LoughTec

IT • CYBER SECURITY

2026 THREAT BRIEFING

INSIDE THE DARK WEB

What every UK and Irish business needs to know about the criminal economy targeting them and how to defend themselves.

LoughTec
IT • CYBER SECURITY

WHY THE DARK WEB SHOULD BE ON YOUR RISK REGISTER

Most people picture the dark web as a shadowy corner of the internet were stolen data changes hands between hooded strangers.

The reality is far more unsettling.

It operates like a mature, professional marketplace, with vendors, customer reviews, subscription services, affiliate schemes and customer support.

If cybercrime were a country, its economy would rank among the largest on Earth.

For SMEs across the UK and Ireland, this matters for a simple reason, your business does not need to be famous to be a target. Automated tools harvest credentials, scan for weaknesses and package up access to networks at industrial scale. Attackers do not choose victims, their software does.

The arrival of accessible AI has accelerated everything.

Convincing phishing, cloned voices and adaptive malware are no longer nation-state capabilities, they are subscription products now.

UK businesses identified a cyber attack or breach in the last 12 months, most began with stolen or phished credentials of the kind traded daily on dark web markets.

WHAT YOU'RE UP AGAINST

LoughTec
IT • CYBER SECURITY

Not one enemy but an entire ecosystem of specialists.
By the time ransomware detonates, four or five separate groups may already have profited.

ORGANISED CYBERCRIME GROUPS
Run like companies, with developers, negotiators and HR. They build the tools and franchise them out, taking a cut of every attack their affiliates land.

SPECIALISTS & SERVICE PROVIDERS
Money launderers, phishing-kit designers and data brokers who never attack anyone directly — they just keep the machine running.

AFFILIATES
Smaller crews who rent the big groups' malware and infrastructure, doing the hands-on-keyboard work for a share of the proceeds.

MALICIOUS INSIDERS
Disgruntled staff and contractors monetising the access they already hold. Among the hardest threats to detect without monitoring.

INITIAL ACCESS BROKERS
Break into networks purely to sell the way in. A working VPN login for an SME can change hands before the victim notices anything.

HACKTIVISTS & STATE-BACKED GROUPS
Motivated by causes or geopolitics rather than money. SMEs get caught in the blast radius through supply chains.

LoughTec
IT • CYBER SECURITY

HOW THE CRIMINAL ECONOMY TRADES

Payment is almost always cryptocurrency

Monero increasingly favoured over Bitcoin

Deals are struck through encrypted messaging or in three main venues:

01 MARKETPLACES

Storefronts that mimic legitimate e-commerce: product categories, escrow payments, seller ratings and refund disputes. Trust systems keep the fraud economy honest among thieves, at least.

02 FORUMS & CHANNELS

Where reputations are built, recruits are found and tradecraft is shared. Much of this activity has spilled onto encrypted apps like Telegram, blurring the line with the mainstream communications.

03 LEEK SITES

Run by ransomware gangs as pressure tools: victims named publicly, deadlines counted down, stolen data drip-published to force payment. Extortion now matters as much as encryption.

Worth knowing, many attacks now skip encryption entirely.

Stealing data and threatening to publish it defeats the ‘we have backups’ defence statement which is why data protection matters as much as recovery.

WHAT'S BOUGHT AND SOLD

LoughTec
IT • CYBER SECURITY

Almost everything an attacker needs can be rented rather than built. 'As-a-service' crime has removed the skills barrier entirely:

RANSOMWARE-AS-A-SERVICE

Ready-made ransomware, payment portals and victim helpdesks, franchised to affiliates. The operator takes a cut of every ransom paid.

PHISHING-AS-A-SERVICE

Subscription kits with cloned login pages and hosting included. Modern kits proxy real logins in real time — capturing MFA codes as they're typed.

ACCESS & ATTACK SERVICES

DDoS-for-hire, exploit kits, credential-stuffing runs and brokered network access — attack capability priced like a business utility.

The commodities moving through these markets:

Credentials & 'fullz'

- harvested logins and complete identity packs used for fraud and account takeover

Business data

- invoices, contracts and email threads that make payment-diversion fraud frighteningly convincing

Personal & medical records

- fuel for spear phishing, insurance fraud and blackmail and many other types of coercion

Zero-day exploits & IP

- unknown software flaws, designs and trade secrets, prized by the most capable buyers

LoughTec
IT • CYBER SECURITY

THE PRICE OF YOUR BUSINESS, IN CRIMINAL MONEY

Indicative figures from recent threat-intelligence reporting — note how cheap the entry point to your business has become:

FROM ~ £5
A single set of stolen corporate login credentials — less than a lunch meal deal.

~ £15 – £80
Compromised remote access (RDP/VPN) to a business network, sold by access brokers.

~ £20 – £100
Cloned payment card data with verification details, priced by balance and freshness.

~ £200+
A sustained DDoS attack against a protected website, hired by the day.

~ £800 – £1,500
High-success-rate malware builds designed to evade mainstream antivirus.

~ £3,000+
A complete forged identity package — documents good enough to open accounts.

The maths that matters, an attacker can buy their way into a typical SME for less than a printer cartridge.
The resulting breach costs tens of thousands of pounds easily, before reputation and downtime are factored in.

LoughTec
IT • CYBER SECURITY

AI THE CURRENT & FUTURE THREAT MULTIPLIER

The biggest shift isn't a new type of attack, it's the speed, scale and polish AI has brought to the old ones:

PERFECT PHISHING

Machine-written lures in flawless English, matched to your suppliers' tone and timed to real business events. The tell-tale typo era is over.

AUTOMATED TARGETING

AI-driven reconnaissance scrapes company sites, LinkedIn and leaked data to build target profiles at scale, without human effort.

DEEPFAKE FRAUD

Cloned voices and video of directors used to authorise urgent payments, finance teams have wired six-figure sums to fake CEOs.

LOWERED BARRIERS

Criminal LLM services strip the safety rails off mainstream AI, writing scams and malware to order for a monthly fee.

ADAPTIVE MALWARE

Malicious code that rewrites itself to slip past signature-based antivirus, one reason legacy AV alone is no longer credible.

FASTER EXPLOITATION

The window between a flaw being disclosed and exploited keeps shrinking, patching ‘when we get to it’ is an unaffordable luxury.

LoughTec
IT • CYBER SECURITY

STAYING OFF THE SHELVES
THE ARP® APPROACH

You can't take your business off the internet, but you can make it a poor product for the dark web economy, expensive to break into, quick to detect intruders, holding nothing easy to monetise.

ASSESS

Know your exposure before criminals price it. We identify leaked credentials already circulating, audit your Microsoft 365 security posture and score your cyber maturity, an honest baseline, not a sales pitch.

REMEDIATE

Close the gaps that matter most, in priority order: multi-factor authentication done properly, mail-forwarding and sharing lockdowns, patching discipline and data protection controls.

PROTECT

Security is an operation, not a configuration: continuous dark web monitoring for your domains and credentials, managed detection and response, and training that turns staff into sensors.

WANT TO KNOW WHAT THE DARK WEB ALREADY HOLDS ON YOUR BUSINESS?

Book a no-obligation dark web exposure assessment

ISO 27001 certified, trusted by SMEs across the UK and Ireland.

LoughTec.com