Picture credit: US Dept Defense

WINDS OF CHANGE

Itay Glick *reports on the lessons learnt from the Salt Typhoon breach and examines what can be done to protect defence networks against state-sponsored attacks*

Cyber adversaries are striking at the core of defence systems, revealing vulnerabilities that could jeopardise national security. Behind these attacks are nation-states wielding cyber warfare and espionage as strategic weapons to erode rivals and steal state secrets. The most recent example of this was the revelation that a Chinese-linked threat group, Salt Typhoon, had infiltrated the US National Guard's IT systems. By exploiting an unpatched firewall and stolen administrator credentials, the attackers maintained covert access for months, quietly collecting admin credentials, network diagrams and other sensitive information.

This was more than an isolated lapse. Salt Typhoon is among the most capable state-sponsored espionage groups active today, with a track record of targeting telecommunications providers and other strategic sectors. Their move into the defence arena signals an expansion in scope that should be highly concerning to defence operations worldwide.

Intelligence from one breach can enable access to others, creating a domino effect that crosses sectors and borders. With rising geopolitical tensions and nation states that have highly sophisticated techniques at their disposal, there is a growing need for strong cyber security capabilities to protect defence infrastructure. Unless the defence sector acts decisively, incidents like this will become more frequent and damaging.

Salt Typhoon is among the most capable state-sponsored espionage groups active today, with a track record of targeting telecommunications providers and other strategic sectors

Salt Typhoon is a state-sponsored espionage operation widely believed to be backed by China's Ministry of State Security. The group has years of experience targeting strategic sectors across the world, but is particularly well-known for espionage against US targets. Historically, they focused on telecommunications, compromising major carriers and, in some cases, accessing lawful intercept systems to monitor communications at scale. The National Guard breach is the clearest sign of a move into defence and homeland security networks. The inner workings of the group are opaque for now, so we can only make informed guesses about the direction they are taking. It may be the work of a different unit within Salt Typhoon, it may mark a decisive turning point in their strategy or it may have been more a case of opportunism.

Whatever the overall strategic movement, the attack demonstrates a shift that should have defence agencies on high alert. What really makes the group dangerous is patience and persistence. They don't deal in ostentatious threats, system outages and ransom demands like many criminal groups, but seek to remain undetected, gather intelligence and be well-positioned for future operations. Systems can be rebuilt, money can be replaced, but compromised intelligence can have consequences lasting decades. One of the greatest concerns here is the potential for escalation. Intelligence stolen in one operation – diagrams, credentials, contact lists – often becomes the key to breaching the next target. Over time, this chain of compromises can span agencies, sectors, and whole nations.

When attackers enter a defence network, the immediate concern is sensitive information: personally identifiable data on service members, operational plans, facility details and administrator credentials. Combined, this can form a detailed map of an organisation's operations and systems. This is damaging enough in isolation, but the risk doesn't end there. Many defence organisations share systems or authentication mechanisms with partners and federated credentials can allow access to multiple networks from a single login. If stolen, these could enable lateral movement into other military units or state-level cyber security partners. There's also the danger of reaching operational technology (OT) systems that control physical assets, including control systems at military installations and even weapons and materiel.

The breaches orchestrated by Salt Typhoon are alarming, but they are far from the only state-backed actors on the stage. Defending against these groups depends on understanding how they work. Unlike the more opportunistic independent criminal gangs that aim to maximise their financial profits, state backing means these attackers have the resources to operate with patience and precision. Their goal is to remain in networks for as long as possible without detection, extracting intelligence and preparing for future campaigns.

A core tool is the Windows kernel rootkit, which embeds deep in the operating system to evade detection. They also exploit "living off the land" techniques, using legitimate tools already in the environment to blend in. Spear phishing is often their entry point, targeting specific individuals to harvest credentials so that they can move laterally and escalate privileges. They also exploit vulnerabilities in edge devices such as firewalls, VPNs, and other internet-facing infrastructure. Many of these vulnerabilities go unpatched for extended periods, enabling attackers to reuse the same exploits repeatedly with success. Supply chain compromise is another route. Contractors or vendors with weaker defences can be leveraged as gateways into high-security networks. As seen with the SolarWinds breach, threat groups may also seek to infiltrate software supply chains to bypass traditional security controls.

Given their vast scale, defence networks are among the most complex environments to secure. They span multiple sites, connect thousands of endpoints and integrate with partner organisations at state, national and even international levels. That complexity can be an operational strength, but it creates a broad attack surface for adversaries to probe. One challenge is the sheer number of edge devices that need to be maintained. The more devices there are, the harder it becomes to ensure every single one is patched and properly configured. The age-old truth – that attackers only need to get it right once, while defenders can't afford a single miss – has never been more critical.

THE BEST SAFEGUARD IS TO ENFORCE POLICIES SO EVERY EXTERNAL DEVICE IS SCANNED BEFORE USE

Defence infrastructure is also likely to include many cyber physical assets, often governed by OT systems that are incompatible with standard security tools and processes. This can make management and visibility difficult. Another physical security issue is the heavy use of removable media such as USB drives. While these will typically be ruggedised models with built-in encryption, any use of removable media introduces another potential attack vector. Finally, there's the challenge of unified enforcement. In a large, distributed defence organisation, applying the same security policies across all units, partners and contractors is difficult. Gaps in implementation can be as dangerous as gaps in the policy itself – and groups like Salt Typhoon know how to find and exploit those inconsistencies.

The reality is that no single tool or control can protect a defence network from a determined state-sponsored attacker, especially in such a dense and complex environment. The only effective approach is defence-in-depth – a layered strategy where each control covers the gaps of the others. If one layer fails, another is there to stop or slow the adversary. There are three key capabilities that are particularly crucial for defence.

The first battle is often won or lost at the network's edge. Firewalls, VPNs and other internet-facing systems must be treated as high-value assets, not just passive gateways. That means regular patching, hardening configurations and applying multiple layers of defence so that if an exploit succeeds in one area, another control can still block the intrusion.

One of the most effective steps is to continuously confirm device compliance before granting network access. Every endpoint, whether it's a laptop, server or virtual machine, should be checked for patch status, antivirus, disk encryption and removable media policy. This must apply to all devices, including both corporate machines and those covered by BYOD. If a single