The Internet DDoS Threat Landscape

Global and Regional Update 2023-06-06

John Kristoff, Principal Analyst, NETSCOUT ASERT
A Brief Segue:
DDoS Attack History
Early DDoS Attack Timeline Highlights

- 1973: First DDoS attack
- 1996: Spoofed TCP SYN attacks
- 1997: Reflection/amplification ICMP floods
- 1999: DNS amplification/reflection debuts
- 2000: Windows botnets debut
- 2003: Slammer worm, IPv6 DDoS
- 2005: Attacks surpass 10 Gbps
- 2008: IoT botnet Linux-based Hydra
Internet Traffic Capacity: To Infinity and Beyond
Measurement Platform Overview

- 500+ of the world’s largest networks
- Exposed to 400+ Tb/s daily traffic
- ~ 93 countries, ~ ½ of the world
- 807% ↑ attack frequency since 2013

What 400 Tb/s looks like
Alerts vs. Mitigation at ISPs

- 25% of alerts lead to counter measures
- ISPs scrub medium+high severity alerts
- But pass lower alerts to balance cost, availability, and scale
ISP Mitigation Breakdown

Alerts

S/RTBH

TMS

Flowspec

Count

01/01/22 01/01/23 01/01/22 01/01/23 01/01/22 01/01/23 01/01/22 01/01/23
Alerts vs. Mitigation in the Enterprise

- Nearly 100% of alerts result in active countermeasures
Enterprise Mitigation Breakdown

- More than 40 different countermeasures used
- 1/3 of Enterprise customers leverage geo-loc (IP address) blocking
- Many block 70+ countries in a counter measure (top 5 blocked countries below)

Russia  China  United States  North Korea  Afghanistan
Bad Bots on the Net
Botnet Attacks Against ISPs

~60,000 botnet alerts in 2022-2H

Top Sources
- United States
- China
- South Korea

Top Targets
- South Korea
- United States
- Italy
~350,000 botnet alerts in 2022-2H

**Top Sources**
- China
- India
- United States

**Top Targets**
- United States
- Mexico
- Spain
Rising Tides: Changes in Methodology
HTTP/HTTPS Application Layer Attacks

487% increase since 2019
Direct-path vs. Reflection/amplification

- **Direct-path**
  - 18% +

- **Reflection/amplification**
  - 18% -
Carpet-Bombing DDoS Attacks

110% increase in 2022-2H
DNS Query Flood (Water-Torture) Attacks

243% total increase since 2019

By region:

- APAC: 108%
- EMEA: 131%
- LATAM: 15%
- NAMER: 41%
Adaptive DDoS: Attack Agility
Dissecting an Adaptive DDoS Attack

Costa Rican energy organization

- DDoS attacks can last from mere seconds to months and even years.
- Over the course of 7 days, this DDoS attack showed significant variance.

**HOUR 1**

- **18 Gbps**
  - 3 Attack Vectors

**DAY 2-4**

- **39–190 Gbps**
  - 9 Attack Vectors

**DAY 5-7**

- **195 Gbps**
DDoS Attack Motivations
Know No Bounds
Optical Instruments and Lens Manufacturing in EMEA

- 14,137% \(\uparrow\) attacks in 2022-2H
- 6,000+ attacks in about four months
- Peaks of 260 Gb/s and 42 Mp/s
- No discernible reason for the attacks

\text{b/s} = \text{gigabits per second}

\text{p/s} = \text{packets per second}
Wireless Telecommunications

Global

- 79% increase in attacks since 2020
- Accounts for 20% of all global attacks
- Coincides with growth of 5G Wireless
- **Motivation**: Attacks almost certainly disproportionate to gaming and general availability of more wireless connected IoT devices.
Manufacturing

Global

• Sustained attacks over four months
• 950+ billion malformed packets/day
• Predominantly app-layer attacks
• Coincides with ransomware event halting manufacturer operations
• Motivation?: Financial gain
• Attack spikes directly aligned with pro-Russian Killnet operations.

- **JULY 1-7, 2022**
  A massive spike in attacks hitting just one day after U.S. President Biden’s public remarks at the G7 Summit in Madrid resulted in hundreds of attacks on the national security sector over several days. The tail end of this spike maps directly to Killnet tweets claiming victory in taking down the congress.gov website.

- **OCTOBER 9, 2022**
  Revealed a more moderate spike that correlates to confirmation from the United States Department of the Treasury on thwarting an attack from Killnet.

- **LATE NOVEMBER-DECEMBER 2022**
  Killnet repeatedly called for attacks on US government entities, contractors, and websites. The blanket call for action had an impact with attacks surging throughout the month. This includes the second-highest peak in attacks against this sector on December 1, the same day the French and U.S. presidents re-affirmed their support for Ukraine.

- **DECEMBER 10-13, 2022**
  Killnet once again called for action against the U.S. Congress. At the same time, we saw an increase in attacks on the national security sector and legislative bodies.

• **Motivation?**: Geopolitical hacktivism
Keeping Our Eyes Open
IPv6 Attacks

We’re seeing activity, but with a caveat
Take Down and Take Action
Botnet Takedown

June 2022 – Moderate Effect
DDoS-for-Hire Takedown

December 2022 – Isolated Effects to Regional Service Providers

Graph showing the number of attacks per day from 10/30/2022 to 01/01/2023, with a peak on 11/11/2022 with 1,184 attacks.
Community Security Efforts

Efforts around Best Current Practices (BCPs) in Effect

18% decrease in reflection/amplification DDoS attacks
DDoS is an Availability Problem
Remember When We Talked About 400 Tb/s?

Outages become visible with network statistics
Thank you.


netscout.com/threatreport