CANADIAN WEB HOSTING
#723 - 602 West Hastings Street Vancouver, BC, Canada V6B 1P2 Canada
Toll Free : 1-888-821-7888 / www.canadianwebhosting.com

Incident Report - Coordinated DDoS Campaign (May 18 - 22, 2026)

Summary

Beginning on May 18, 2026, we experienced a large-scale coordinated DDoS campaign targeting our network infrastructure. Multiple waves of malicious traffic were directed at our network over several days, affecting connectivity across our Internet-facing services and multiple upstream network paths.

While our server environments remained operational throughout the event, external network connectivity was intermittently impacted by the scale, duration, and evolving nature of the campaign.

Our engineering and network teams worked continuously with upstream carriers, network providers, and mitigation partners to identify attack patterns, implement filtering, restore routing, and stabilize connectivity.

Cause of Service Interruption

The service interruption was caused by a large-scale coordinated DDoS campaign directed at our network infrastructure. Multiple waves of malicious traffic were observed over several days, disrupting connectivity across our network and the upstream paths used to deliver traffic to our environments.

The incident was not the result of a server, storage, virtualization, or customer application failure. The affected server environments remained online; however, external connectivity was disrupted due to the volume, duration, and evolving nature of the malicious traffic.

Timeline of Events (All times are Pacific Time)

Monday, May 18, 2026

6:27 PM: Our Support and NOC teams began receiving multiple service-down alerts and immediately initiated an investigation to determine the scope of the issue.

6:42 PM: The incident was escalated to infrastructure management.

7:00 PM: Engineering resources were engaged to investigate a network issue affecting connectivity across multiple data centre environments.

7:15 PM: Our network team began working with upstream providers to identify traffic patterns and available mitigation options.

8:00 PM: Traffic analysis from multiple monitoring systems confirmed that the disruption was related to a coordinated DDoS campaign.

8:10 PM: Additional monitoring adjustments were implemented to improve visibility into attack traffic and capture additional diagnostic information.

8:30 PM: Connectivity impacts increased as upstream network providers began implementing protective measures to safeguard their infrastructure.

8:30 PM - 9:00 PM: Engineering teams continued gathering traffic data, reviewing mitigation options, and coordinating with network providers.

9:00 PM - 9:30 PM: Attack activity temporarily subsided and service availability improved.

9:30 PM: A new wave of attack traffic was detected and began affecting an additional network location.

10:55 PM: Attack activity ceased. Additional monitoring and alerting were deployed to improve visibility and prepare for further activity.

11:00 PM: Enhanced monitoring was implemented at additional locations affected by the campaign.

Tuesday, May 19, 2026

7:30 AM: A new wave of DDoS traffic was detected.

7:37 AM: Follow-up analysis was performed on traffic associated with the previous attack wave.

8:13 AM: Additional filtering information was provided to upstream providers to assist with mitigation efforts.

8:20 AM: Further analysis of attack characteristics was completed to support filtering and traffic engineering activities.

8:35 AM: Discussions were initiated with additional DDoS mitigation providers regarding enhanced protection options.

9:00 AM: A cross-functional incident response team met to coordinate response efforts, recovery planning, and mitigation strategy.

9:20 AM: Follow-up coordination occurred with network providers to review restoration options and mitigation activities.

9:40 AM: Additional third-party mitigation providers were engaged to evaluate longer-term protection options.

10:00 AM: Work began to deploy additional network infrastructure required to support restoration and mitigation activities.

10:48 AM: Configuration and deployment of additional network equipment commenced.

11:23 AM: Additional filtering rules were implemented to reduce the impact of malicious traffic.

11:52 AM: Discussions continued with DDoS mitigation providers regarding available protection services.

12:54 PM: Evaluation of enhanced mitigation services continued.

3:00 PM: Active attack traffic was no longer being observed against network segments that had been restored.

3:19 PM: Additional network connectivity was provisioned to assist with restoration efforts.

4:21 PM: Restoration of routing and network announcements continued across affected environments.

5:00 PM: Newly provisioned network connectivity was brought into service and testing began.

6:52 PM: Additional IP announcements and routing updates were performed.

8:23 PM: One of the affected Vancouver network paths was restored.

8:25 PM: Attention shifted toward restoring remaining network paths and services.

8:35 PM: Additional mitigation planning was completed in preparation for potential future attack waves.

8:45 PM: Packet loss was reported from certain Vancouver locations and further investigation commenced.

9:00 PM: Troubleshooting continued to address remaining routing inconsistencies and BGP session issues.

10:30 PM: Additional routing updates were coordinated with network providers.

Wednesday, May 20, 2026

Routing issues affecting the Toronto environment were corrected through routing policy adjustments.

Additional network paths were restored, and work continued to address packet loss affecting some Vancouver locations.

No active DDoS traffic was observed during this period.

Thursday, May 21, 2026

12:30 PM: Additional BGP routing sessions affecting Vancouver connectivity were restored.

Temporary traffic controls that had been applied during the mitigation process were reviewed and removed where appropriate.

5:51 PM: A renewed wave of DDoS activity was detected against the network.

Mitigation efforts resumed and continued throughout the evening as attack activity persisted.

Friday, May 22, 2026

2:15 AM: Attack activity subsided and network connectivity stabilized.

10:21 AM: Following discussions and planning efforts that had been underway earlier in the week, we accelerated our engagement with Cloudflare and began implementation activities to move traffic through their network for additional filtering and DDoS mitigation.

Throughout the remainder of the incident, engineering teams continued monitoring attack activity, refining mitigation measures, and implementing longer-term protections designed to improve resilience against future events.

Resolution

The immediate issue was addressed through a combination of:

- Identifying and analyzing malicious traffic patterns
- Applying upstream filtering where possible
- Adjusting monitoring thresholds to improve attack visibility
- Restoring affected BGP routing sessions and IP announcements
- Making routing policy adjustments to restore affected network paths
- Working with upstream carriers and external network resources
- Engaging with Cloudflare and other mitigation providers to enhance DDoS protection capabilities
- Beginning implementation of Cloudflare-based filtering and DDoS mitigation services
- Preparing additional mitigation options to reduce the risk of repeat impact

As attack activity subsided and routing was restored, affected services gradually became reachable again.

Corrective and Preventative Actions

Following the incident, we began implementing additional measures to improve resiliency against similar events, including:

- Expanding DDoS detection and monitoring visibility
- Reviewing upstream filtering and escalation procedures
- Improving coordination procedures with network providers
- Reviewing routing failover and recovery processes
- Making routing policy adjustments to improve network stability
- Deploying additional Cloudflare-based filtering and DDoS mitigation capabilities
- Improving internal incident communications and customer update procedures

We have also opened a case with the RCMP and the appropriate cybercrime division regarding this campaign. The matter is currently being investigated, and the incident has been formally documented for further review.

Closing Statement

We understand the impact this outage had on customers and sincerely apologize for the disruption. Our team treated this as a high-priority incident and worked continuously with network providers and mitigation partners to restore stable connectivity.

We are continuing to review the event and improve our network resiliency, mitigation capabilities, and response procedures to reduce the likelihood and impact of similar incidents in the future.