ncc group

FOX IT
part of ncc group

Scattered Spider Update

July 2025

Executive Summary

Scattered Spider has broadened their operations to include campaigns against the insurance and aviation sectors.[1] This follows on from the targeting of the retail sector, which was initially reported by NCC Group on 1st May 2025. The associated Threat Briefing for their campaign against Retail can be accessed here.

The following points summarise the key findings from this research output:

- Scattered Spider is a financially motivated threat group that conducts crafty social engineering campaigns to gain unauthorised access into the target environment.
- Several security incidents have been reported across Aviation and Insurance by major organisations such as WestJet, Hawaiian Airlines, Qantas, Aflac, Erie Insurance and Philadelphia Insurance in June and early July 2025.
- These incidents have not been officially attributed to Scattered Spider, however, some of the observed behaviours resemble the group's operations.
- Aviation presents a high-value target for this adversary given the highly sensitive data, which is collected, processed and stored across the sector daily, and thus, providing opportunities for data theft and extortion.
- The opportunity to cause a major operational disruption during the peak travelling summer season could be weaponised by Scattered Spider to apply additional pressure to aviation organisations, where ransom cases are concerned.
- Like the aviation sector, insurance companies collect, process and hold high volumes of sensitive data such as Personally Identifiable Information (PII), thus, making it a high targeting priority for Scattered Spider.
- Insurance's unique position within the wider financial services' sector and Critical National Infrastructure (CNI) makes it an extremely attractive target for the group, as there is the opportunity to target further organisations connected.
- A sample attack chain highlighting Scattered Spider's operational sophistication has been included alongside key Indicators of Compromise (IOCs) and Tactics, Techniques, and Procedures (TTPs) observed during the period May to July 2025.

Scattered Spider Overview and Modus Operandi

Aliases: 0ktapus, DEV-0971, Muddled Libra, Octo Tempest, Oktapus, Scatter Swine, Scattered Swine, Starfraud, Storm-0971, UNC3944

Targeted Sectors: Retail, Aviation, Insurance, Telecommunications, Critical National Infrastructure (CNI)

Targeted Regions: Europe, North America

The threat collective has been operating since at least 2022, with their main motivation being financial gain. This is typically achieved through conducting crafty social engineering campaigns to gain initial access into the target environment. A distinct feature of this group is the human element behind their operations that includes young individuals between the ages 19 and 20, mainly from Western countries such as United Kingdom (UK) and North America (NA). A brief overview of their typical modus operandi pinpoints to:[2,3,4,5]

- **Social Engineering:** Excelling in social engineering tactics with a heavy focus on phishing, SIM swapping, and multi-factor authentication (MFA) fatigue (push bombing) attacks.
- **Impersonation**: Posing as IT staff to trick individuals into divulging extremely sensitive information such as credentials or granting remote access to resources.
- **Exploiting Vulnerabilities:** Known to utilise specific vulnerabilities (such as CVE-2015-2291) and relying on tools such as STONESTOP and POORTRY to disarm security software.
- **Persistence and Lateral Movement:** Using legitimate remote access tools, such as AnyDesk and LogMeIn, to maintain access and progress laterally within the victims' networks.
- **Ransomware:** Deploying DragonForce ransomware, and previously, RansomHub and BlackCat (or ALPHV) ransomware.

Aviation

In their most recent attacks, Scattered Spider has continued to rely on sophisticated social engineering techniques to exploit identity-focused software and help desks for unauthorised access to airlines, which was confirmed by The Federal Bureau of Investigation (FBI) in a warning released on X/Twitter on 28th June 2025.

A potential uptick in the group's attack volume was also suggested concerning anyone else in the airline ecosystem, for example, trusted vendors and contractors, which could indicate a supply chain attack.[6]

In early July, Charles Carmakal, the Chief Technology Officer (CTO) of Mandiant, a subsidiary of Google, confirmed that "multiple incidents in the airline and transportation sector" have been observed resembling Scattered Spider's TTPs.[7] Airlines such as WestJet, Hawaiian Airlines and Qantas reported security related incidents in the period 13th June 2025 to 2nd July 2025.[8,9,10] There is limited information available for these incidents due to the ongoing investigations, however, the airlines confirmed the following impact: WestJet experienced internal systems disruption which specifically affected their mobile application. Hawaiian Airlines' incident has only impacted their non-critical IT operations while Qantas' call centre platform was accessed exposing the personal data of over 6 million of their passengers. Some of the observed behaviours in these incidents suggest possible alignment with the recent warnings about Scattered Spider's increased focus on the sector.

The group's social engineering prowess could yield highly successful results when considering the typical operations taking place within Aviation, for example, the heavy utilisation of third parties (or contractors and software) to efficiently conduct business as usual (BAU) activities. Such high utilisation of external parties presents a higher cyber risk when it comes to protecting sensitive data. Aviation enterprises would be considered as high-value targets for the adversary given the vast amount of highly sensitive data, for example, passenger details, which they collect, process and store daily. As a result, this provides a substantial basis for the group to concentrate on gaining unauthorised access to victims' critical assets for the purpose of data theft and extortion.

The sector also plays a crucial part in global economic development and connectivity through generating a substantial revenue, enabling international trade, and facilitating freight transportation.[11] For example, the UK aviation sector alone, which includes commercial, general and military segments, has an estimated market value of £3.92 billion this year, with the expectation to reach £5.61 billion in the next 5 years, or by 2030.[12] This specifically highlights what a lucrative target the sector is for this financially motivated threat collective.

The opportunity to cause major operational disruption during the peak travelling season (or summer) is another important factor which could be weaponised by the group to apply additional pressure to organisations, when ransom cases are concerned, to avoid disruption or the complete unavailability of their systems and resources.[13] As such, organisations within the sector would benefit from taking a proactive stance to their defensive approach and monitoring for any activity resembling Scattered Spider's TTPs.

Insurance

In mid-June, Google Threat Intelligence Group (GTIG) alerted on their observations related to multiple intrusions in the US insurance sector, which resembled Scattered Spider's activity, urging organisations within the sector to remain vigilant.[14] From the 7th to 20th June 2025, major providers in the US, including Aflac, Erie Insurance and Philadelphia Insurance reported security incidents.[15,16,17] It is important to note that these cases have not been officially attributed to Scattered Spider, however, it is widely believed that the threat collective is responsible for them. The observed activity appears to align with Scattered Spider's already well-established attack pattern of targeting a specific sector with a high attack volume, before switching to another sector. Large insurance businesses which tend to incorporate substantial help desk functions or even outsourced IT functions, would be of particular interest to the group.

Insurance's unique position within the wider financial services' sector and CNI makes it an extremely attractive target to a variety of threat actors including financially motivated Organised Criminal Groups (OCGs), nation-states, and hacktivists. The sector collects, processes and holds high volumes of sensitive data such as PII making it a high targeting priority for Scattered Spider. The adoption of cloud services and artificial intelligence (AI) combined with the heightened focus on process automation within the sector, due to the ever-growing customer demand for highly efficient services, has expanded the attack surface for insurance enterprises, making them more susceptible to cyber-attacks including, but not limited to, ransomware and supply chain attacks.[18]

A lot of the targeting criteria which was discussed for aviation also applies to Insurance. As part of the wider financial services sector, insurance is required to adhere to the relevant regulatory requirements which present a distinct operational challenge but could also present an increase in adversarial targeting. Breaches occurring within the sector because of a cyber-attack often result in hefty regulatory fines and penalties when an institution fails to adequately safeguard customer data, adhere to the relevant industry standards, or report the incident promptly.[19]

Many cyber adversaries, such as ransomware operators, are also familiar with the applicable fines and penalties and exploit such regulatory practices to further pressure their targets, especially when ransom payments are concerned. Scattered Spider's notable associations with ransomware groups such as DragonForce and RansomHub could enable them to exploit this distinctive feature.

Given Scattered Spider's history of concentrating on a single sector at a time within Western/English-speaking organisations, larger insurance organisations in these regions are advised to remain vigilant and proactively monitor their environments for activity which could align to the observed TTPs for Scattered Spider.

Scattered Spider

Attack Chain
A sample attack chain based on recently observed campaigns in the period May to July 2025 is captured in the table below.

Tactic	Technique (ID & Title)	Procedure / Tool / Detail
Resource Development	T1583.001: Acquire Infrastructure: Domains	Register phishing domains for luring
Initial Access	T1556: Phishing	Phishkits
	T1078: Valid Accounts	Purchased/stolen credentials or session tokens
	T1025: Data from Removable Media	SIM swaps via telecom/BPO access
	T1199: Trusted Relationship	Abuse trusted relationships of contracted IT help desks to gain access to targeted organisations
Execution	T1204: User Execution	Fake login portals, malicious links
	T1219: Remote Access Software	AnyDesk, LogMeIn, ScreenConnect, Tactical RMM, TeamViewer, RustDesk, Level.io, Pulseway, Tailscale, TeamViewer, spectreRAT, WarZone
Persistence	T1136: Create Account	New user identities
	T1556.006: Modify Authentication Process	MFA token registration or manipulation
	T1078: Valid Accounts	Continued access via compromised credentials
Privilege Escalation	T1068: Exploitation for Privilege Escalation	Malicious drivers
	T1078.004: Valid Accounts: Cloud Accounts	Permissions escalation
	T1484.002: Domain Policy Modification; Domain Trust Modification	Adds federated identity provider to the victim's SSO tenant and enables automatic account linking
Defense Evasion	T1656: Impersonation	Password reset, MFA removal
	T1562.001: Impair Defenses: Disable or Modify Tools	Malicious driver
Credential Access	T1003: OS Credential Dumping	Mimikatz, LaZagne
	T1552: Unsecured Credentials	Raccoon, VIDAR, Atomic, ULTRAKNOT, Stealc
Discovery	T1213.002: Data from Information Repositories	SharePoint enumeration
	T1018: Remote System Discovery	ESXi discovery scripts
	T1482: Domain Trust Discovery	AD Enumeration
Lateral Movement	T1021: Remote Services	Impacket, SSH
	T1538: Cloud Service Dashboard	AWS Systems Manager, Azure, vSphere
Collection	T1005: Data from Local System	Raccoon, VIDAR
	T1213: Data from Information Repositories	Cloud sync tools
Exfiltration	T1567.002: Exfiltration Over Web Service: Exfiltration to Cloud Storage	Rclone, MegaSync, Dropbox, StorageExplorer
	T1048: Exfiltration Over Alternative Protocol	Ngrok
Impact	T1486: Data Encrypted for Impact	BlackCat, DragonForce

Scattered Spider - IOCs[20,21,22,23]

Indicators of compromise associated with Scattered Spider's intrusions remain limited, making detection and attribution challenging. However, the group's heavy use of social engineering has revealed recurring patterns, particularly in how they register domains that closely mimic legitimate company infrastructure or login portals. Their typical naming conventions include:

- victimname-sso[.]com
- victimname-okta[.]com
- victimname-servicedesk[.]com
- sso-victimname[.]com
- servicenow-victimname[.]com

The table below captures IOCs associated with Scattered Spider for the period May to July 2025. Some IOCs were identified independently using OSINT tools, specifically Censys, VirusTotal, Triage, URLScan, and Shodan.

Indicator	Description
Domains	ai-sso[.]com
	aliasintelligence-sso[.]com
	amci-sso[.]com
	asurion-sso.net
	bit-sso[.]com
	bses-sso[.]com
	bytedance-sso[.]com
	collegenet-sso[.]com
	grid-sso[.]com
	jlr-sso[.]com
	meta-sso[.]com
	dfm-sso[.]com
	mygov-sso[.]com
	orthoscan-sso[.]com
	oss-sso[.]com
	sport-sso[.]com
	trustetc-sso[.]com
	verify-sso[.]com
	klv1[.]it[.]com
	sso-accountservices[.]com
	sso-akb[.]com
	sso-binance[.]com
	sso-crypto[.]com
	sso-dms[.]com
	sso-gservices[.]com
	sso-juliusbaer[.]com
	sso-juliusbaer.net
	sso-juliusbar[.]com
	sso-juliusbar.net
	sso-ki[.]com
	sso-mydf[.]com
	sso-mygov[.]com
	sso-nutrition[.]com
	sso-ontic[.]com
	sso-relay[.]com
	sso-rhisac[.]com
	sso-roblox[.]com
	sso-sa[.]com
	sso-securelogin.net
	sso-socure[.]com
	sso-solanocounty[.]com
	sso-update[.]com
	sso-venndigital[.]com
	sso-x[.]com
	sso-zweiplus[.]com
	servicenow-moveworks[.]com
	servicenow-paulpace[.]com
	servicenow-talentrecruitment[.]com
	alldus-servicenow[.]com
	iss-servicenow[.]com
	themeweaver-servicenow[.]com
	travelportprod-servicenow[.]com
	ametek-servicedesk[.]net
	mgb-servicedesk[.]org
	anddigital-servicedesk[.]com
	tirerack-servicedesk[.]com
	tirerackwholesale-servicedesk[.]com
	markel-servicedesk[.]com
	internal-servicedesk[.]com
	uts-servicenow[.]com
	ametek-servicenow[.]net
	microsoftoffice-login[.]com
	okta.microsoftoffice-login[.]com
	sso.microsoftoffice-login[.]com
	chipotle-sso[.]com
	gemini-servicedesk[.]com
	carlsondesigngroup-servicedesk[.]com
	devonindustrial-servicedesk[.]com
	cna-servicedesk[.]com
	lrqa-servicedesk[.]com
	hubspot-okta[.]com
	dfm-okta[.]com
	binance-okta[.]com
	devonindustrial-okta[.]com
	nexo-okta[.[com
	alm[.]gg
	synlace[.]ai

	kennedywilsoninc[.]com
	okta.kennedywilsoninc[.]com
	update.kennedywilsoninc[.]com
	verify.kennedywilsoninc[.]com
	www-mlcrosoft[.]com
	account.www-mlcrosoft[.]com
	sso.www-mlcrosoft[.]com
	ssoo.www-mlcrosoft[.]com
	mcicrosoft[.]com
	microsoff[.]net
	sso.mcicrosoft[.]com
	sso.microsoff[.]net
	ssoo.mcicrosoft[.]com
	ssoo.microsoff[.]net
IPs	198[.]199[.]71[.]206
	192[.]81[.]219[.]116
	18[.]117[.]173[.]7

Scattered Spider – TTPs

A complete set of TTPs utilised by Scattered Spider in the period May to July 2025 is captured in the table below.

MITRE ID	Technique Name
T1047	Windows Management Instrumentation
T1071.001	Web Protocols
T1497.002	User Activity Based Checks
T1059.004	Unix Shell
T1134.001	Token Impersonation/Theft
T1016	System Network Configuration Discovery
T1497.001	System Checks
T1566.002	Spearphishing Link
T1566.001	Spearphishing Attachment
T1547.001	Registry Run Keys / Startup Folder
T1012	Query Registry
T1059.001	PowerShell
T1027	Obfuscated Files or Information
T1003.003	OS Credential Dumping: NTDS
T1036.005	Match Legitimate Name or Location
T1204.001	Malicious Link
T1003.001	LSASS Memory
T1574	Hijack Execution Flow
T1083	File and Directory Discovery
T1190	Exploit Public-Facing Application
T1055.001	Dynamic-link Library Injection
T1189	Drive-by Compromise
T1583.001	Domains
T1584.001	Domains
T1562.001	Disable or Modify Tools
T1562.004	Disable or Modify System Firewall
T1486	Data Encrypted for Impact
T1071.004	DNS
T1574.002	DLL Side-Loading
T1574.001	DLL Search Order Hijacking
T1555.003	Credentials from Web Browsers
T1134.002	Create Process with Token
T1584	Compromise Infrastructure
T1123	Audio Capture

DragonForce

IOCs[24,25,26]
The table below captures IOCs associated with DragonForce ransomware in the period May to July 2025.

Indicator	Description
SHA256	b10129c175c007148dd4f5aff4d7fb61eb3e4b0ed4897fea6b33e90555f2b845
	cee6a7663fad90c807c9f5ea8f689afd0e4ece04f8c55d7a047a7215db6be210
	c844d02c91d5e6dc293de80085ad2f69b5c44bc46ec9fdaa4e3efbda062c871c
	005ed5de8a3e72a91f8a2e0d2a3088c41c681feb70dffbd9097e22c288b6b70c
	a31f222fc283227f5e7988d1ad9c0aecd66d58bb7b4d8518ae23e110308dbf91
	822ceefb12b030f2ff28dcda6776addda77b041dbb48d2e3a8c305721f4cc8ef
	f862d24a5bd536d8b0ba17b59ed9a215580337337c3ee3858b4bacedd849c681
	a9fc91dda5c6f16904e8fe7ca298a7895674232ad77e5ef5c232b77e86df127c
	01f1e82d4c2b04a4652348fb18bb480396db2229c4fd22d2be1ea58e6bf4a570
	b714cb02cfd5d67e1502b45242636ee6b35c1b609072d3082378c50a177df15d
	80e3a04fa68be799b3c91737e1918f8394b250603a231a251524244e4d7f77d9
	d06b5a200292fedcfb4d4aecac32387a2e5b5bb09aaab5199c56bab3031257d6
	24e8ef41ead6fc45d9a7ec2c306fd04373eaa93bbae0bd1551a10234574d0e07
	6677e07bcccdeb28e532bb030f2ff2e4e39049caf6a1a0f9cd7f50e6d829daac
	f5df98b344242c5eaad1fce421c640fadd71f7f21379d2bf7309001dfeb25972
	005ed5de8a3e72a91f8a2e0d2a3088c41c681feb70dffbd9097e22c288b6b70c
	d67a475f72ca65fd1ac5fd3be2f1cce2db78ba074f54dc4c4738d374d0eb19c7
	6782ad0c3efc0d0520dc2088e952c504f6a069c36a0308b88c7daadd600250a9
	8a193db0ff08237f63c036d422f52276a4e575476763dc391455ed5b12269c07
	b714cb02cfd5d67e1502b45242636ee6b35c1b609072d3082378c50a177df15d
	70afd8efb34382badead93ae104d958256de6be8054227ccc85fe95d5c5f9db0
	b9ee022489931c6b68b63b0ae34eb1b4ef141e9bb456e84034603a9ae04e5db9
	a399a293cc3f25f6250ebee65e6e60e818831925769d540354275e9ad87bb5bb
Files	socks.exe Path: :\Users\username\AppData\Local\Temp\2\ socks aug\socks.exe
	a65.exe Path: C:\Users\username\AppData\Local\Temp\ 2\a65.exe
	netscanold.exe
	df.exe

The table below contains the top exploited vulnerabilities associated with DragonForce.

CVE	Product	Impact	CVSSv3 Score
CVE-2021-44228	Apache Log4j2 (“Log4Shell”)	Remote Code Execution (RCE)	10
CVE-2023-46805	Ivanti Connect Secure and Policy Secure	Authentication Bypass	8.2
CVE-2024-21412	Microsoft Windows SmartScreen	Security Feature Bypass	8.1
CVE-2024-21887	Ivanti Connect Secure and Policy Secure	Command Injection	9.1
CVE-2024-21893	Ivanti Connect Secure and Policy Secure	Path Traversal	8.2

DragonForce – TTPs
A complete set of TTPs related to DragonForce in the period May to July 2025 is available in the table below.

MITRE ID	Technique Name
T1047	Windows Management Instrumentation
T1071.001	Web Protocols
T1497.002	User Activity Based Checks
T1059.004	Unix Shell
T1134.001	Token Impersonation/Theft
T1016	System Network Configuration Discovery
T1497.001	System Checks
T1566.002	Spearphishing Link
T1566.001	Spearphishing Attachment
T1547.001	Registry Run Keys / Startup Folder
T1012	Query Registry
T1059.001	PowerShell
T1027	Obfuscated Files or Information
T1003.003	OS Credential Dumping: NTDS
T1036.005	Match Legitimate Name or Location
T1204.001	Malicious Link
T1003.001	LSASS Memory
T1574	Hijack Execution Flow
T1083	File and Directory Discovery
T1190	Exploit Public-Facing Application
T1055.001	Dynamic-link Library Injection
T1189	Drive-by Compromise
T1583.001	Domains
T1584.001	Domains
T1562.001	Disable or Modify Tools
T1562.004	Disable or Modify System Firewall
T1486	Data Encrypted for Impact
T1071.004	DNS
T1574.002	DLL Side-Loading
T1574.001	DLL Search Order Hijacking
T1555.003	Credentials from Web Browsers
T1134.002	Create Process with Token
T1584	Compromise Infrastructure
T1123	Audio Capture

Recommendations

Practical Guidance Against Scattered Spider[27,28,29]

The adversary operates with urgency; for example, the group has breached organisations, established persistent access, exfiltrated data and detonated ransomware within a matter of hours. As such, mitigations implemented by organisations operating within the aviation and insurance sectors should be in-depth to ensure adequate coverage of both the technical and human elements of their infrastructure.

Reinforce Help Desk Security Protocols

- Educate Help Desk users on the prevalence of these social engineering attacks/campaigns.
- Consider implementing escalation pathways for sensitive account reset requests.
- Never reset MFA or passwords without high-assurance identity verification [see below].
- Identity verification:
  - Verify the user's identity on video call where they must present valid ID.
  - If a user's identity cannot be verified through standard process, have the user's line manager or a third party confirm their identity.
  - Verify the caller's phone number is known or listed as belonging to the user. Where it cannot be verified or if suspicious, contact the user using an out-of-bands medium to verify the account reset.
  - Ask the user job-specific questions with verifiable answers an impersonator would not know, e.g:
  - Who is your line manager or a colleague you work with daily?
  - Name two internal systems you use daily outside of Office365.
  - Name an internal email address or mailing list which you receive emails from.

Note: If your Helpdesk function is outsourced to an external provider, it is recommended to contact that organisation and request an outline of the verification checks they take prior to resetting accounts, as well as the protocols they have in place to mitigate the attack techniques associated with Scattered Spider.

Harden Identity and Access Management

- Require phishing-resistant MFA, i.e., hardware tokens or app-based authentication instead of SMS or email codes, where possible.
- Implement just-in-time access and least privilege policies on admin accounts.
- Audit inactive accounts, especially third-party contractors and former employees, to ensure they have been correctly decommissioned.

Monitoring

- Ensure complete visibility across all infrastructure, identity, and critical management services.
- Ensure complete segregation of identities throughout infrastructure.

Based on previous Scattered Spider campaigns, specific attention should be paid to identify the following:

- The presence or use of credential dumping tools and/or abnormal privilege escalation.
- Attempts at lateral movement within identity infrastructure.
- Unusual use of remote admin tools like PowerShell or PsExec.
- Unusual use of remote access tools on networks.
- The creation of unusual hosts or virtual machines on managed domains.

Backups and Recovery

- Maintain offline backups of data with regular backup and restoration (daily or weekly as advised by CISA).
- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, and secure location.

About NCC Group

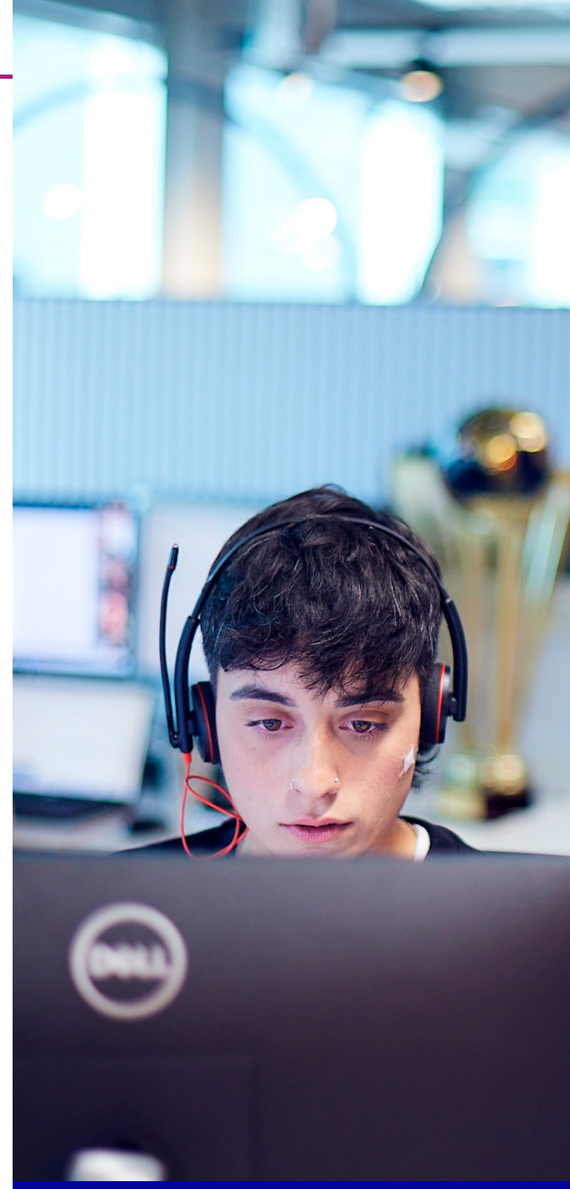
"People powered, tech-enabled cyber security"

We're a people powered, tech-enabled global cyber security and resilience company withover 2200 colleagues around the world.

For over 25 years, we've been trusted by the world's leading companies and Governments to manage and deliver cyber resilience, working together to create a more secure digital future. We are proud to deliver important and groundbreaking projects for our clients.

We operate as one global business, with in-country delivery tailored to local needs and cultures, as well as a global delivery team to respond quickly to our client's challenges. We have a significant market presence in the UK, Europe, North America and APAC, including our global delivery and operations centre in Manila, the Philippines.

+44 (0)161 209 5200
response@nccgroup.com
www.nccgroup.com




ncc
group


FOX IT
part of ncc group