Salt Typhoon

A New Cyber Threat Businesses Can't Ignore

AN ALLEGEDLY Chinese state-sponsored hacker campaign dubbed "Salt Typhoon" has infiltrated major cell phone providers, including AT&T and Verizon, potentially exposing your company's communications to threat actors.

The attack has been described as the most significant telecommunications hack in U.S. history. While the breach is alarming for individuals, the implications for businesses are profound and demand immediate attention.

What is Salt Typhoon?

Salt Typhoon is a sophisticated cyber-espionage operation allegedly orchestrated by the Chinese government.

The campaign has targeted vulnerabilities in telecom providers' infrastructure to access text messages, monitor communications and extract sensitive metadata.

The ongoing breach has affected at least eight major U.S. telecom companies and poses a severe threat to national security and corporate privacy.

Potential dangers to businesses

Exposure of sensitive information –Hackers can intercept text messages, which may contain business-critical details, such as contracts, client discussions, or even login credentials.

Corporate espionage – Competitors or foreign entities gaining access to a company's internal strategies could result in lost market advantages or intellectual property theft, information that hackers can sell on the dark web to other criminal groups.

Regulatory and legal repercussions – Many industries are subject to strict data protection laws. A breach exposing customer or employee information could lead to fines and legal actions under regulations such as GDPR or CCPA.

Government warning

In response to Salt Typhoon, the U.S. government recommended using end-to-end encrypted communication platforms.

Unlike standard text messaging or phone calls, end-to-end encryption ensures that only the sender and recipient can read the messages.

Protecting your firm

Some steps businesses can take include:

- Shifting internal and external communications to end-to-end encrypted platforms such as Signal or WhatsApp, or enterprise solutions with encryption features.
- Avoiding using text-based, one-time passwords for authentication; instead, deploy hardware security keys or app-based authenticators.
- Updating systems regularly: Ensure all devices and software are updated to patch known vulnerabilities.
- Conducting regular training to educate employees about phishing, secure communications and device management.
- Limiting data access: Implement least-privilege access controls to restrict sensitive data to only those who need it.
- Regularly auditing your infrastructure for vulnerabilities.

Consider Cyber Insurance

Cyber insurance can help pay for the costs associated with a breach like Salt Typhoon. Talk to us about securing a robust cyber-insurance policy that covers:

- Forensic investigations
- System remediation and restoration
- Legal and regulatory compliance
- Business interruption losses. ❖