DomainTools

THREAT BRIEF

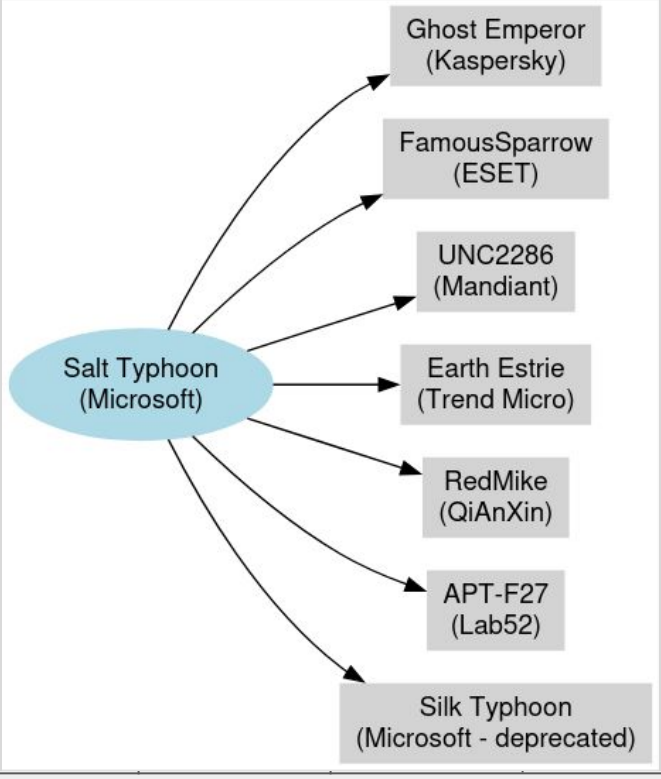
Inside Salt Typhoon: China's State-Corporate Advanced Persistent Threat

Operational Structure, Campaigns, and Tradecraft

Background

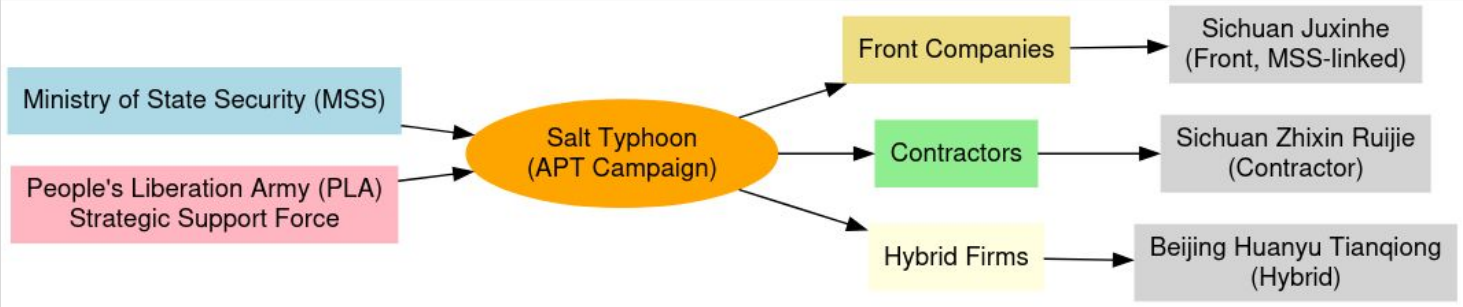
Salt Typhoon is a People's Republic of China (PRC) state-sponsored cyber threat group aligned with the Ministry of State Security (MSS), **specializing in long-term espionage operations targeting global telecommunications infrastructure**. Active since at least 2019, Salt Typhoon has demonstrated advanced capabilities in exploiting network edge devices, establishing deep persistence, and harvesting sensitive communications data. The group's targets include the U.S., U.K., Taiwan, and EU, with confirmed breaches in at least a dozen U.S. telecom firms, multiple state National Guard networks, and allied communications providers.

Salt Typhoon operates with both direct MSS oversight and the support of pseudo-private contractor ecosystems, **leveraging front companies and state-linked firms to obscure attribution**. However, their use of publicly-trackable domains registered with false U.S. personas marks a rare lapse in tradecraft, providing new insights into the PRC's espionage activities and priorities.



DomainTools

Salt Typhoon's Operational Structure



Salt Typhoon activity is consistent with the model observed across other PRC "Typhoon" actors: centralized tasking from the Ministry of State Security (MSS), supplemented by the use of contractor and front-company ecosystems that provide scalable infrastructure, tooling, and deniability, allowing MSS operators to mask espionage as commercial or third-party actions.

Organization	Connection to Salt Typhoon
Ministry of State Security (MSS)	Primary civilian intelligence service responsible for foreign intelligence, counterintelligence, and cyber-enabled espionage. Primary beneficiary of Salt Typhoon activity.
People's Liberation Army (PLA)	The military wing of the Chinese Communist Party. Salt Typhoon's targeting of backbone and edge routers suggests technical overlap with PLA's mandate to prepare battlefields in cyberspace.
Sichuan Juxinhe Network Technology (四川聚信和)	Likely MSS front company. Facilitated domain control, server management, and malware staging for Salt Typhoon.
Beijing Huanyu Tianqiong Information Technology (北京寰宇天穹)	Founded in 2021, coinciding with early Salt Typhoon activity. An example of a "hybrid firm" that offers both legitimate security services and products with potential C2 and covert access functions.
Sichuan Zhixin Ruijie Network Technology (四川智信 锐捷)	Established in 2018, later certified as a high-tech contractor for government and military clients. Geographic proximity to Beijing Huanyu Tianqiong suggests operational synergy.
i-SOON (安洵科技)	Cybersecurity contractor linked to both the MSS and Ministry of Public Security (MPS). Salt Typhoon used i-SOON managed infrastructure.

Campaign Case Studies

Salt Typhoon has carried out a series of highly targeted cyber espionage campaigns since at least 2019, primarily focused on telecommunications infrastructure, military networks, and intelligence collection across strategic geographies. These operations are consistent with MSS objectives such as signals intelligence (SIGNIT) acquisition, persistent access to critical infrastructure, and preparation of the battle-space for potential geopolitical escalation.

U.S. Telecom Metadata Breach: Early - Late 2024	
Victims	AT&T, Verizon, T-Mobile, Lumen, Windstream, and other major telecoms
Tactics	Exploitation of router/firewall CVEs, configuration hijacking, long-dwell persistence
Data Exfiltrated	• Subscriber metadata • Call detail records (CDRs) • VoIP infrastructure configurations • Lawful intercept logs
Motivation	To collect high-value SIGINT across U.S. telecom layers, including surveillance of communications and infrastructure maps. Likely tasking involved counterintelligence and strategic insight into U.S. domestic and foreign communications channels.

U.S. National Guard Network Intrusions: March - December 2024	
Victims	State-level National Guard military networks
Tactics	Exploitation of VPN gateways and edge devices; lateral movement
Data Exfiltrated	• Network diagrams • VPN configurations • Credentials • Incident response playbooks
Motivation	Preparation of the battle space and long-term espionage within defense-adjacent infrastructure. Access to National Guard systems may serve to identify mobilization thresholds, crisis response mechanisms, or gaps in Cybersecurity posture.

Domain Infrastructure & Tradecraft

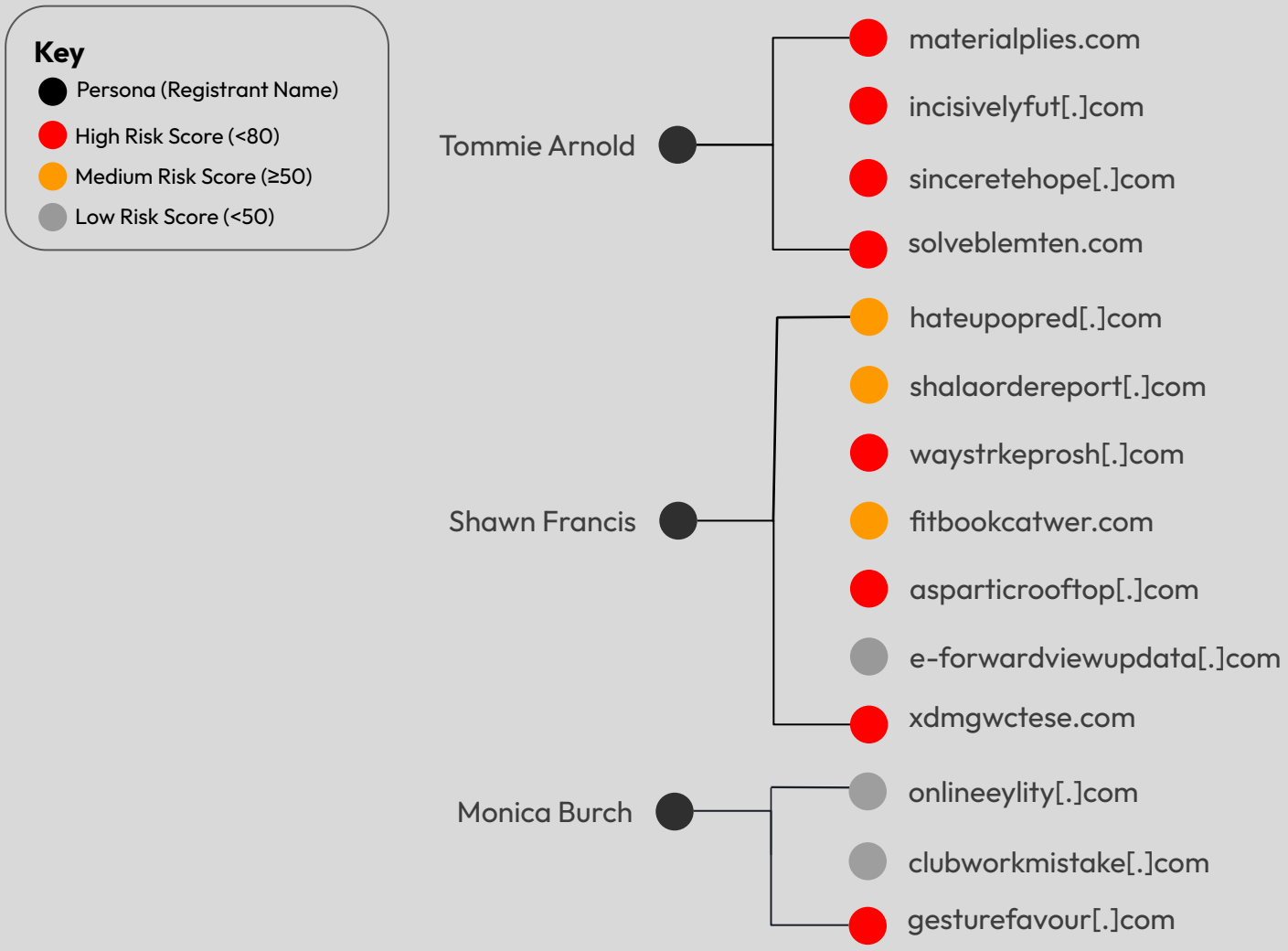
Salt Typhoon's use of large-scale, repeatable domain registration infrastructure enables the public attribution of at least 45 domains to its campaigns between 2020 and 2025. Common patterns in their domain infrastructure included:

- **Identity Reuse** - domains were consistently registered using ProtonMail email addresses and fabricated U.S. personas, often featuring plausibly American names and residential addresses.
- **Thematic Patterns** - Several domains in early Salt Typhoon campaigns mimicked legitimate technology or telecom services (e.g. cloudprodcenter[.]com, dateupdata[.]com), while more recent domains focused on action-oriented language (solveblemten[.]com) or appeared to be randomly-generated (xdmgwctese[.]com).
- **Name Server (NS) Clustering** - many identified domains resolved to the same or closely-related sets or authoritative names servers, often hosted within low-density Virtual Private Server (VPS) environments controlled by a limited number of providers.
- **SSL Certificate Patterns** - Saly Typhoon used commercial domain-validated certificates issued by authorities such as GoDaddy and Sectigo rather than free alternatives, likely to make their infrastructure appear more legitimate.

Salt Typhoon's reliance on bulk registration pipelines, shared DNS backends, and commercial DV certificates suggests a **contractor-enabled, semi-automated provisioning model**, likely stemming from entities such as i-SOON. This infrastructure pipeline prioritizes speed, scalability, and low-friction staging environments over long-term stealth. While it ultimately enabled attribution and exposure, it reveals a key insight into the industrialization of PRC cyber operations: the demand for deniability is often subordinated to operational efficiency and technical convenience.

DNS and the DomainTools Value

Salt Typhoon campaigns can be tracked over time using passive DNS clustering, SSL certificate pivots, registrar telemetry, and persona overlap, offering defenders viable opportunities to anticipate and disrupt the group's infrastructure before it matures into active operations. Below is an example of how pivoting on Salt Typhoon DNS registration personas using DomainTools IRIS Investigate revealed additional actor-affiliated domains, many of which have high predictive Risk Scores.



DomainTools