HOW ZKX HELIX COULD PREVENT THE SALT TYPHOON CYBER ATTACKS

Salt Typhoon is a Chinese state-linked advanced persistent threat (APT) group focusing on cyber-espionage. Its campaigns date back to at least 2022, where it targets government, intelligence, and industrial sectors worldwide, with an emphasis on counterintelligence and data theft. In late 2024, U.S. officials revealed that Salt Typhoon operatives had gained a foothold in the core networks of several major U.S. telecommunications carriers such as AT&T, Verizon, Spectrum, and more.

A QUICK OVERVIEW OF SALT TYPHOON'S TECHNICAL EXECUTION

Salt Typhoon gained initial access by exploiting known software vulnerabilities in telecom and security products. Researchers report that Salt Typhoon used: Ivanti Connect (CVE-2023-46805, CVE-2024-21887) to bypass authentication and gain remote code execution; a SQL-injection flaw in Fortinet's FortiClient EMS (CVE-2023-48788); a remote code execution bug in Sophos Firewall (CVE-2022-3236); and a server-side request forgery vulnerability in Microsoft Exchange Server (CVE-2021-26855). Notably, in late 2023 Salt Typhoon began exploiting critical Cisco IOS XE router vulnerabilities (CVE-2023-20198 and CVE-2023-20273) that allowed unauthorized creation of admin accounts and root-level command execution.

These router exploits enabled attackers to establish persistent access to core network devices (the routers that form the backbone of telco networks). Once inside, Salt Typhoon used living-off-the-land tactics to explore networks, harvest credentials, and avoid detection.

ZKX HELIX MITIGATES ATTACKS LIKE SALT TYPHOON

ZKX Helix is designed to strengthen exactly the kinds of access controls that Salt Typhoon breached. Helix enforces strict zero-trust access policies using a patented multi-factor authentication technology. Helix also ties its user to a specific device and never stores private keys on servers or devices.

In practice, this means that even if an attacker obtained a user's password (via phishing or exploitation of a vulnerable login page for example), they still could not log in without the user's physical device and cryptographic key fragments. For an APT like Salt Typhoon, which relied on stealing or reusing credentials to access network devices, Helix would greatly raise the bar: a compromised password alone would be useless without the full and complete Helix proof of identity.

Helix continuously re-authenticates sessions in the background. Once a user is logged in under Helix, the system silently verifies the user and device with each action. Any anomalous behavior (such as an unexpected remote session or parallel logins) can be configured to trigger a re-check, potentially alerting on or blocking intruders. This continual-validation approach would completely shut down Salt Typhoon's ability to move laterally or maintain an undetected presence.

HELIX'S CAPABILITIES MAP DIRECTLY TO THE WEAKNESSES EXPLOITED BY THE SALT TYPHOON ATTACKS

PREVENTING CREDENTIAL THEFT

Since Helix does not store static passwords or keys on a server or device, attackers cannot simply extract or reuse them. The system is immune to conventional password attacks. Even if Salt Typhoon hackers had planted software on an admin workstation, they could not intercept a reusable credential.

MULTI-FACTOR ASSURANCE

Helix's multi-key ZKP (zero-knowledge proof) scheme requires an adversary to defeat multiple cryptographic challenges, not just one password. This exponential increase in attack complexity makes Salt Typhoon style attacks impractical. Helix enforces true multi-factor security with strong cryptography, thwarting repeated attempts to guess or phish credentials.

DEVICED-BASED ACCESS CONTROLS

By design, Helix ensures that only a pre-configured device can respond to the MFA challenge. If Salt Typhoon tried to use stolen credentials from an unrecognized machine, Helix's policies would block it. This prevents adversaries from exploiting remote or shadow IT logins – a likely path given their use of Cisco web vulnerabilities.

VISIBILITY & RESPONSE

Helix's continual authentication provides ongoing telemetry on user behavior. In a Salt Typhoon scenario, Helix could generate alerts if a user's session suddenly originates from a different location or if certain high-risk actions are attempted without re-proving identity.

SECURE YOUR NETWORKS TODAY WITH HELIX

Attacks like Salt Typhoon are devastating, and yet we have reason to believe the worst is yet to come. Now is the time to lock down critical infrastructure networks to prevent the next disaster. For unparalleled security and peace of mind, secure your network today with ZKX Helix. If you would like to schedule a demo or learn more about how ZKX Helix can improve your cybersecurity posture, visit our website at **zkxsolutions.com** or give us a call at **(585) 301-4081.**