Countermeasures against DDoS attacks (Advisory)
Feb 4, 2025

From December last year to the beginning of this year, several critical infrastructure companies in Japan, such as airlines, financial institutions, and telecommunications companies, have been hit by DDoS attacks using various types of methods, including UDP flood and HTTP flood. And some of them have used IoT botnets. In this situation, it is undeniable that large-scale cyberattacks will occur in the future.

NISC recommends that companies and organizations take appropriate measures against DDoS attacks, using this advisory as a reference to mitigate risks, in addition to their current measures.

In the meantime, NISC urges all Internet users to properly configure their IoT devices, such as routers and IP cameras, to prevent them being infected with malware and becoming part of an IoT botnet that participates in cyberattacks.

【Security measures to mitigate risks】

Some countermeasures against DDoS attacks are time-consuming and costly, and it is not possible to prevent all attacks. However, in order to prepare for severe DDoS attacks such as the recent ones, please consider the following points and take action in each of your offices: **review the settings of the devices and systems you have installed, check for vulnerabilities, and update software.**

1. Measures to mitigate damage from DDoS attacks

① Block communications from unexpected IP addresses such as those assigned overseas.

Since botnets are often used for DDoS attacks, you can mitigate the impact of DDoS attacks by blocking communications from countries or domains with many infected bots. This is particularly effective for systems that are only expected to receive domestic access within Japan. Of course, you must consider the impact on legitimate communications. Please also consider using features that block a large number of requests that exceed the threshold from a single IP address.

② Deploy appropriate equipment and services to mitigate the impact of DDoS attacks

Consider installing and properly configuring appropriate equipment and services, such as WAF (Web Application Firewall), IDS/IPS, UTM (Unified Threat Management), dedicated anti-DDoS appliance products to mitigate the impact of DDoS attacks.

③ Use Content Delivery Network (CDN) services

When using a content delivery network (CDN) service, you must hide the IP address of the origin server to prevent direct access to the origin server that stores the original distributed content.

④ Use other anti-DDoS measures

Internet or cloud service providers also offer other helpful measures, such as blocking communications that cause DDoS attacks.

⑤ Implement redundant servers and communication lines

When switching to an alternative, you should do so within a short period of time to avoid interfering with the detection of DDoS attacks. Consider implementing redundant server arrangements and communication lines.

⑥ Review server settings

Where available, enable DDoS mitigation features in servers, endpoints, and communication lines, such as packet filtering, 3-way handshake timeout reduction, flood attack prevention, and application gateway.

2. Measures based on stimulating damage of DDoS attacks

① Sort and separate systems in the basis of the importance

You should sort services based on whether they need to be protected at all costs or they can accept a certain period of downtime, and develop a response policy for each based on the sorting. You should also separate critical systems that are necessary for business continuity from networks for other systems.

② Monitor traffic store monitoring records during peacetime

By understanding the traffic conditions in peacetime, you can detect abnormal traffic earlier. As for storing monitoring records, you need to set a certain storage period to understand the fluctuation of monitoring target situations because they are generally fluctuating.

③ Set alerts for abnormal communication

You should set up an alert mechanism so that the appropriate people receive an alert when abnormal communication occurs.

④ Prepare “sorry page”

You should prepare to place “sorry page” on another server and post the situation on social networking sites to inform users about the service situation when the online service or website is unavailable.

⑤ Develop a countermeasure manual with a list of helpful contacts in the event of an incident

You should make a list of contacts, such as the police and relevant government organizations, to whom you should report DDoS attacks, and develop a countermeasure manual and a business continuity plan that include alternatives and notification methods in case your server or Internet connection or any service is unavailable, as well as the contact list.

3. Measures to prevent participation in DDoS attacks

① Take open resolver countermeasures

You should verify that DNS servers you run do not accept recursive queries from unspecified external IP addresses.

② Apply security patches

You should apply security patches to fix OS and application vulnerabilities.

③ Check filtering settings

You should check filtering settings to prevent your organization from sending packets with spoofed IP addresses.

National Center of Incident Readiness and Strategy for Cybersecurity