Monthly
CYBER THREAT INTELLIGENCE REPORT

June 2026

Version 1.0 June 2026

Prepared by **System Force IT**

Classification **TLP:CLEAR**

System Force I.T.
Secure IT Simplified

1 Executive summary

June was defined by a clear shift away from file-encrypting ransomware towards straight data-theft extortion, Microsoft's largest-ever Patch Tuesday, and a change at the top of the ransomware leaderboard for the first time in 2026.

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.

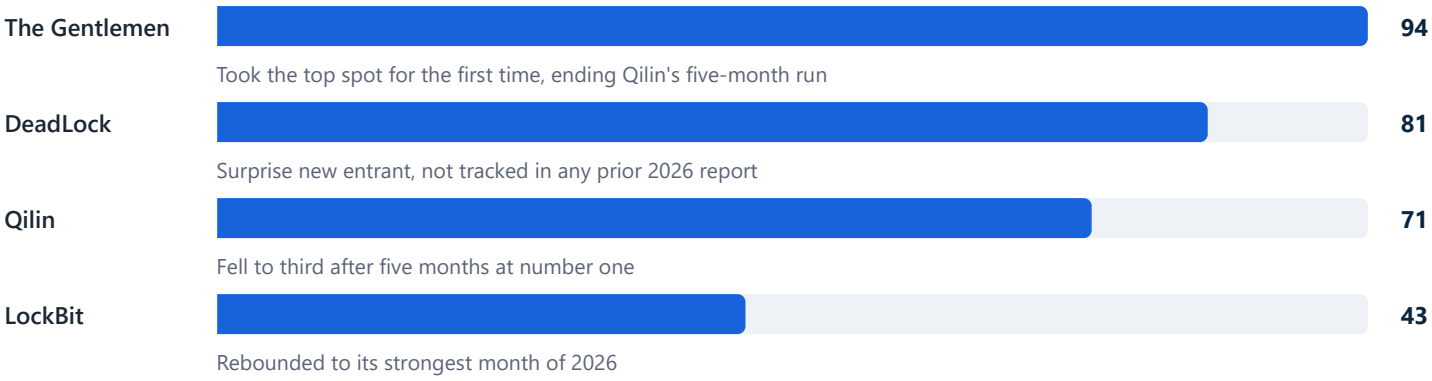
- Data-theft extortion overtook file-encrypting ransomware. The ShinyHunters group ran a pay-or-leak campaign across healthcare, insurance and entertainment by chaining an Oracle PeopleSoft zero-day with social engineering, shifting the risk from encrypted backups to sensitive-data exposure.
- Microsoft shipped its largest-ever Patch Tuesday, fixing 206 vulnerabilities including three publicly disclosed zero-days, with critical remote code execution in the Remote Desktop client, Hyper-V and Office.
- CISA added 23 actively exploited vulnerabilities to its catalogue, spanning internet-facing gear from Ivanti Sentry and Cisco SD-WAN Manager to SolarWinds Serv-U, Ubiquiti UniFi and the Linux kernel.
- Ransomware leak sites listed 707 victims across 63 groups. The Gentlemen led with 94, ending Qilin's five-month run; the previously untracked DeadLock surged to 81.
- For UK businesses, a breach is now a regulatory risk as well as an operational one: the NCSC issued a June alert on Fortinet firewalls, and the ICO continues to fine security failings after cyber attacks.

2 Ransomware activity

707	63	87
VICTIMS LISTED	ACTIVE GROUPS	COUNTRIES HIT

For the first time in 2026, Qilin was not the busiest group. After leading for five consecutive months it was displaced, in a leaderboard that continues to churn from month to month.

Most active groups, by victims claimed



Most-targeted sectors and countries

Sector	Victims	Country	Victims
Healthcare	54	United States	234 (33%)
Manufacturing	49	Germany	38
Construction	44	Italy	30

A growing share of groups now skip encryption entirely and run pure data-extortion operations. Reliable backups still matter, but they do not protect against the reputational and regulatory damage of a data leak, so preventing access and detecting exfiltration early become just as important.

3 Vulnerability watch

206	33	3	23
MS VULNERABILITIES	RATED CRITICAL	ZERO-DAYS	ADDED TO CISA KEV

Microsoft's June Patch Tuesday was the largest in its history. Two flaws reached CVSS 9.8, and critical remote code execution clustered in the Remote Desktop client, Hyper-V and Office.

Publicly disclosed zero-days

CVE	Component	Type
CVE-2026-49160	Windows HTTP.sys	Denial of service
CVE-2026-45586	Windows CTFMON	Elevation of privilege
CVE-2026-50507	Windows BitLocker	Security feature bypass

Selected critical remote code execution flaws

CVE	Product	Type	CVSS
CVE-2026-44815	Windows DHCP Client	Remote code execution	9.8
CVE-2026-47291	Windows HTTP.sys	Remote code execution	9.8
CVE-2026-45607 +2	Windows Hyper-V	RCE, guest-to-host escape	Critical
CVE-2026-44801 +6	Remote Desktop client	Remote code execution	Critical
CVE-2026-45648	Active Directory DS	Remote code execution	Critical
CVE-2026-45458 / 45456	Office (Word, Outlook)	Remote code execution	Critical

CISA Known Exploited Vulnerabilities

CISA added 23 actively exploited flaws in June (six zero-days), affecting Ivanti Sentry, Cisco Unified Communications Manager and Catalyst SD-WAN Manager, SolarWinds Serv-U, Splunk, Ubiquiti UniFi OS, Oracle PeopleSoft and the Linux kernel. 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
Novo Nordisk	Pharma	Clinical-trial and patient data accessed, 25m USD demand	Hunters International
Tata Electronics	Electronics	200,000+ internal files exfiltrated and leaked	Hunters Int. / World Leaks
One Medical (Amazon)	Healthcare	Senior-care records exposed via a third-party file store	ShinyHunters (claimed)
Eastman Kodak	Manufacturing	Around 2 million records exposed	ShinyHunters
DentaQuest	Dental benefits	2.6 million accounts affected	Unknown
Nintendo	Gaming	Job-applicant data stolen via a third-party platform	Unknown
Chelan County, WA	Local government	Three-week outage of networks, phones and email	Malware

One Medical: third-party storage is still your risk

The weak point was a supplier, not the organisation's own core systems, the pattern that ran through June. Outsourcing a function does not outsource the risk; supplier security needs the same scrutiny as your own.

Silent Ransom Group: the phone call is the attack

The group targeted law firms with fake IT-support phone calls, persuading staff to grant remote access. No software vulnerability is involved, which makes staff awareness the primary defence, however well patched your systems are.

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.

43%
UK BUSINESSES ATTACKED IN THE PAST YEAR

£963,900
ICO FINE, SOUTH STAFFS WATER (MAY)

£3.2m
AVERAGE ICO PENALTY, 2026

NCSC alert: Fortinet firewalls and VPN gateways (18 June)

The NCSC warned of a global campaign after a threat actor leaked a database of credentials gathered by credential-stuffing internet-facing FortiGate and VPN portals, with indications of potential UK impact. Its advice: check the FortiBleed asset checkers, look for indicators of compromise, and factory-reset compromised devices, because changing credentials alone may not remove an attacker with persistence. Then enforce MFA on all VPN and management logins and keep management interfaces off the internet.

ICO and regulatory watch

A breach is now a regulatory problem, not only an operational one. The ICO has shifted to fewer but far larger penalties, averaging around £3.2 million in 2026, and increasingly fines security failings after cyber attacks. In May it fined South Staffordshire Water £963,900 under the UK GDPR security provisions after a cyber incident exfiltrated data on around 633,000 people, following a £1.23 million fine for LastPass UK and the landmark £14 million penalty against Capita, where a high-priority alert fired within ten minutes but the affected device was not isolated for 58 hours. The lesson for UK SMEs: slow detection and response now carry a direct financial cost.

The government's 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. UK organisations breached in June included the University of Nottingham.

6 What this means for your business

1. **Patch internet-facing systems first.** Edge devices and remote-access tools (Ivanti Sentry, Cisco SD-WAN, SolarWinds Serv-U, Ubiquiti UniFi, Fortinet) and Windows RDP, Hyper-V and Active Directory were all in the firing line. Prioritise anything on the CISA KEV list.

2. **Treat data theft as a board-level risk.** With extortion shifting away from encryption, backups alone are no longer enough. Focus on preventing access and detecting data leaving the network.

3. **Harden identity and third-party access.** MFA everywhere, least-privilege access, and a real review of what suppliers can reach. Several June breaches came through third parties.

4. **Train people against social engineering.** The Silent Ransom Group's fake IT-support calls show a convincing phone call can bypass good technology.

5. **Keep tested, offline backups and a tested recovery plan.** Chelan County's three-week outage is what happens without one.

6. **Know and test your breach response times.** The ICO's Capita fine turned on a device left unquarantined for 58 hours. In the UK, a slow response now carries a regulatory cost.

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 (ransomware); Microsoft, Qualys, BleepingComputer (Patch Tuesday); CISA and HivePro (KEV); NCSC alert of 18 June 2026 (Fortinet); ICO enforcement notices (ico.org.uk); Cyber Security Breaches Survey 2026; CM-Alliance and TechCrunch (incidents). Figures checked at time of writing and should be verified before distribution.