SecurityScorecard Threat Research:

# Volt Typhoon Compromises 30% of Cisco RV320/325 Devices in 37 Days

**Chinese state-sponsored group continues to actively compromise Cisco devices possibly affected by vulnerabilities publicly disclosed in 2019**

SecurityScorecard

# Executive Summary

The SecurityScorecard Threat Research, Intelligence, Knowledge, and Engagement (STRIKE) Team has identified new infrastructure that appears to be linked to the threat actor group tracked as Volt Typhoon.

- Volt Typhoon is a state-sponsored group based in China that typically focuses on espionage and information gathering.

Approximately 30% of the Cisco RV320/325 devices observed by SecurityScorecard in a 37-day period may have been compromised by Volt Typhoon.

- The Cisco RV320/325 vulnerability was publicly disclosed in January 2019.
  - For RV320, there are 35 known vulnerabilities for the Dual Gigabit Wan VPN Router Firmware, all with a CVSS score of 9.
  - Two vulnerabilities from 2019 mentioned in the CISA KEV list (CVE-2019-1653, CVE-2019-1652) could have been exploited by Volt Typhoon.
- SecurityScorecard research illustrates state-sponsored threat actor groups' ongoing ability to identify vulnerable devices in anattempt to compromise targetnetworks.
- The STRIKE Team observed frequent connections between these devices and known Volt Typhoon infrastructure from 12/1/23 to 1/7/2024, suggesting a very active presence.
- **The devices are end-of-life, so Cisco has not released and will not release software updates to address vulnerabilities affecting them.**

SecurityScorecard researchers uncovered evidence of a previously unspecified webshell, fy.sh, on Cisco routers and other network edge devices targeted by the group.

- China Chopper is probably the best-known web shell used by China-linked APT groups; SecurityScorecard has now observed evidence of another.
- The STRIKE Team observed possible targeting of U.S., U.K., and Australian government assets by two such devices.
- Public reporting on Volt Typhoon has not previously noted its targeting of Australian or U.K. government assets in addition to U.S. ones.

Researchers identified two previously unidentified IP addresses belonging to a cluster of activity linked to Volt Typhoon, 45.63.60[.]39 and 45.32.174[.]131.

The file name and IP addresses the STRIKE Team discovered may offer further indications of Volt Typhoon's preparation of new infrastructure, which other recent reports have also observed.

# Recommendations

**See what a hacker sees to stop adversaries:**

## 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.

## Digital footprint mapping

A visualization of all the assets attributes to an organization, organized by IP addresses, IP ranges, domains, and geographic distribution. SecurityScorecard also identifies the number of dynamic IP addresses at any point in time.

Because SecurityScorecard scans the entire IPv4 internet weekly, it continuously compiles and updates asset data to keep the security assessment current. Using data collected by SecurityScorecard proprietary scanners, web crawlers, honeypots, and other in-house analyses, we proactively flag issue findings.

Every IP in your digital footprint is part of a domain. Since domains often group IPs by business units, or initiatives, the domain view in your digital footprint enables you to review IPs in logical subsets.

# Background

Following the publication of reports of new activity attributed to the threat actor group tracked as Volt Typhoon and Bronze Silhouette, which the cybersecurity community believes to conduct espionage on behalf of the People's Republic of China (PRC), the STRIKE Team began to track and identify covert infrastructure linked to the campaign. The reports already published about the group note varying levels of complexity, but its use of compromised small office and home office (SOHO) equipment such as routers and firewalls to conduct attacks abroad is a recurring feature. This research is based on the infrastructure that SecurityScorecard's global internet data and other passive signals collections identified.

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 discussed below.

FIGURE 1:
**Global distribution of targeted models of NETGEAR ProSAFE devices.**

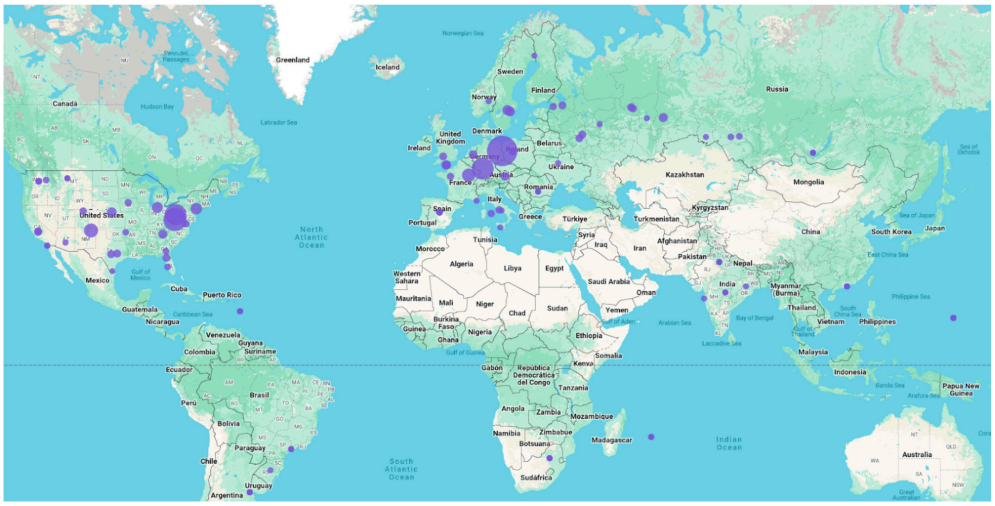
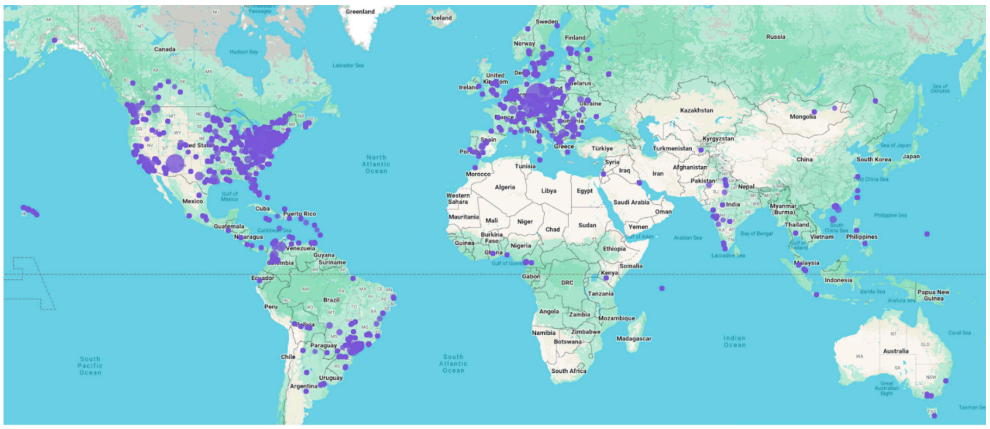



FIGURE 2:
**Global distribution of targeted Cisco router models (RV320 and RV325) visible on the Internet in a seven-day period.**



Further research suggests that the Volt Typhoon-linked botnet's compromise of Cisco RV320 and RV325 routers may be more extensive than previously reported. Researchers additionally used a strategic partner's network flow (NetFlow) data to develop additional insights into activity involving this population of possible target devices and found that approximately 30% of them (325 of 1,116 devices) communicated with two IP addresses previously named as proxy routers used for command and control (C2) communications, 174.138.56[.]21 and 159.203.113[.]25, in a thirty-day period. Communication with known botnet C2 infrastructure may suggest participation in that same botnet's activities.

FIGURE 3:

**Connections between IP addresses known to be Volt Typhoon IoCs and other IP addresses by ISO country code.**

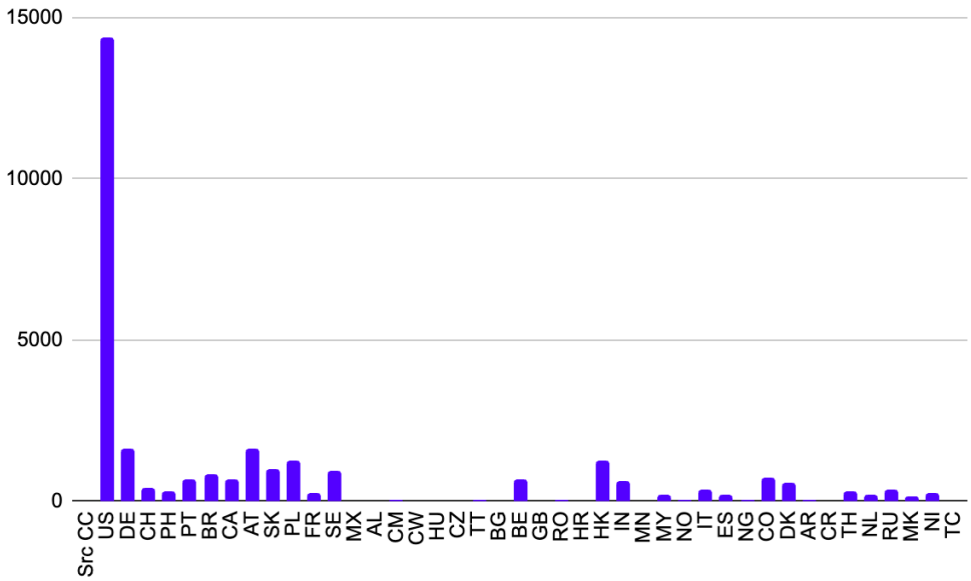



FIGURE 4:

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

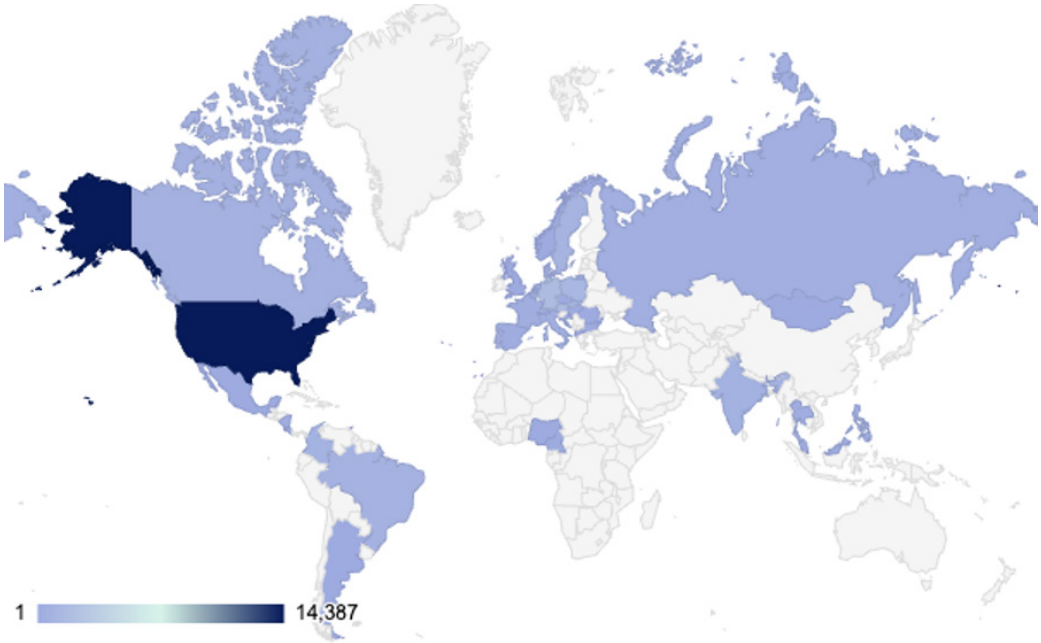


FIGURE 5:

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

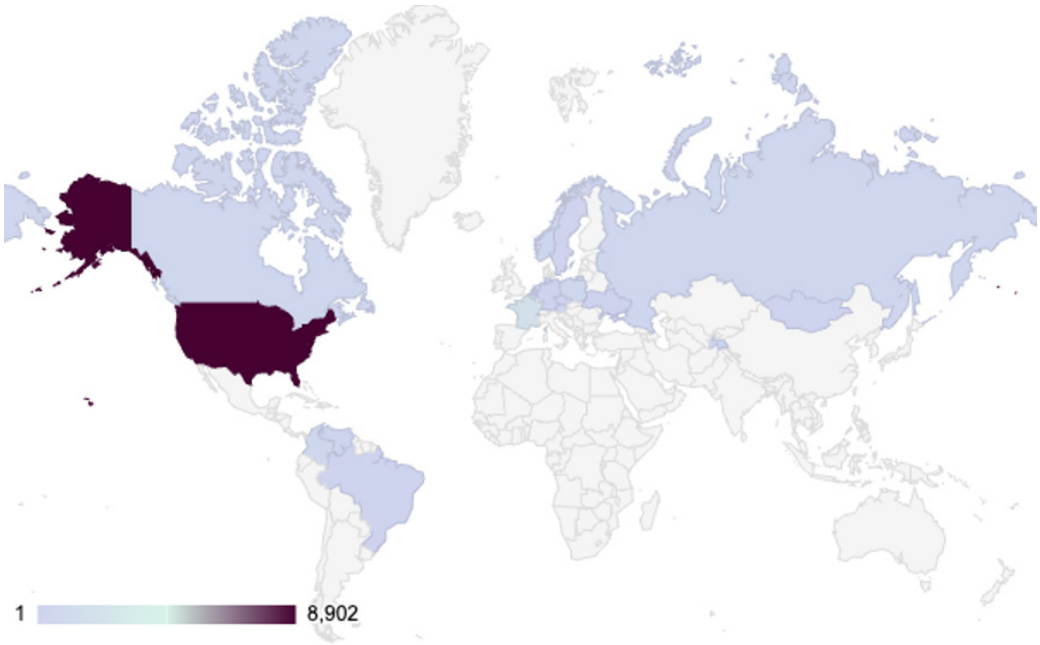
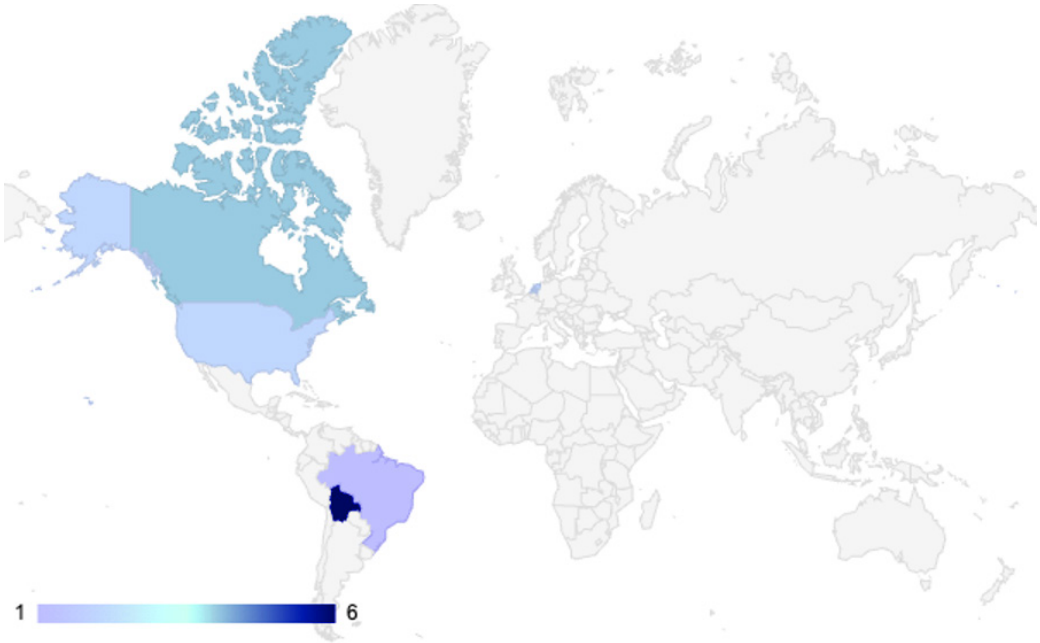



FIGURE 6:

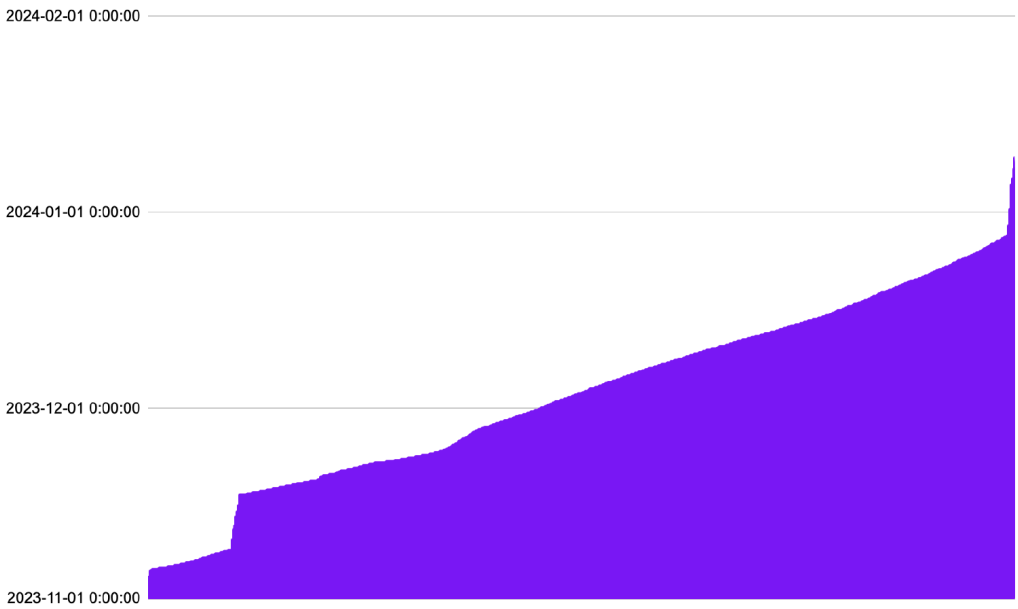
**Geographical distribution of IP addresses observed communicating with known Volt Typhoon C2 infrastructure between January 1 and 8, 2024.**




The continued activity by one of the aforementioned C2 proxies, 159.203.113[.]25, into early January, appears to reflect a shift in the botnet's C2 infrastructure, which the dates provided by Black Lotus Labs may also reflect. Prior to mid-November, another DigitalOcean IP address named as an IoC linked to the same botnet, 159.203.72[.]166, appears to have been more active, but the increased activity from 159.203.113[.]25, another DigitalOcean IP address, from November 17 onward, suggests that the latter took the former's place. A similar shift appears to have occurred in the botnet's Vultr infrastructure as well, with activity involving 144.202.49[.]189 increasing and activity involving 140.82.20[.]246 diminishing in mid-November.

FIGURE 7:

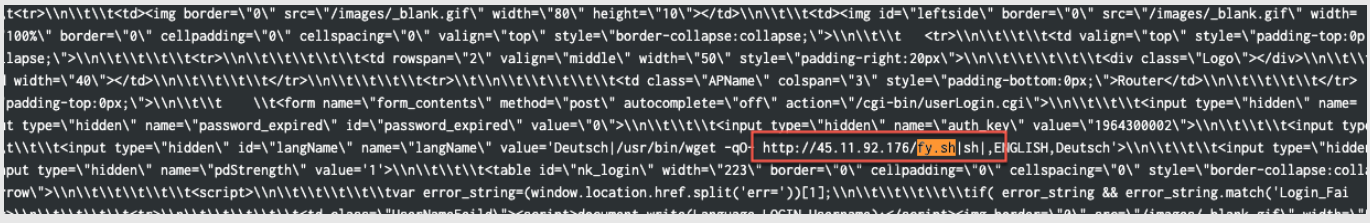
**Traffic activity involving sample population of C2 proxy servers increased from October 2023 to January 7, 2024.**




Additionally, SecurityScorecard's scan data has revealed a group of Cisco routers with metadata containing an IP address the Black Lotus Labs report cited above named as a payload server, which suggests compromise by Volt Typhoon or another threat actor using the same botnet. This metadata refers to a **wget** command featuring 45.11.92[.]176, a known Volt Typhoon IoC, and references a file, **fy.sh**, that the devices in question retrieve and execute from 45.11.92[.]176. However, as of January 8, 2024, the payload server is offline.

FIGURE 8:

**Content from our data collections indicates that a group of Cisco routers' HTML appears to contain a hidden wget command to a Volt Typhoon-linked payload server.**



Metadata for the following IP addresses indicates that they contact the payload server at the IP address listed among other new IoCs associated with Volt Typhoon. Given that they do not themselves appear in the previously published list, they may represent previously unidentified IoCs related to Volt Typhoon activity:

- 46.10.197[.]206
- 176.102.35[.]175
- 93.62.0[.]77
- 194.50.159[.]3
- 80.64.80[.]169
- 24.212.225[.]54
- 208.97.106[.]10
- 70.60.30[.]222
- 184.67.141[.]110

The following maps display the geographical distribution of the devices with metadata containing fy.sh:

FIGURE 9:
**Distribution of European IP addresses with metadata featuring Volt Typhoon payload server IP address.**

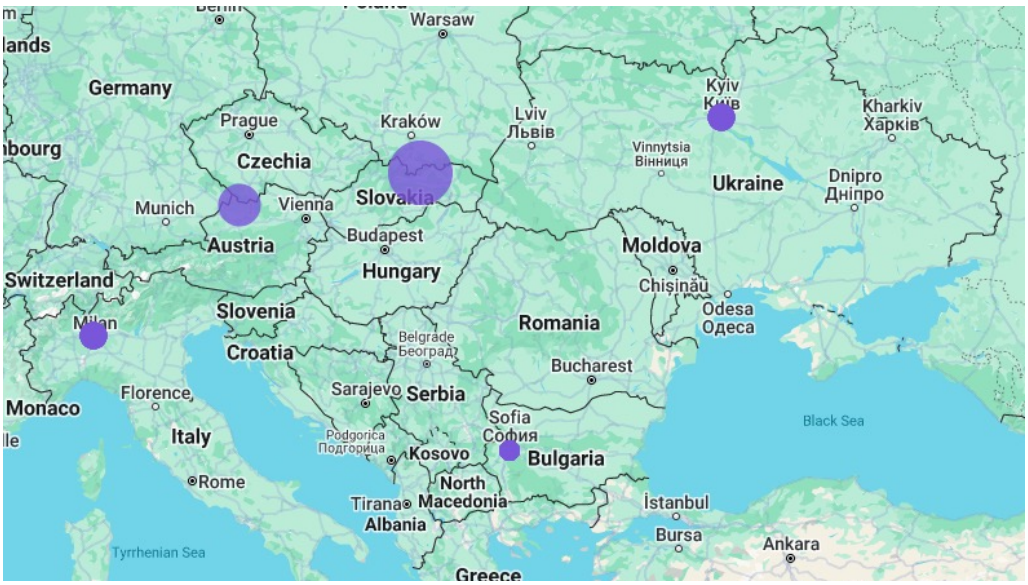
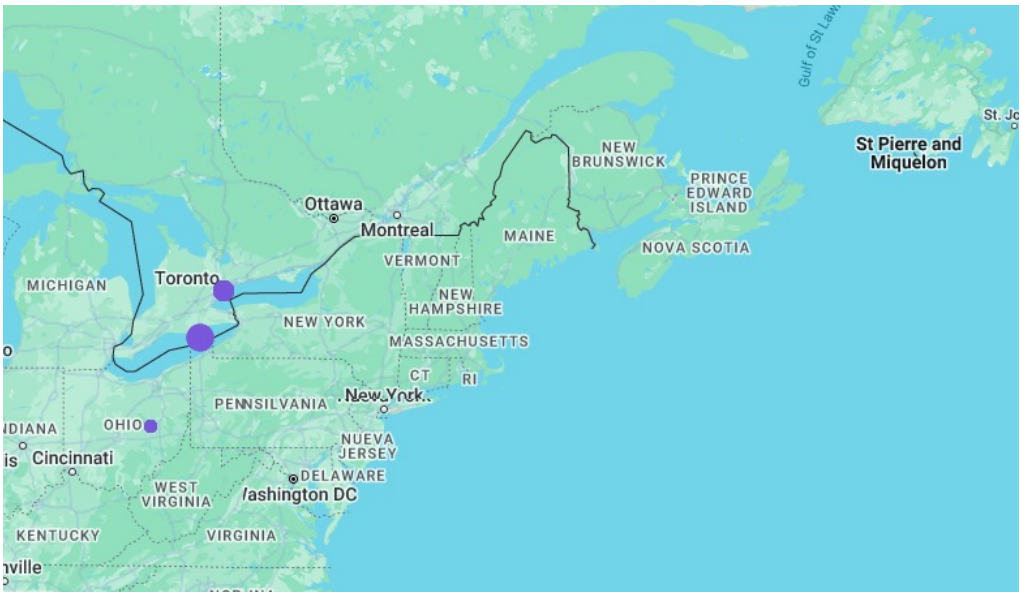



FIGURE 10:
**Distribution of North American IP addresses with metadata featuring Volt Typhoon payload server IP address.**



# Findings: Cisco Webshell

Researchers additionally noted that the infrastructure observed communicating with 45.11.92[.]176 features a webshell implant. This implant performs a wget request to the payload server to download a file named fy.sh.

Of the IoCs Lumen circulated, the two files identified by the SHA256 hashes 7043ffd9ce3fe48c9fb948ae958a2e9966d29afe380d6b61d5efb826b70334f5 (the file named Kv-all.sh) and 36c63d0c2a78497ccf555e84f0233a514943faeff38281d99d00baf5df23f184 are, as indicated by the .sh extension they have in common with fy.sh, shell files. A sample of the particular file named fy.sh that 45.11.92[.]176 served does not yet appear to be publicly available, but two files with that name have appeared in VirusTotal. These two files, however, appear to be unrelated to the recent campaign; vendors detect them as macOS adware and both were last seen in Summer 2021, while the activity discussed in Lumen's report began in February 2022. The fy.sh served by 45.11.92[.]176 may therefore more likely correspond to a different file also named fy.sh, one which may be similar to either of the .sh files Lumen named as IoCs, both given that an IP address named as an IoC in the same report as those files has served fy.sh and that it is, in general, fairly common for PRC-linked APT groups to use webshells (the China Chopper webshell is perhaps the most famous example but by no means the only one).

# Findings: Additional NetFlow Analysis

Researchers conducted further analysis of NetFlow data to develop additional insights into activity that may be related to the campaign. The analysis below focuses on traffic involving the payload server discussed above, devices observed communicating with it, and other newly-identified compromised devices; communications between these compromised devices and other network devices may also offer insights into the campaign's victimology.

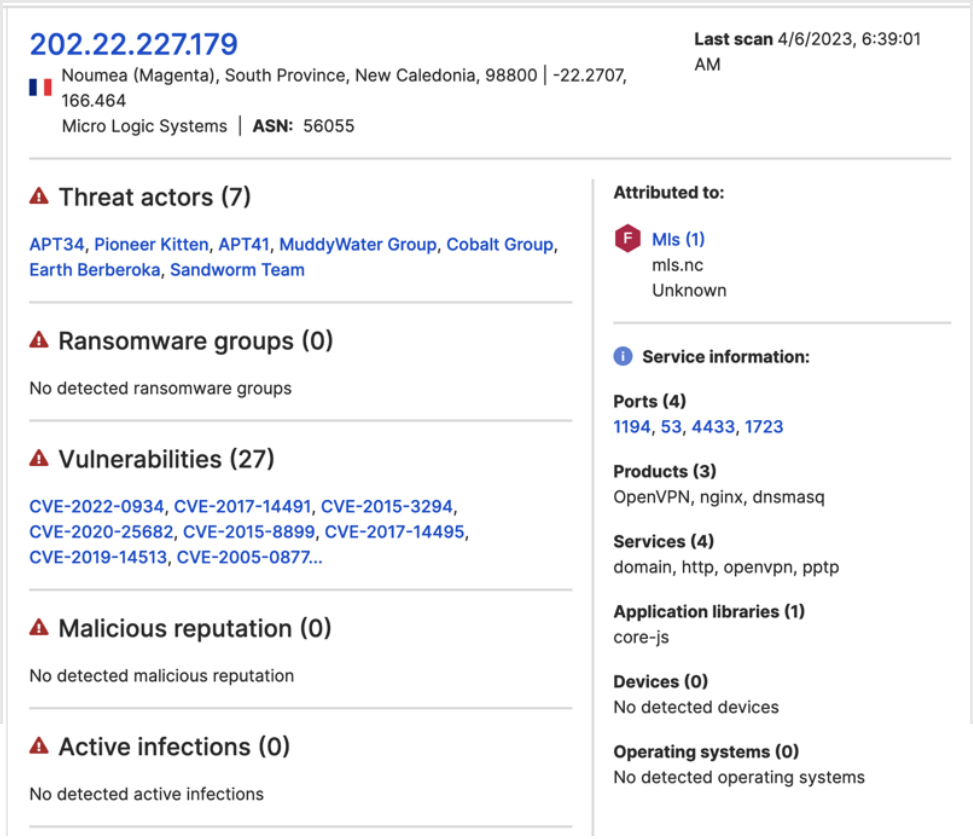
Researchers identified new IP addresses that belong to the Volt Typhoon-linked C2 infrastructure Lumen termed the "JDY Cluster" on the basis of the recurrence of the same common name, "jdyfj," in the SSL certificates observed at the IP addresses in this cluster. The two new IP addresses belonging to the cluster are 45.63.60[.]39 and 45.32.174[.]131.

To identify these IP addresses, researchers first used SecurityScorecard's scan data to collect a group of IP addresses where products Volt Typhoon is known to compromise are in use and then leveraged a strategic partner's network flow (NetFlow) data to collect traffic samples for those IP addresses. 202.22.227[.]179 is one such IP address; SecurityScorecard's data indicates that a Cisco RV325 device is in use there and, according to the traffic samples for established Volt Typhoon-linked IoCs, it has communicated regularly IP addresses previously linked to Volt Typhoon.

SecurityScorecard's Attack Surface Intelligence module indicates that 202.22.227[.]179 is located in Noumea, New Caledonia and belongs to Micro Logic Systems (mls[.]nc), a New Caledonian internet service provider (ISP).

FIGURE 11:

**SecurityScorecard locates 202.22.227[.]179 in New Caledonia and attributes it to a New Caledonian ISP.**




Its location and attribution to an ISP may further suggest 202.22.227[.]179's use as a transit point for Volt Typhoon-related traffic; New Caledonia is an island chain in the Southwest Pacific, so it may be a common occurrence for traffic between the Asia-Pacific (APAC) region and the Americas to pass through New Caledonian communications infrastructure en route to a final destination either elsewhere in APAC or in the Americas. The available analysis of Volt Typhoon has highlighted its targeting of communications between APAC and the Americas – its intrusions into the networks of telecommunications providers and other critical infrastructure in Guam attracted particular attention in previous reporting–so its exploitation of telecommunications infrastructure on another Pacific island may be in keeping with this previous behavior.

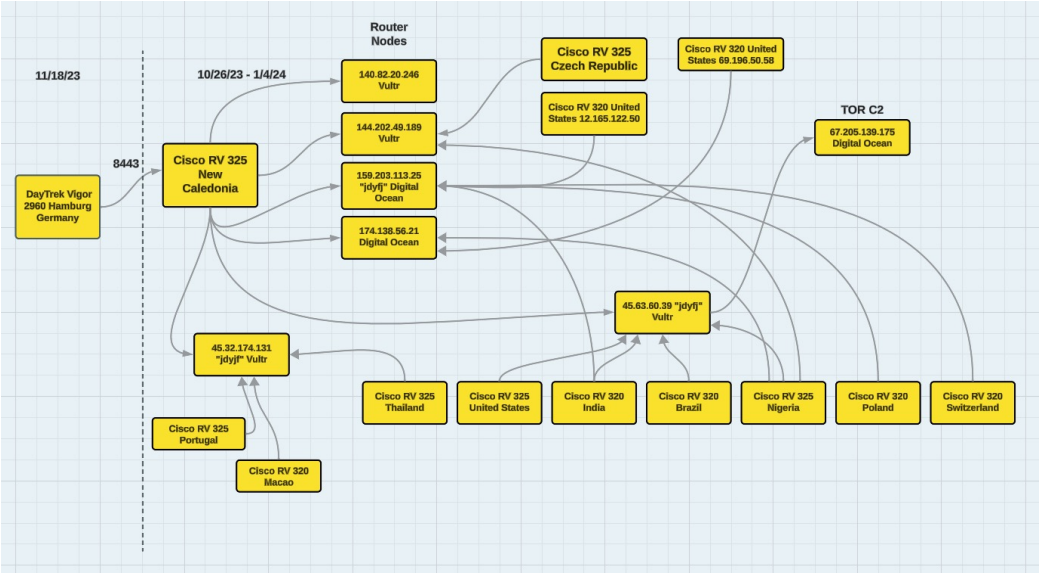
However, a separate traffic sample focused specifically on 202.22.227[.]179 indicated frequent communication between 202.22.227[.]179 and both 45.63.60[.]39 and 45.32.174[.]131. 45.63.60[.]39 communicated with 202.22.227[.]179 3,097 times between December 28 and 31 and 45.32.174[.]131 communicated with it 3,358 times over the same period. Both of these IP addresses belong to the same hosting provider as others previously identified as Volt Typhoon IoCs and both feature SSL certificates issued to jdyfj, the same subject that appeared in the SSL certificates at IP addresses Lumen previously named as part of the JDY cluster. Both 45.63.60[.]39 and 45.32.174[.]131 are therefore likely previously unidentified parts of that cluster.

Additional activity involving 45.63.60[.]39 may further reflect behavior associated with Volt Typhoon. It and 67.205.139[.]175, a Tor exit node, communicated twenty-five times between December 28 and December 30. Previous reports have noted that Volt Typhoon has used Tor for its C2 communications, so this traffic may reflect C2 communications between different Volt Typhoon-controlled resources (one routing traffic through Tor and the other hosted at 45.63.60[.]39).

STRIKE Team researchers additionally observed four instances of communication between 31.19.153[.]48, an IP address where SecurityScorecard's data indicates another product Volt Typhoon has been observed exploiting, a DrayTek Vigor 2960 router, is in use and 202.22.227[.]179 on November 18. Given that Volt Typhoon is known to compromise the specific DrayTek and Cisco devices in use at 31.19.153[.]48 and 202.22.227[.]179, that they were communicating with one another, and that 202.22.227[.]179 also communicated regularly with other Volt Typhoon-linked IP addresses, communications between these two IP addresses may also reflect Volt Typhoon activity, although it is not clear at present if the IP addresses represent infrastructure particular to Volt Typhoon.

Researchers also collected and analyzed samples of traffic involving known Volt Typhoon infrastructure, given that the behavior originating IP addresses named as Volt Typhoon-related IoCs could offer additional insights into the group's activity. This sample led researchers to other IP addresses that may represent additional, previously unidentified Volt Typhoon infrastructure. 144.202.49[.]189, an IP address Lumen identified as a proxy router for Volt Typhoon's C2 communications, and 82.117.159[.]158, an IP address where SecurityScorecard's data indicates a Cisco router is in use, communicated 68,164 times between December 1 and December 7. Given the frequency of its communication with a known Volt Typhoon asset, and the observation of a product Volt Typhoon has been observed exploiting in use at it, 82.117.159[.]158 may represent an additional Volt Typhoon-linked IoC.

FIGURE 12:
**Communications between some targeted Cisco models and Volt Typhoon infrastructure.**



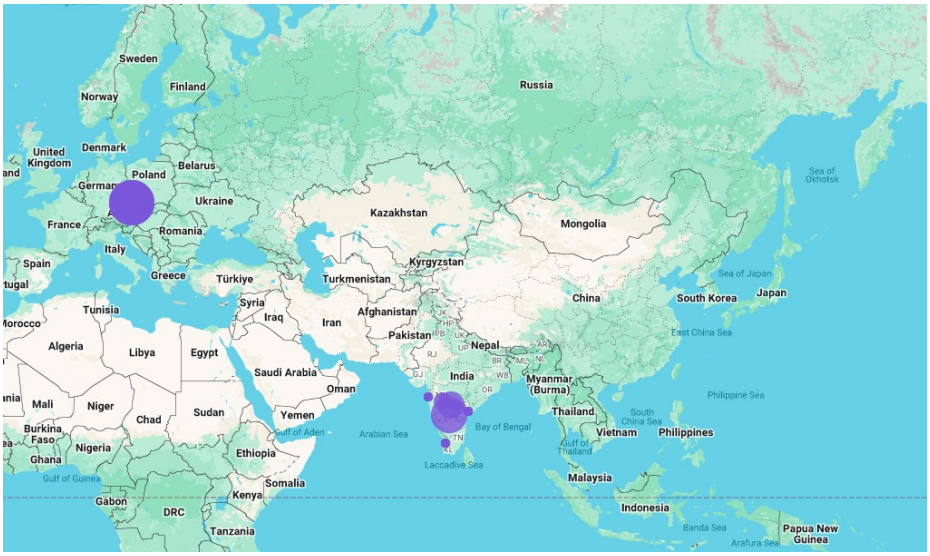
As with the findings discussed previously, these communications may suggest that the botnet linked to Volt Typhoon is more extensive than previously reported, as communications between known IoCs linked to it and devices it is known to exploit could suggest compromise (and subsequent malicious reuse) of those devices.

The payload server's traffic sample, meanwhile, featured communication between it and fourteen IP addresses that appear to host routers and other devices like those listed in Lumen's recent report on the botnet Volt Typhoon has used from November 9th to December 18th. The use of these devices and the IP addresses' communication with the payload server, may, taken together, suggest that the following are the fourteen IP addresses also represent previously unpublished IoCs linked to the botnet identified by Lumen:

- 192.149.47[.]110
- 212.11.106[.]139
- 89.203.140[.]246
- 94.125.218[.]19
- 183.82.110[.]178
- 117.239.157[.]74
- 210.212.224[.]124
- 49.204.75[.]92
- 61.2.141[.]161
- 49.204.75[.]90
- 114.143.222[.]242
- 117.211.166[.]22
- 49.204.65[.]90
- 49.204.73[.]250

While STRIKE Team researchers have not observed published vulnerabilities affecting the products at the IP addresses above in SecurityScorecard's datasets, they did note that many of these products may be outdated. Twelve of the fourteen IP addresses above feature SSL certificates for NETGEAR products issued in either 2007 or 2013. If these certificates' issue dates are also an indication of their products' age, it may suggest that these products have reached end-of-life. This may, in turn, reflect the previously published observation that Volt Typhoon and other threat actors using the newly-identified botnet appeared to be taking advantage of the widespread use and easy accessibility of end-of-life SOHO devices.

FIGURE 13:
**Geographical distribution of devices communicating with the payload server.**



In order to identify additional, possibly-compromised infrastructure involved in the same activity, researchers next filtered the traffic sample by product type and focused on IP addresses where the strategic partner furnishing the sample observed DrayTek routers, given that in one cluster of activity discussed in Lumen's report, DrayTek devices comprised distinct layers of infrastructure through which the threat actors tunneled traffic from other compromised devices. This yielded the following IP addresses:

- 112.120.122[.]88
- 219.76.184[.]200
- 14.224.157[.]129
- 31.120.199[.]123
- 110.175.91[.]70
- 125.227.15[.]174
- 37.224.98[.]249
- 218.161.3[.]216
- 82.69.127[.]130

Finally, researchers collected separate traffic samples for each of the IP addresses where SecurityScorecard's partner observed a DrayTek device and then compared these samples to identify IP addresses that recurred across them, as their recurrence may suggest that the IP addresses correspond to other layers in the same cluster of activity represented by the DrayTek routers should this group of DrayTek devices constitute such a layer. The following are the IP addresses that appeared in multiple DrayTek devices' traffic samples:

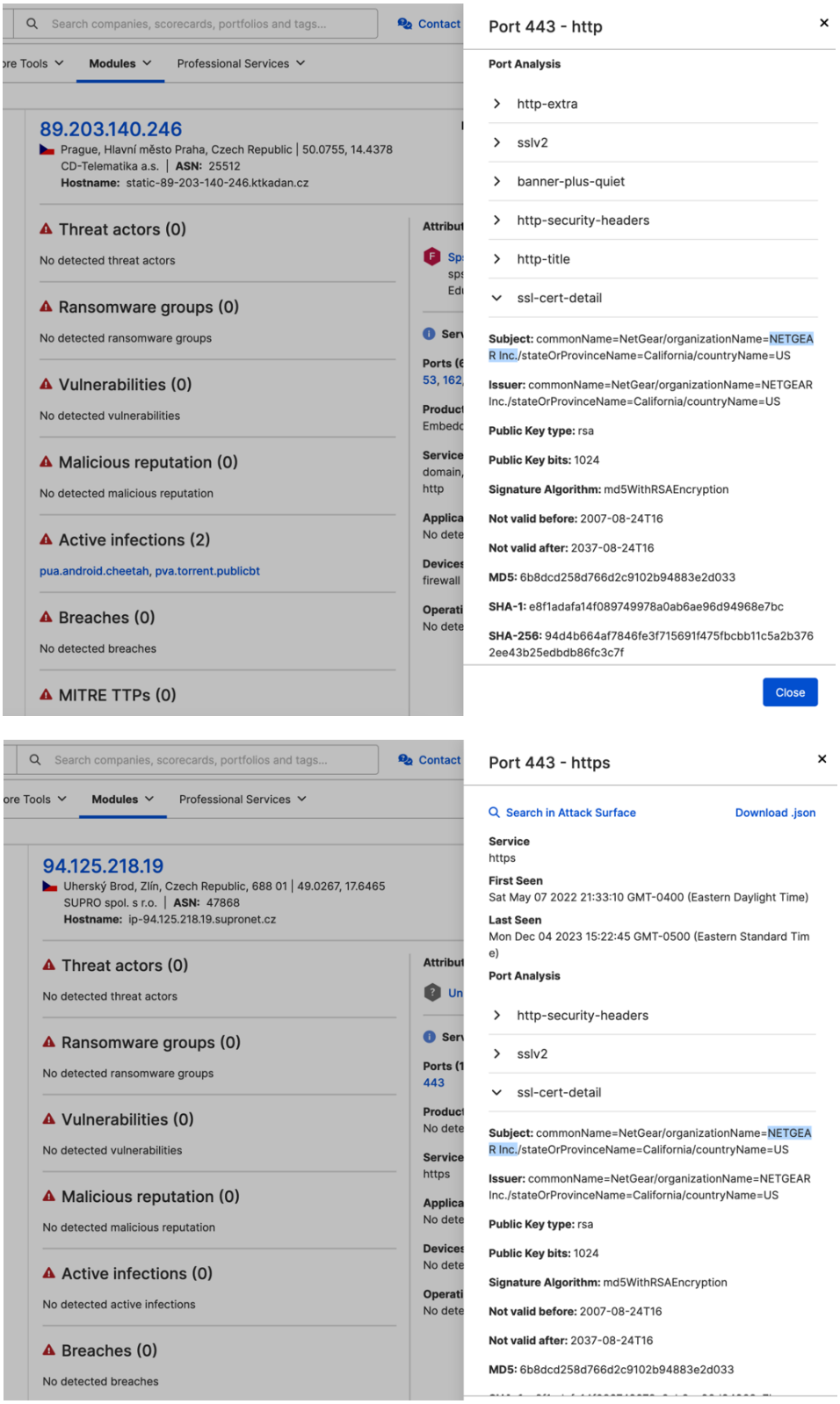
- 212.11.108[.]127
- 212.11.107[.]193
- 212.11.124[.]98
- 129.132.120[.]59
- 212.11.106[.]139
- 147.87.210[.]109

## Potential Victimology

STRIKE Team researchers additionally observed communication between two Czech IP addresses that appeared in the payload server's traffic sample and IP addresses hosting U.S. government domains. SecurityScorecard's Attack Surface Intelligence tool indicates that both Czech IP addresses host NETGEAR ProSAFE devices.

FIGURE 14-15:

**Possibly end-of-life NETGEAR firewalls appear to be in use at both of the Czech IP addresses in question.**



The recently published reports on new Volt Typhoon activity have noted that it exploited NETGEAR firewalls with some regularity. Given that SecurityScorecard's data reflects the use of NETGEAR products at the IP addresses observed and that the same IP addresses both contacted a payload server previously linked to Volt Typhoon and other IP addresses hosting US government domains, these IP addresses may not only be previously unidentified components of Volt Typhoon's network of compromised devices, but may also reflect Volt Typhoon's targeting of a U.S. and allied government entities.

An initial traffic sample for these two possibly compromised IP addresses reflected communication between them and seven IP addresses to which two different .gov domains, login[.]gov and login.gov.external-domains-production.cloud[.]gov, and one Australian government domain, login.service.nsw[.]gov[.]au, resolved at the time of observation. A second, more recent traffic sample for these same two Czech IP addresses revealed repeated communication between them and twenty-seven IP addresses hosting a total of sixty-nine U.S. U.K., Australian, and Indian government sites. Given that these domains appear to correspond to government assets and that Volt Typhoon has previously targeted U.S. government entities, this traffic may reflect additional targeting of the U.S. and allied governments by Volt Typhoon or a similar group, although it does not indicate a successful compromise. It also bears noting that the IP addresses with which the possible Volt Typhoon assets communicated belong to cloud services and content distribution networks, so the government domains are likely just a few of many that resolved to them within the observation period. That being the case, the possibility that the observed traffic involved other, non-government domains at the same IP addresses and therefore does not reflect targeting of government assets also merits consideration.

While public reporting on Volt Typhoon has not previously noted its targeting of Australian or U.K. government assets in addition to U.S. ones, such activity would be in keeping with PRC nation-state cyber activity more generally, as these countries' roles in the Western alliance system (including their Five Eyes and AUKUS membership) have contributed to their frequent targeting by China-linked APT groups.

# Conclusion

Black Lotus Labs' recent report assessed that the Volt Typhoon activity observed likely reflected the group's development of 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.

Similarly, the newly-identified IP addresses specified above that may represent new, Volt Typhoon-linked IoCs may offer further indication that the group's preparation of new infrastructure has continued. Given their communication with known Volt Typhoon IoCs and the appearance of other Volt Typhoon-linked artifacts in SecurityScorecard's scan data about them, the STRIKE Team assesses with moderate confidence that the following IP addresses represent previously unidentified Volt Typhoon IoCs:

- 45.63.60[.]39
- 45.32.174[.]131
- 82.117.159[.]158
- 46.10.197[.]206
- 176.102.35[.]175
- 93.62.0[.]77
- 194.50.159[.]3
- 80.64.80[.]169
- 24.212.225[.]54
- 208.97.106[.]10
- 70.60.30[.]222
- 184.67.141[.]110
- 89.203.140[.]246
- 94.125.218[.]19
- 183.82.110[.]178
- 117.239.157[.]74
- 210.212.224[.]124
- 49.204.75[.]92
- 61.2.141[.]161
- 49.204.75[.]90
- 114.143.222[.]242
- 117.211.166[.]22
- 49.204.65[.]90
- 49.204.73[.]250

While certain contextual factors (the use of devices Volt Typhoon has previously targeted and communication with other such devices, including some that in turn communicated with IP addresses linked to Volt Typhoon) may suggest that the other IP addresses discussed elsewhere in this document are involved in Volt Typhoon-linked activity, the available evidence does not appear, at present, to indicate that they represent Volt Typhoon-specific infrastructure.

**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

## To learn more and create your free account, visit SecurityScorecard.com

### ABOUT SECURITYSCORECARD

Funded by world-class investors, including Evolution Equity Partners, Silver Lake Partners, Sequoia Capital, GV, Riverwood Capital, and others, SecurityScorecard is the global leader in cybersecurity ratings, response, and resilience, with more than 12 million companies continuously rated.

Founded in 2013 by security and risk experts Dr. Aleksandr Yampolskiy and Sam Kassoumeh, SecurityScorecard's patented rating technology is used by over 25,000 organizations for enterprise risk management, third-party risk management, board reporting, due diligence, cyber insurance underwriting, and regulatory oversight.

SecurityScorecard makes the world safer by transforming how companies understand, improve, and communicate cybersecurity risk to their boards, employees, and vendors. SecurityScorecard achieved the Federal Risk and Authorization Management Program (FedRAMP) Ready designation, highlighting the company's robust security standards to protect customer information, and is listed as a free cyber tool and service by the U.S. Cybersecurity & Infrastructure Security Agency (CISA). Every organization has the universal right to its trusted and transparent Instant SecurityScorecard rating. For more information, visit securityscorecard.com or connect with us on LinkedIn.

SecurityScorecard

**SecurityScorecard.com**
info@securityscorecard.io

United States: (800) 682-1707
International: +1(646) 809-2166