Dataminr

NEWCOM Authorized Partner



Forecasting Typhoons: Volt Typhoon Next Steps

Volt Typhoon is a concerning cyber threat, but one with no actual known impacts to date. In this analysis, we will examine what a Volt Typhoon cyber-physical event would look like, and what defenders can do to mitigate it.

The threat actor Volt Typhoon first emerged in reporting from Microsoft in May 2023 as a group uniquely and concerningly interested in the U.S. critical infrastructure entities. Subsequent reporting identified the group as one of the most concerning threats to U.S. national security, where any number of assessed intrusions "is likely an underestimate." Volt Typhoon, associated with People's Republic of China (PRC) cyber operations, is assessed to be an entity preparing for disruptive attacks against critical infrastructure as a deterrent or response mechanism, likely associated with potential U.S. support for Taiwan in a PRC invasion scenario.

No Immediate Impact Should Still Prompt Concern

While reporting on Volt Typhoon has been alarming, actual impacts have been essentially non-existent to date. Aside from potential intrusions in Guam—home to many U.S. military facilities—and in the northeast U.S., Volt Typhoon has been relatively quiet in terms of publicly-disclosed activity. As a result, the group's operations have been overshadowed by other PRC-linked intrusion activity, such as telecommunication provider compromises associated with another entity referred to as Salt Typhoon.

Author
Joe Slowik, Director, Cybersecurity Alerting Strategy

OCTOBER 13, 2025

Yet the nature of Volt Typhoon activity should still prompt concern. Particularly, Volt Typhoon has focused almost exclusively on gaining access to critical infrastructure environments without obvious intelligence collection motives throughout its period of operation. Thus, the group appears to be something else: not pursuing immediate disruption while also eschewing traditional information gathering. Volt Typhoon instead represents a preparatory actor, gathering the access and information necessary to facilitate a disruptive event in U.S. critical infrastructure at some unknown point in the future.

With this in mind, threat intelligence analysts and critical infrastructure asset owners need to consider Volt Typhoon as a latent, potential threat as opposed to an immediate concern. While ransomware entities and similar manifest shortly after intrusion, and espionage actors siphon off data over long periods of time, Volt Typhoon appears dedicated to information gathering for a purpose. Discerning this purpose, and how it could be achieved, is critical for defensive action and countermeasures.

Volt Typhoon Could Become a Cross-Domain Threat

Based on a review of known Volt Typhoon operations and historical attempts to disrupt the cyber-physical systems delivering critical infrastructure functionality, we can arrive at possibilities for Volt Typhoon-induced disruption scenarios and their requirements. A review of past events largely identifies localized, immediate disruptive incidents targeting operational technology (OT) and similar systems in critical infrastructure—an attack possibility that is likely already available to Volt Typhoon—given the group's work to develop and maintain access to sensitive environments over time.

However, the group's association with PRC strategy during a conflict scenario indicates likely grander ambitions. We thus need to explore Volt Typhoon as an adversary focused on either the long-term disabling or destruction of critical infrastructure systems, or the widespread disruption of such systems to induce large-scale impacts. Both of these represent far more challenging scenarios to achieve as they have never been attained via cyber mechanisms in any known instance.

For those interested in learning more, please see the linked white paper for a more thorough analysis of Volt Typhoon and its potential impacts. In this whitepaper, you'll learn how to:

- Identify high-probability Volt Typhoon next steps to guide and focus your organization's defensive resource allocation.
- Adopt resilience strategies to help close significant defender awareness and understanding gaps.
- Spot weaknesses in current behavioral mapping frameworks.
- Understand why entities like Volt Typhoon pose unique problems for threat intelligence analysis and how existing analytical frameworks must evolve in the face of similar threat actors.

NEWCOM

To learn more, contact **NEWCOM**
781.826.7989 | sales@newcomglobal.com | NEWCOMGlobal.com



Determining Volt Typhoon Next Steps & Defensive Responses

Learn how to identify high-probability Volt Typhoon next steps to guide and focus defensive resource allocation.

GET WHITEPAPER

@ 2025 Dataminr. All rights reserved