse

Ofcom announces new rules to block, limit and disrupt criminal gangs who exploit mobile messaging services to scam victims Robust guidance to crack down on scam calls from abroad which "spoof"UKmobile

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.

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 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.

Types of scam calls, texts and messages - Ofcom

https://www.ofcom.org.uk/phones-and-broadband/scam-calls-and-messages/types-of-scam-calls-texts-and-messages

Scammers impersonating us, to obtain your personal information We have received reports of scam calls in which the caller claims to be from Ofcom, says there is a problem with the recipient's phone or

11 Phishing Simulation Templates You Can Try in 2026

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

Explore 11phishingsimulationtemplatesyou can try in2026to strengthen your employees' cybersecurity skills and protect sensitive information.

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

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

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.

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.

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: 27 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: 530
- Search sessions completed: 71
- Unique queries tracked: 6
- Pipeline runs executed: 7

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