CYXCEL®
TRACE

August 2025

The TRACE Brief

Welcome to the TRACE Brief,
CyXcel's monthly Cyber Threat Intelligence briefing.

Cyberattack Round-up

The past month has continued to see significant activity from financially motivated threat actors.

ShinyHunters carried out targeted attacks to steal data from several global brands through Salesforce CRM instances, impacting organizations across technology, retail and luxury goods. They employed sophisticated social engineering tactics, deceiving employees into granting them extensive APP access, which was used to facilitate the extraction of sensitive customer and business data. Organizations impacted include Google, Qantas, Allianz Life, LVMH and Pandora. The attacks did not exploit technical vulnerabilities in Salesforce itself but relied heavily on impersonation to bypass existing security controls, with stolen data subsequently being used for extortion or sold on dark web markets.

Co-op provided an update on the cyberattack impacting the organization earlier this year, confirming that data for all 6.5m members was stolen, including names, addresses and contact information.

The Tea dating advice app, a popular women-only platform, suffered a significant data breach at the end of July 2025, exposing thousands of sensitive user images, including documents used for age verification, and 1.1m private messages. Attackers gained access to legacy data exposing private conversations and raising serious privacy concerns, including risks of blackmail and emotional distress to those impacted in the breach.

Ingram Micro, a leading global technology brand and significant technology distributor in the UK, suffered a ransomware attack from the group SafePay, leading to encryption and the exfiltration of 3.5TB of data. The attack forced a shutdown of ordering, licensing and shipping systems globally, impacting 170,000 customers across 200 countries.

Key Takeaways

- Financially motivated threat actors continue to target global organizations both directly and through their supply chain.
- Significant cyberattacks such as ransomware can quickly disrupt operations, leading to customer dissatisfaction and mistrust, as well as downtime and escalating financial losses for impacted companies.
- Recent incidents highlight the evolving threat landscape where social engineering is increasingly being used to bypass defenses, and attackers are targeting the weak link in a supply chain.

UK Online Safety Act Updates

The UK Online Safety Act 2023 was introduced to make the internet safer, especially for children by placing legal duties on organizations such as social media companies, search engines and user-generated content platforms to tackle illegal and harmful online material. This includes age verification measures to restrict access to adult content and protect users from harmful content like bullying, hate speech and self-harm encouragement. The Act is enforced by Ofcom, which can fine companies or block services for non-compliance.

It has received increased media attention over the past month, with active regulation being enforced by Ofcom from 25 July that requires platforms impacted by the legislation to deploy "highly effective" age verification systems to prevent children from accessing pornography and other harmful material. This enforcement has brought the Act's implications into sharper public focus as users and companies confront practical challenges, including privacy concerns, the effectiveness of age checks and the rise in VPN use to bypass restrictions.

Since the age verification rules took effect, VPN use in the UK has surged, with Proton VPN reporting an 1,800% increase in user sign ups, and other free VPN services leading app downloads on the Apple App Store. Tor usage has also shown an increase, with users seeking other methods of bypassing verification, which; while offering anonymity, does pose significant risks of exposure to harmful or illegal content, whilst posing challenges to effective enforcement.

Key Takeaways

- ⓘ The UK Online Safety Act (2023) was introduced to make the internet safer, especially for children. Enforcement by Ofcom began on 25 July 2025.
- ⓘ VPN and Tor usage has increased since enforcement began, with users unwilling to give away personal information and using tools to circumnavigate legislative requirements - potentially exposing themselves to greater risk.

CYXCEL® *We offer fully integrated, customizable solutions that combine expertise in technology, cybersecurity, law, and geopolitics.*

Rescue

All aspects of incident management and response, to ensure your business emerges from a breach swiftly, effectively, and more resilient.

Resolve

A full-spectrum suite of services to strengthen your business against disruption and threats, while protecting its rights and reputation.

Transform

A bespoke service to upgrade your digital and cybersecurity infrastructure, covering everything from design to delivery.

Operate

Hosted and managed security solutions, specialist industry services, and on-demand access to extra capacity and skills augmentation.

TRACE

CYXCEL TRACE

August 2025

In Focus: Malware Stealers

Stealer malware is a type of malicious software designed to steal valuable information from affected computers.

The stealer ecosystem has evolved into a sophisticated supply chain that feeds virtually every other form of cybercrime and is increasingly being used by threat actors as a means of gaining initial access to organizations.

As well as valid usernames and passwords, stealer malware often contains valid session cookies or authentication tokens, allowing attackers to bypass multi-factor authentication.

The malware is typically deployed through phishing emails, free or cracked software, malicious advertisements or by exploiting known vulnerabilities in software. Data is sent back to a command-and-control server, and the data from the logs made available for sale.

Recent reporting showed that credentials available through infostealers enabled 54% of ransomware attacks, serving as the initial access vector. In March 2025 Jaguar Land Rover were impacted by a Hellcat ransomware attack, with access gained through compromised credentials targeting a third-party. This led to the exposure of around 350GB of data including proprietary documents, source code and employee information.

Types of Information Commonly Stolen

Type	Description
Usernames and Passwords	Login credentials for various accounts, often with valid session cookies or authentication tokens
Financial Information	Credit card numbers, bank account details
Personal Identification	Social Security numbers, driver's license
Email Credentials	Email account usernames and passwords
Browser Data	Saved passwords, cookies, browsing history
Cryptocurrency Wallets	Private keys, wallet addresses
Personal Files	Documents, photos, sensitive files
System Information	Computer and network configuration details
Software Licenses	Serial numbers, license keys
Gaming Accounts	Usernames and passwords for gaming platforms

Our Trace team monitors the dark web and digital communications platforms for client exposure and risk across three core areas.

CYXCEL TRACE

Data, Credentials and Access

We monitor for threats which pose the greatest risks to your organisation, searching across stealer marketplaces or initial access brokers offering valid credentials or access to your business, identification of leaked credentials and the offering for sale or exposure of company data.

Organisational Risk

Monitoring for adversarial chat which could indicate an impending or future cyber attack, the registration of domains which may be intended to spoof legitimate company infrastructure.

Supply Chain and Vendor Risks

We dig deeper, monitoring your critical supply chain partners to identify risks which might expose your data or risk downtime which might disrupt your business operations. If a breach does occur within your supply chain, we identify leaked data to allow you to assess the risks posed.