verizon

Threat Research Advisory Center
Intelligence

Threat Intelligence Advisory

Killnet DDoS Attacks

Executive Summary

Killnet, a Russia aligned threat actor group, recently claimed responsibility for a series of DDoS (distributed denial of service) attacks against U.S. airport websites. The group has called for DDoS attacks on other U.S. infrastructure targets, in retaliation for the U.S. government's support for Ukraine in its war with Russia.

Findings and Impact

The group first appeared in January 2022 as a cybercriminal hack-for-hire vendor. Using Killnet, users could perform Layer 3/4 or Layer 7 DDoS attacks. According to the group's Telegram channel, users could rent a botnet for $1,350 USD per month, which had a capacity of 500Gbps and included 15 infected computers. However, when Russia invaded Ukraine at the end of February, the group quickly voiced its support of Russia's offensive and Killnet's developers began using the Killnet name to launch DDoS attacks against countries opposing Russia or supporting Ukraine. In the past several months the group has targeted organizations in more than 10 NATO member states, including Estonia, Latvia, Lithuania, Norway, Italy, and most recently the United States.

In its most recent campaign, the group asked its supporters to join in on the airport attacks and posted a list of domains to be targeted on its Telegram channel. In total, the group mentioned 49 domains belonging to airports across the United States. The list includes airports in over 20 states including California, Delaware, Florida, Georgia, Illinois, Maryland, Massachusetts, and Michigan. Security researchers observed a total of 15 U.S. airport websites being impacted by DDoS attacks.

The group focuses most of its attacks on government entities while its followers target key industries, such as financial services, transportation, law enforcement, and technology. Killnet often invites subscribers on its Telegram channel to join in on attacks, publicly listing the domains and IP addresses of its targets on Telegram.

Techniques used by Killnet include the following:

- ICMP Flood
- TCP SYN Flood
- TCP SYN / ACK
- TCP RST Flood
- IP Fragmentation
- NTP Flood
- DNS Amplification
- LDAP Connection less (CLAP)

Recommendations

Organizations can employ the following defensive measures to create a more resilient environment to reduce the risk and impact of DDoS attacks:

- **Firewall and router configurations:** Configure firewalls primarily to block unauthorized IP addresses, close unnecessary ports, disable port forwarding, and prevent DNS and ping-based volumetric attacks.
- **Network traffic monitoring:** Understand the organization's network traffic patterns, continuously monitor network traffic, and recognize abnormal activity that would indicate a DDoS attack regardless of volume and duration. Look for warning signs, such as network slowdowns, spotty connectivity, or irregular website shutdowns.
- **DDoS resiliency plan:** Establish business continuity, disaster recovery, and incident response plans that include DDoS protections through ISPs or third-party firms that specialize in DDoS mitigation. Partner with a backup DNS provider to maintain continuity in the event of an attack on primary DNS infrastructure. While these services do not guarantee that attacks will not result in outages, most organizations are not capable of defending against the many varieties of attack tactics on their own.
- **Monitor:** As attacks by Killnet are typically announced on the group's Telegram channels prior to occurring, it is important that organizations monitor these channels for any mentions of their domains and assets.

Customers of Verizon cybersecurity services are reminded that they may engage Verizon's security consulting services to conduct a detailed assessment of their networks. This preventative due-diligence review will help to identify and mitigate any possible malicious activities affecting critical services that can result in data loss and system integrity. For more information or further assistance, please contact your Verizon RRR liaison.