

# Threat Intelligence Research: Volt Typhoon Compromises 30% of Cisco RV320/325 Devices in 37 Days

[securityscorecard.com/blog/threat-intelligence-research-volt-typhoon/](https://securityscorecard.com/blog/threat-intelligence-research-volt-typhoon/)



As part of our effort to make the world safer, SecurityScorecard has been tracking threat actor groups conducting cyberattacks on behalf of nation states.

The SecurityScorecard Threat Research, Intelligence, Knowledge, and Engagement (STRIKE) Team has been investigating covert infrastructure linked to Volt Typhoon (also known as Bronze Silhouette) following reports of new activity attributed to the group. Volt Typhoon is a state-sponsored threat actor group believed to act on behalf of the People's Republic of China that typically focuses on espionage and information gathering. The group conducts multiple types of cyberattacks, but its use of compromised small office and home office (SOHO) equipment such as routers and firewalls is a recurring theme.

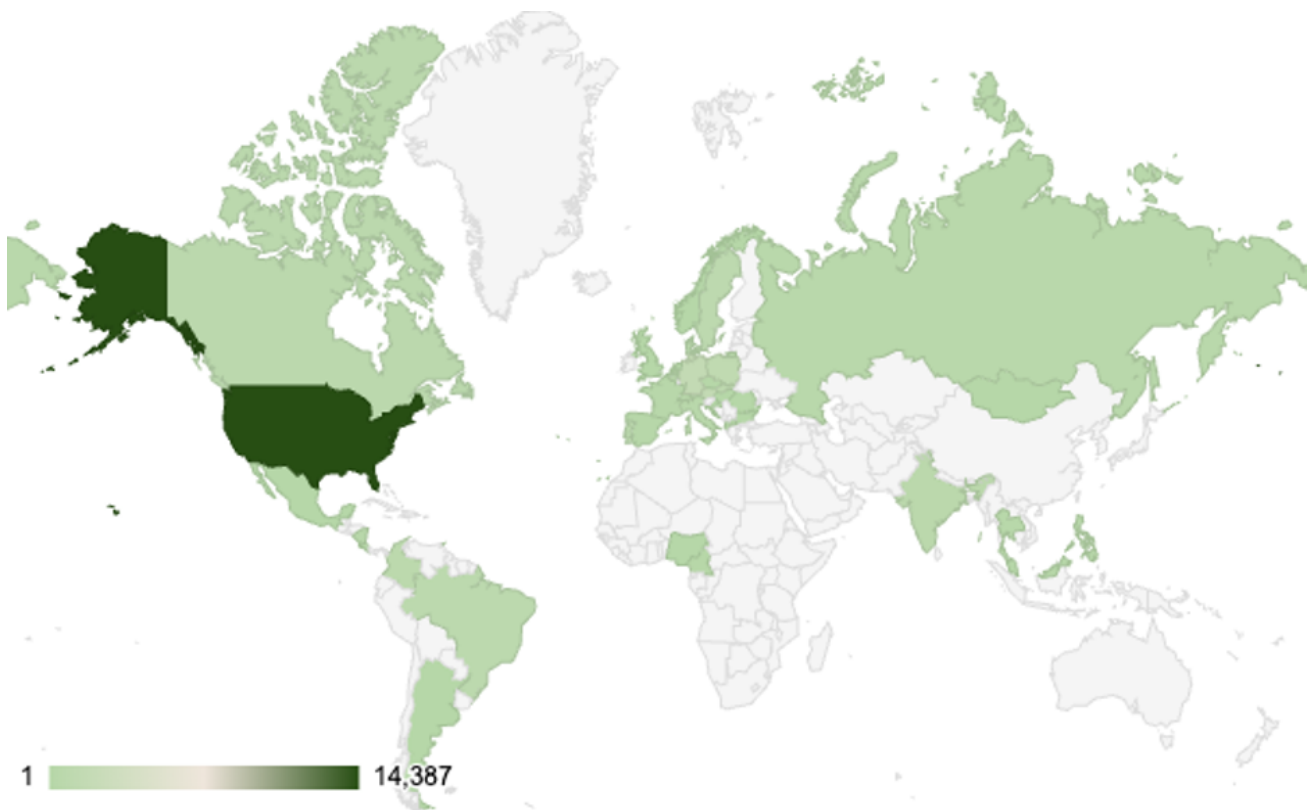
Lumen's Black Lotus Labs' recently-published report identified a group of compromised SOHO devices appearing to constitute a botnet that threat actors including but not limited to Volt Typhoon have used to covertly transfer data. The compromised devices the botnet

uses include Cisco and DrayTek routers, NETGEAR firewalls, and Axis IP cameras. STRIKE researchers used the indicators of compromise (IoCs) published alongside that report to conduct further research, which led to the newly-identified infrastructure.

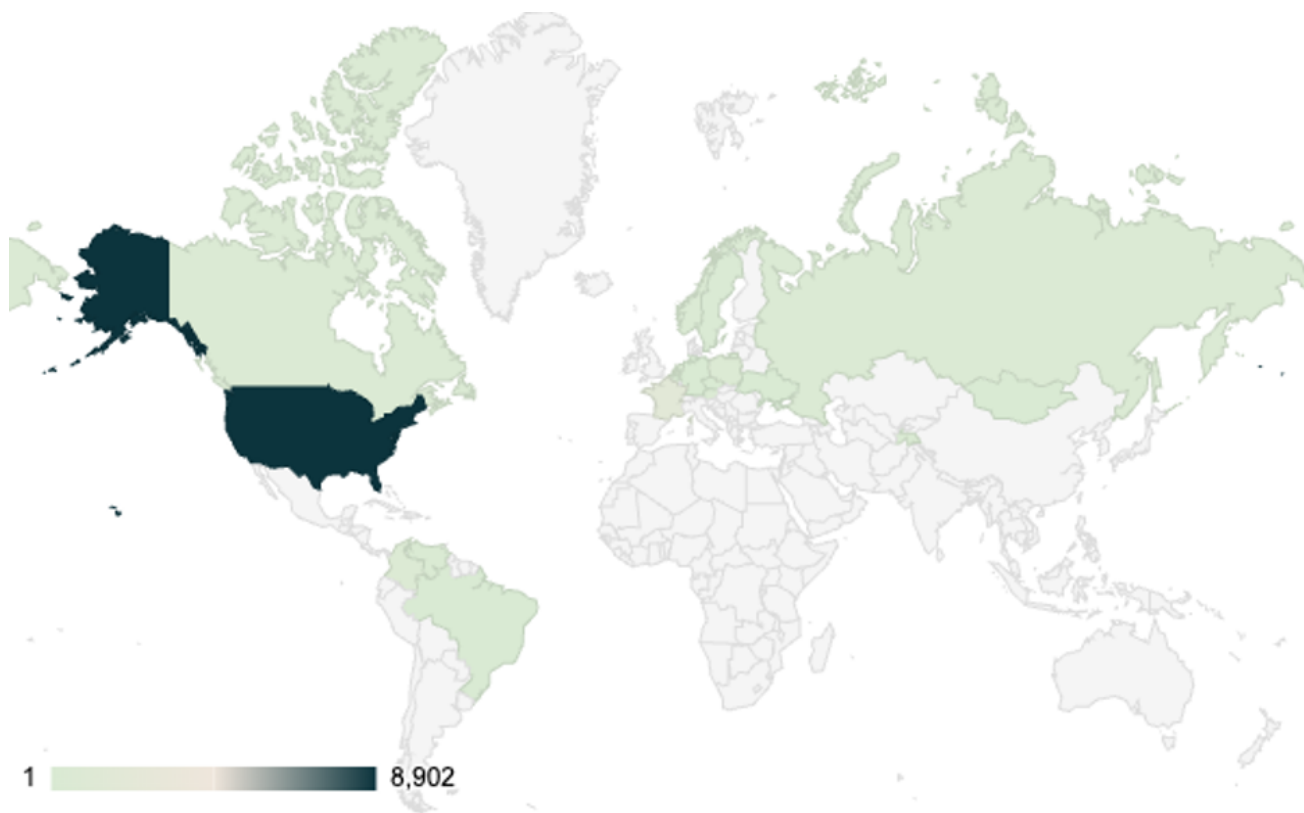
## Cisco devices are vulnerable

---

What emerged was a network of covert infrastructure operating in Europe, North America, and Asia Pacific that appears to be composed of compromised routers and other network edge devices. Our data indicates that **predominantly Cisco RV320/325 devices were impacted in the last 37 days**. Cisco RV's are network edge devices. It appears that, in keeping with previous reports, Volt Typhoon may aim to use these compromised devices to transfer stolen data or connect to target organizations' networks.



*Image 1: Geographical distribution of possibly infected Cisco RV320 devices by count of connections to C2 router nodes*



*Image 2: Geographical distribution of possibly infected Cisco RV325 devices by count of connections to C2 router nodes*

## Why this matters

---

These findings may suggest that Volt Typhoon’s activity is more extensive than previously reported; the extent of the campaign may reflect the easy accessibility of end-of-life devices, which means that Cisco has not released and will not release software updates to address vulnerabilities affecting them. Consequently, Volt Typhoon and other threat actors may be taking advantage of the ongoing use and easy accessibility of end-of-life SOHO devices.

According to SecurityScorecard’s scan data, varieties of the devices Volt Typhoon has targeted are distributed fairly broadly across the globe, but are especially heavily concentrated in the U.S. and Europe. This research is based on the infrastructure that SecurityScorecard’s global internet data and other passive signals collections.

## Recommendations

---

Organizations are encouraged to take the following steps to protect themselves from Volt Typhoon:

1. **Identify vulnerable devices:** Map your digital footprint with SecurityScorecard to identify Cisco RV320/325 devices on your network.

2. **Upgrade end-of-life devices:** Since the vendor no longer provides support or patches for these devices, it is recommended to upgrade to supported products immediately.
3. **Continuous monitoring:** SecurityScorecard validates your digital footprint on a continuous basis, so you can keep track of changes in your network that introduce new security issues.

## Final thoughts

---

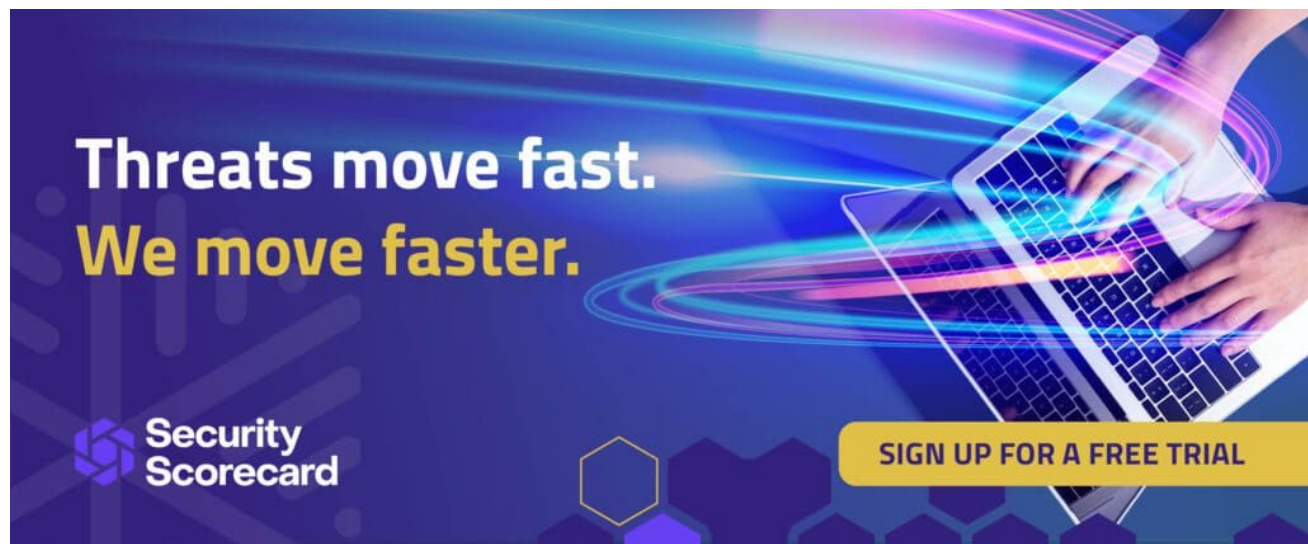
Black Lotus Labs' recent report assessed that Volt Typhoon is developing new infrastructure in preparation for a period of renewed activity. The communications between targeted models of Cisco routers and known Volt Typhoon IoCs, which STRIKE Team researchers observed, suggests that these preparations are ongoing and extensive, as almost a third of the Cisco devices appearing in SecurityScorecard's dataset communicated with these IoCs in a seven-day period.

To learn more about the STRIKE Team's findings, including previously unreported Volt Typhoon-linked IoCs researchers identified, [read the full report here](#).

**Explore SecurityScorecard's previous threat intelligence research on China-backed cyber activity:**

[SecurityScorecard Identifies Possible Flax Typhoon Infrastructure](#)

[STRIKE Team Investigation Identifies Possible Flax Typhoon Links to Higher Education](#)



The advertisement banner features a dark blue background with vibrant, glowing light trails in shades of blue, purple, and yellow. On the right side, a person's hands are shown typing on a laptop keyboard. The text "Threats move fast. We move faster." is prominently displayed in white and yellow. The SecurityScorecard logo is in the bottom left, and a yellow button with the text "SIGN UP FOR A FREE TRIAL" is in the bottom right.

**Threats move fast.  
We move faster.**

**Security Scorecard**

**SIGN UP FOR A FREE TRIAL**