

Salt Typhoon: Churning Up a Storm of Consternation

 nattothoughts.substack.com/p/salt-typhoon-churning-up-a-storm

Share this post



Natto Thoughts

Salt Typhoon: Churning Up a Storm of Consternation

[Copy link](#)



[Facebook](#)



[Email](#)



[Notes](#)

[More](#)

Public knowledge of the Salt Typhoon intrusions has been driven by the media, while the government and private-sector cybersecurity companies appear to have agreed on keeping mum

The public first heard the name of Chinese threat actor “Salt Typhoon” on September 25, 2024, when the Wall Street Journal published an article titled “China-Linked Hackers Breach US Internet Providers in New ‘Salt Typhoon’ Cyber Attack.” Many of us were not expecting another typhoon to blow in so quickly. We were still trying to understand Flax Typhoon, which had been revealed barely a week before. Since then, reporting of the Salt Typhoon threat actor has flooded the media. We have been gradually learning the magnitude of the threat actor and its impact. However, as the Natto Team observes how Salt Typhoon stories have unfolded, we have more questions than answers, as we always do.



Typhoon Haiyan October 17, 2001. Source: [Defense Visual Information Distribution Service](#)

[Share](#)

Salt Typhoon Intrusion Reporting Driven by Media Reports

Unlike most cyber intrusion cases – which are often revealed and tracked by cybersecurity firms based on telemetry data – this time it was a media outlet, the Wall Street Journal (WSJ), that first broke the Salt Typhoon intrusions. The Natto Team would like to look into

how the Salt Typhoon intrusion reporting unfolded from the context of reporting source, adversary, victim, target and intent by reading through the Salt Typhoon articles published by the WSJ.

September 25, 2024: China-Linked Hackers Breach US Internet Providers in New ‘Salt Typhoon’ Cyberattack

- **Reporting source:** people familiar with the matter; the people
- **Adversary:** Salt Typhoon, possible APT40
- **Victims:** a handful of US internet-service providers
- **Target and Intent:** possible threat to core US infrastructure

In the first report that disclosed Salt Typhoon on September 25, the WSJ wrote that “people familiar with the matter” had revealed a “hacking campaign, called Salt Typhoon by investigators,” which “hasn’t previously been publicly disclosed” and which targeted “a handful of US internet-service providers.” Since the “Typhoon” naming taxonomy for China-based nation-state actors comes from Microsoft, it seems likely that Microsoft was one of the investigators. Citing “people familiar with the matter,” the WSJ article stated that “Microsoft is investigating the intrusion,” but Microsoft’s spokesman “declined to comment.”

The significance of Salt Typhoon intrusions, the WSJ explained, was the possible threat to “core US infrastructure”; the threat actors could establish “a foothold within the infrastructure of cable and broadband providers that would allow them to access data stored by telecommunications companies or launch a damaging cyberattack.” As to who is behind the Salt Typhoon attack, the WSJ article said US investigators had linked it to China. More particularly, Chris Krebs, the chief intelligence and public-policy officer of US cybersecurity company SentinelOne, hypothesized that Salt Typhoon could be APT40. [APT40](#), threat group affiliated with China’s Ministry of State Security (MSS) Hainan provincial bureau, specializes in intelligence collection. The US Department of Justice (DoJ) released an [APT40 indictment](#) in July 2021, identifying [four Chinese individuals](#) allegedly associated with the group. Three years later, in July 2024, the US and the so-called Five-Eye country partners issued a [joint advisory](#) that called out APT40 for targeting Australian networks.

Is Salt Typhoon indeed APT40? Not everyone thinks so. Within hours after the WSJ report, Microsoft updated its threat actor table to add Salt Typhoon. The Natto Team noticed from the indexed webpages of Internet Archive Wayback Machine that the webpage of Microsoft threat actors table did not have an entry for Salt Typhoon on [September 25th](#), but Salt Typhoon appeared into the table on [September 26th](#), the day after the WSJ first wrote about the threat group. Was this just a coincidence, or did Microsoft hold the information in reserve until the WSJ had made public the existence of Salt Typhoon?

Microsoft also already had its own opinion on whether Salt Typhoon was APT40. In its table, it listed other names that researchers have used for the activity set. It listed “GhostEmperor” and “FamousSparrow” but not APT40.

October 4, 2024: U.S. Wiretap Systems Targeted in China-Linked Hack

- **Reporting source:** people familiar with the matter; the people
- **Adversary:** Salt Typhoon, a.k.a FamousSparrow, GhostEmperor
- **Victims:** Verizon Communications, AT&T, Lumen Technologies and other companies, including “a small number of (internet) service providers outside the US.”
- **Target and Intent:** accessing the US wiretap systems

The second Salt Typhoon article from WSJ on October 4 disclosed that victim companies included Verizon Communications, AT&T and Lumen Technologies, “among other companies,” including “a small number of (internet) service providers outside the US.” The article gave some new information on the intrusions, saying that Salt Typhoon “penetrated the networks of a swath of U.S. broadband providers, potentially accessing information from systems the federal government uses for court-authorized network wiretapping requests.” The source of the information was still described as “people familiar with the matter.” These people told the WSJ reporters that Salt Typhoon is a “sophisticated” Chinese hacking group, and that the US government viewed the intrusions as potentially “catastrophic” and “historically significant and worrisome.”

The article stated that Microsoft and other cybersecurity companies are “investigating the new Salt Typhoon intrusion.” Citing a research note written by Microsoft in August 2024, the WSJ stated, “Salt Typhoon has been active since 2020 and is a nation-state hacking group based out of China that focuses on espionage and data theft, particularly capturing network traffic.” Microsoft said, “Most of Salt Typhoon’s targets are based in North America or Southeast Asia” and that “other cybersecurity companies call the group GhostEmperor and FamousSparrow.” The WSJ reporters didn’t indicate whether the August 2024 Microsoft research note is public or not. However, the Natto Team could not locate that research note in the publicly available information as of the date of this post.

October 25, 2024: Chinese Hackers Targeted Phones of Trump, Vance, and Harris Campaign

- **Reporting source:** people familiar with the matter; the people; a Democratic aide

- **Adversary:** Salt Typhoon
- **Victims:** presidential candidates, campaign staff and other politicians
- **Target and Intent:** presidential candidate communications; possible interference and disruption of the presidential election

The third Salt Typhoon article from the WSJ disclosed more details on prominent people whose communications the Salt Typhoon actors targeted, including “the phones of former President [now President-elect] Donald Trump, his running mate, JD Vance, and people affiliated with Vice President Kamala Harris's presidential campaign.”¹ Plus, “a number of prominent Democrats in Congress.” The article indicated a broader scope for the attack, noting that “at least several dozen different companies and people” were now known to be “targeted or compromised.” Although the source of the information was still “people familiar with the matter,” the WSJ reporters explicitly cited “a Democratic aide” as saying investigators had “notified a bipartisan group of politicians targeted by the hackers.” The WSJ reporters likely had communications either with Congressional staffers who had been briefed on the investigation or with investigators of Salt Typhoon themselves. The alarming notion was that since the Salt Typhoon intrusion was first exposed in September, Salt Typhoon actors have been fighting back; they “re-entered patched systems after being rejected” and unsuccessfully attempted to “access an account held by a Wall Street Journal journalist involved in coverage of the breaches.” The timing of the intrusions, right before the November 5th US election, made the case even more worrisome, suggesting the potential for “a far more significant effort to interfere or disrupt the election.” Lastly, “one person involved in the response” assessed that the brazenness of the Salt Typhoon operation “marked a ‘new frontier’ in how the Chinese government is leveraging cyber activity against the US.”

November 15, 2024 : T-Mobile Hacked in Massive Chinese Breach of Telecom Networks

-
- **Reporting source:** people familiar with the matter; the people
 - **Adversary:** Salt Typhoon
 - **Victim:** T-Mobile and some foreign telecommunications firms in countries that maintain close intelligence-sharing partnerships with the US
 - **Target and Intent:** cell phone calls and communications records

In the fourth Salt Typhoon related article, the WSJ reporters added US wireless network operator T-Mobile to the victim list of the Salt Typhoon intrusions. The source of the information is the same – “people familiar with the matter”- as in the previous three Salt

Typhoon articles. The additional information was that “investigators suspect the hackers relied on artificial intelligence or machine learning to further their espionage operations.”

Overall, the four Salt Typhoon-related reports from the Wall Street Journal, from breaking the news of the existence of the Salt Typhoon threat actor to exposing more and more victims in each article, spanned a month and half. Without providing any technical details, these articles stress the sophistication and significance of Salt Typhoon intrusions. Therefore, responses from the US government seem like a matter of course.

US Government Publicly Responds as the Media Investigation Unfolds

Public commentary by the US government on the Salt Typhoon intrusions followed closely after the media outlets’ reporting and ensured the public that the relevant government agencies were investigating the intrusions and aware of their significance. The October 5 WSJ article said, “The attack and its significance was discovered in recent weeks [i.e. likely not long before the publication of the September 25 WSJ article] and remains under active investigation by the U.S. government and private-sector security analysts.” The following are some of the major direct public government statements we have seen:

October 8, 2024: The White House set up a “unified coordination group” to ensure a “consistent interagency visibility into the response by the Federal Bureau of Investigation (FBI), the Office of the Director of National Intelligence, and the Department of Homeland Security’s Cybersecurity and Information Security Agency (CISA)” to address the Salt Typhoon intrusions. Similar coordination groups were formed previously to respond to Microsoft Exchange servers breach in 2021 and SolarWinds hack in 2020, according to [a report](#) from Washington Post. Likely referring to this group, the WSJ reported on October 25, “In recent weeks, the White House has convened highly confidential meetings to assess the damage of the compromises.”

October 11, 2024: The bipartisan Energy and Commerce (E&C) Committee of the US House of Representatives [sent letters](#) to AT&T, Verizon, and Lumen for answers and a closed-door briefing following the reporting of Salt Typhoon intrusions to companies’ networks.

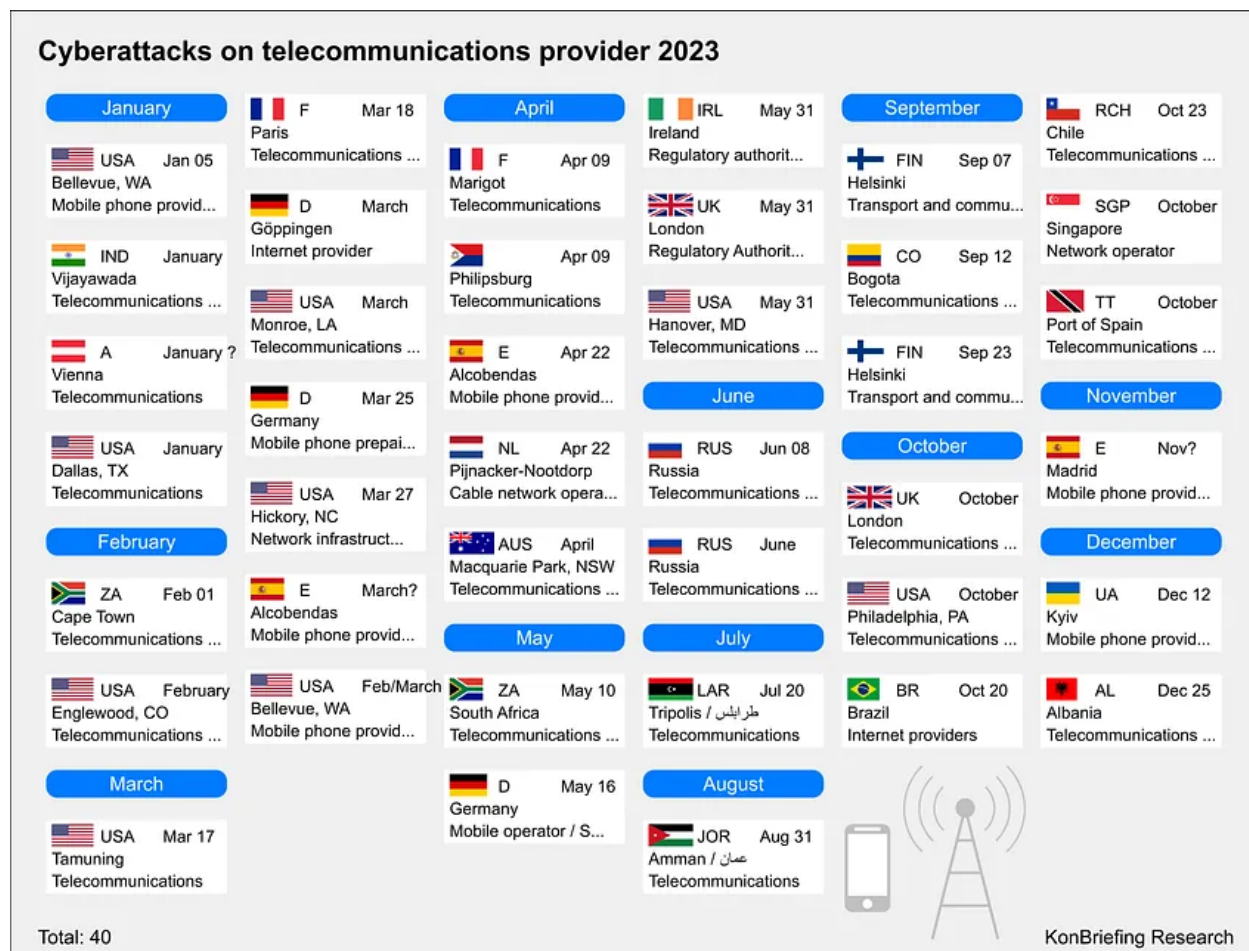
October 25, 2024: [Joint Statement](#) by FBI and CISA on PRC Activity Targeting Telecommunications. The joint statement does not mention the threat actor Salt Typhoon, but confirmed that the FBI “identified specific malicious activity targeting the sector” and had “immediately notified affected companies, rendered technical assistance, and rapidly shared information to assist other potential victims.” It added that “the investigation is ongoing” and that “Agencies across the U.S. Government are collaborating to aggressively mitigate this

threat and are coordinating with our industry partners to strengthen cyber defenses across the commercial communications sector.” The WSJ noted that the FBI’s statement was “the first formal acknowledgment by the U.S. government about the massive breach.”

October 28 2024: A Department of Homeland Security spokesperson acknowledged that the US Cyber Safety Review Board "will initiate a review of this incident at the appropriate time."

November 13, 2024: Joint Statement from FBI and CISA on the PRC Targeting of Commercial Telecommunications Infrastructure. The joint statement, again, does not mention the name Salt Typhoon, but its description of the campaign aligns with the WSJ reports of Salt Typhoon intrusions. It said “PRC-affiliated actors have compromised networks at multiple telecommunications companies to enable the theft of customer call records data, the compromise of private communications of a limited number of individuals who are primarily involved in government or political activity, and the copying of certain information that was subject to U.S. law enforcement requests pursuant to court orders.”

Targeting Telecoms is not New, but Particularly Sensitive in 2024



Cyberattacks on telecommunications provider 2023. Source: KonBriefing Research

Hackers have targeted the telecoms industry before. Sadly, it has happened quite frequently. 2023 alone saw some 40 attacks on telecommunications providers, as seen in the chart above. The Chinese state threat actors, too, have targeted core information and communications technology. Investigators looking at the Salt Typhoon activity initially suspected the threat actors may have obtained access to Cisco routers; earlier in 2024, reports had emerged of Chinese abuse of Cisco routers.

However, the revelations about Salt Typhoon come at a time of heightened concern about Chinese cyber threats among US Congress members of both parties and the US executive branch. Around the time of the US election in particular, the US government has warned about attempts to influence the American electorate. The targeting of law enforcement information could help the threat actors track US efforts to track Chinese espionage. In addition, the WSJ pointed out, the tapping of the US candidates “could reveal close associates” of the potential incoming presidential teams. In addition, the Natto Team notes that, given the numerous criminal investigations against one of the candidates, tapping into law enforcement information could give China blackmail material that could be used for leverage in case that candidate came into office. As for the targeting of the WSJ journalist, it was “highly unusual and likely an attempt at retaliation or intimidation,” the WSJ said, citing “former intelligence officials.” The targeting of US candidates may have been intended partly as a psychological operation in the leadup to the election. As one “person involved in the response” told the WSJ, “They’re taunting us....What is the diplomatic messaging behind them doing it, them showing us that they’re doing it, and continuing to do it after they are caught?”

Missing Industry Reports on Salt Typhoon Intrusions

As many cyber threat intelligence (CTI) analysts in the cybersecurity industry look for Salt Typhoon intrusion details, such as indicators of Compromise (IoC), after the Wall Street Journal broke the news, they discovered no industry reports on the described intrusions could be found.

Public statements on the investigation of the Salt Typhoon intrusion suggest a careful and coordinated release of information between the public and private sector, as this chronology of WSJ reporting and the public government statements has indicated. The US government may have asked cybersecurity companies that were involved in the investigation not to publicize the technical details of the intrusion. This approach likely results from the sensitivity of the Salt Typhoon intrusion case. In the leadup to the 2024 US presidential election, US officials tread a fine line, wanting to warn the public against the risks of foreign interference but also reassure them that the elections would be secure and reliable. Another reason for caution in public statements was likely the risks of exposing their awareness of threat actor modus operandi. It is also possible the US government is preparing indictments for the case

and wants to keep it quiet until then. Lastly, as the FBI and CISA statements said the investigation is ongoing, maybe the investigators want to establish solid confirmation for the information they make public.

However, as media outlets have been driving the Salt Typhoon intrusion reporting, “people familiar with the matter” have been feeding information to media outlets such as the Wall Street Journal in a continuing cadence for at least seven weeks so far. If the US government is authorizing these piecemeal revelations to the public, it makes us wonder whether this is a new approach to an attribution and deterrence strategy; the Natto Team raised such a question in connection with Volt Typhoon . Aside from possible authorized leaks, anyone from any of the investigation teams at the cybersecurity companies, or from the multiple US agencies who are investigating Salt Typhoon and participating in those top-secret White House meetings, as well as any of the targeted politicians or their staffers who were present at the briefings on the threat, could have revealed the information to the Wall Street Journal and other media outlets for a variety of reasons. Finally, if Chinese intelligence agencies themselves have burrowed into US government communications, they might themselves have access to information on the ongoing investigation and provide it to reporters as evidence of China’s own hacker prowess. (The Natto Team has cited such self-aggrandizement in the Russian case.) For their part, reporters assiduously cultivate “people familiar with the matter” who might be willing to share what they know, probably over a few drinks. If that’s the case, a lot of drinks have been consumed in the last two months.

Further Reading

For more information on the Salt Typhoon threat actor, the Natto Team highly recommends NotSimon on Mastodon who has posted a detailed Salt Typhoon threat actor profile including actor aliases, links to other groups, vulnerabilities exploited, and links of reporting references.

Thanks for reading Natto Thoughts! Subscribe for free to receive new posts and support the Natto Team’s work.

1

According to the Associated Press, it was the New York Times (NYT) that first disclosed the targeting of Trump and Vance. It is unclear whether the NYT article came before or after the WSJ’s, as the NYT article’s dateline does not give the specific time of publication.



11

Share this post



Natto Thoughts

Salt Typhoon: Churning Up a Storm of Consternation

Copy link



Facebook



Email



Notes

More



1



6

Share

No posts