Monthly
CYBER THREAT INTELLIGENCE REPORT

July 2026

Version 1.0 July 2026

Prepared by **System Force IT**

Classification **TLP:CLEAR**

System Force I.T.
Secure IT Simplified

1 Executive summary

July was dominated by Microsoft SharePoint: a wave of actively exploited flaws drove repeated CISA additions and a dedicated hardening alert, alongside Microsoft's largest-ever Patch Tuesday, a Russian state zero-click email-theft campaign exposed by the NCSC, and a resurgent Qilin ransomware operation.

This briefing covers the most significant cyber incidents, emerging threats, vulnerability disclosures and ransomware activity of the month, drawn from primary sources including CISA, Microsoft, the NCSC and the ICO. It is written for business owners, IT leaders and risk managers who need a concise monthly picture without wading through fragmented vendor advisories.

- SharePoint was July's biggest story. Multiple actively exploited SharePoint flaws drove repeated additions to CISA's Known Exploited Vulnerabilities catalogue and a dedicated CISA hardening alert. Any business running on-premises SharePoint should patch now and check for compromise.
- Microsoft shipped its largest-ever Patch Tuesday, fixing well over 500 vulnerabilities, around three times June's total, with three publicly disclosed zero-days. Two, in SharePoint Server and Active Directory Federation Services, were already being exploited.
- The NCSC, part of GCHQ, and partners in 15 countries exposed LAUNDRY BEAR, a Russian state-supported group using a zero-click exploit named beehive to steal email from organisations running Zimbra webmail. Simply viewing a malicious message compromises a vulnerable server.
- In ransomware, Qilin surged more than fourfold year on year and ran neck and neck with The Gentlemen for the top spot through July, with Akira and DragonForce also highly active.
- A threat actor claimed to have stolen 35GB of source code and security keys from Accenture, underlining the exposure of source code and secrets and the value of tight access control around development systems.
- For UK businesses, the ICO gave a council worker a suspended sentence for unlawfully accessing hundreds of personal records, and the NCSC again urged UK organisations to sign up to its free Early Warning service.

2 Ransomware activity

443%
QILIN'S YEAR-ON-YEAR SURGE

146
ACTIVE GROUPS IN 2026

43.6%
SHARE HELD BY THE TOP FIVE

Qilin roared back in July, up more than fourfold year on year and accounting for roughly one in every five to six disclosed cases across more than 50 countries. It ran neck and neck with The Gentlemen for the top spot through the month, with Akira and DragonForce also among the most active operators.

Among the most active groups this month

Group	July activity
Qilin	Surged more than fourfold year on year; battled The Gentlemen for first place all month
The Gentlemen	Overtook and was overtaken by Qilin repeatedly through July
Akira	Remained one of the highest-volume operators
DragonForce	Continued to account for a disproportionate share of attacks

Across 2026, trackers recorded more than 7,500 ransomware victims across 146 active groups. Qilin's resurgence was the story of the month, up more than fourfold year on year, from around 250 to over 1,350 victims on its leak site, and trading first place with The Gentlemen throughout July. The market stays fragmented at the long tail but concentrated at the top, with the five largest groups accounting for roughly 44 per cent of all victims.

3 Vulnerability watch

570+	59	3	Record
MS VULNERABILITIES	RATED CRITICAL	ZERO-DAYS	LARGEST EVER PATCH TUESDAY

Microsoft's July Patch Tuesday was the largest in its history, roughly three times June's total, reinforcing that the era of small monthly updates is over as AI-driven vulnerability discovery accelerates. Two of the three publicly disclosed zero-days were already being exploited, and SharePoint was the dominant theme through the month.

Publicly disclosed zero-days

CVE	Component	Type
CVE-2026-56164	SharePoint Server	Elevation of privilege (exploited)
CVE-2026-56155	AD Federation Services	Elevation of privilege
CVE-2026-50661	Windows BitLocker	Security feature bypass

SharePoint under active exploitation

CVE	Product	Note
CVE-2026-56164	SharePoint Server	Zero-day, actively exploited
CVE-2026-45659	SharePoint Server	Deserialisation, added to CISA KEV
CVE-2026-58644	SharePoint	Added to CISA KEV
CVE-2026-50522	SharePoint	Deserialisation, added to CISA KEV
CVE-2026-46817	Oracle E-Business Suite	Added to CISA KEV
CVE-2026-16232	Check Point SmartConsole	Added to CISA KEV

CISA Known Exploited Vulnerabilities

CISA repeatedly added actively exploited flaws through July, heavily weighted towards SharePoint, alongside Oracle E-Business Suite, Check Point SmartConsole and Langflow, and issued a dedicated alert urging organisations to harden SharePoint. These are confirmed exploited in the wild and should be treated as patch-now priorities on internet-facing systems.

4 Notable incidents and breaches

Organisation	Sector	What happened	Actor
Accenture	Professional services	A threat actor claimed to have stolen 35GB of source code and various security keys	"888"
SharePoint servers (many)	Cross-sector	On-premises SharePoint compromised through actively exploited deserialisation flaws	Multiple
Zimbra users (multiple)	Government, defence, education, energy	Email stolen via the zero-click beehive exploit (see UK focus)	LAUNDRY BEAR

On-premises SharePoint was the month's most exposed platform

Several SharePoint flaws were actively exploited and repeatedly added to CISA's catalogue. Patch immediately, and assume compromise is possible on any server that was internet-facing before it was patched. SharePoint Online is managed by Microsoft, but self-hosted servers are entirely your responsibility.

These were among the month's most significant publicly reported incidents; given the pace of disclosure, more from July may yet come to light.

5 UK focus

Most global threat reporting is US-centric, but the UK picture has its own shape, set by UK regulation, the NCSC and the ICO. July's UK story was espionage and insider risk.

43%
UK BUSINESSES ATTACKED IN THE PAST YEAR

15
COUNTRIES EXPOSED LAUNDRY BEAR WITH THE NCSC

Zero-click
THE BEEHIVE EMAIL EXPLOIT NEEDS NO USER ACTION

NCSC exposes LAUNDRY BEAR, a Russian state email-theft campaign (23 July)

The NCSC, part of GCHQ, and partners in 15 countries exposed LAUNDRY BEAR, a Russian state-supported group stealing email from organisations running Zimbra Collaboration Suite. Its zero-click exploit, named beehive, needs no user action: simply viewing a malicious email in a vulnerable webmail server is enough to be compromised. Organisations using Zimbra should patch immediately and improve monitoring. The NCSC warns the technique could be adapted to other email platforms, and again urged all UK organisations to sign up to its free Early Warning service.

ICO and regulatory watch

In July the ICO secured a suspended sentence against a council worker who had unlawfully accessed hundreds of personal records, a reminder that insider misuse is a criminal matter, not only a disciplinary one. More broadly, the ICO continues to fine security failings after cyber attacks, with penalties averaging around £3.2 million in 2026, and it recently fined South Staffordshire Water £963,900 after a breach exposed data on around 633,000 people. Access controls, least privilege and monitoring of staff activity matter as much as defending the perimeter.

The government also brought UK businesses together during the month to pledge stronger cyber defences. The Cyber Security Breaches Survey 2026 found 43 per cent of UK businesses had experienced a breach or attack in the previous 12 months, with the revenue impact on smaller firms roughly doubling.

6 What this means for your business

1. **Patch on-premises SharePoint immediately.** Actively exploited zero-days drove repeated CISA additions and a dedicated hardening alert. Assume any internet-facing SharePoint server may already be compromised, and check for it.

2. **Patch and monitor email platforms.** The LAUNDRY BEAR zero-click campaign targets Zimbra and needs no user action; patch Zimbra now, and watch for the technique spreading to other webmail systems.

3. **Triage the record Patch Tuesday by what is confirmed exploited first.** Over 500 CVEs cannot be handled all at once. Prioritise the CISA KEV list and the two exploited zero-days in SharePoint Server and Active Directory Federation Services.

4. **Harden identity.** Multi-factor authentication everywhere, and tighten Active Directory and AD Federation Services given the exploited AD FS zero-day.

5. **Control insider access.** The ICO's council-worker case shows insider misuse carries criminal consequences. Enforce least privilege and monitor who accesses personal data.

6. **Keep tested offline backups and a tested recovery plan, and sign up to the NCSC Early Warning service** for free notifications of malicious activity on your network.

Not sure where your defences stand?

If anything in this report raises a question about your own systems, System Force IT offers a free, no-obligation IT and cyber security review. We are UKAS ISO/IEC 27001:2022 Certified and support businesses across Gloucestershire and the UK.

Call 01452 701355 · sales@systemforce.co.uk

Sources: BreachSense and Black Kite (ransomware); Microsoft, Qualys, BleepingComputer and Malwarebytes (Patch Tuesday); CISA and HivePro (Known Exploited Vulnerabilities); NCSC advisories of 13 and 23 July 2026 (Russian state activity and LAUNDRY BEAR); ICO enforcement notices (ico.org.uk); Cyber Security Breaches Survey 2026; CM-Alliance and TechCrunch (incidents). Figures reflect data available as at the end of July 2026.