CASE STUDY

NSFOCUS
SECURITY MADE SMART AND SIMPLE

A 400G DDoS Attack Event Captured by NSFOCUS in Hong Kong S.A.R.

About NSFOCUS

NSFOCUS is an iconic network and cyber security provider for telecom carriers, BFSI, enterprises, healthcare, retail and SMBs. It has a proven track record of protecting over 25% of the Fortune Global 500 companies, including four of the five largest banks and six of the world's top ten telecommunications companies.

NSFOCUS delivers a holistic suite of security products powered by industry leading threat intelligence. These security products work in concert to protect you from massive volumetric DDoS attacks, Web threats and advanced persistent threats (APTs).

Connect with NSFOCUS:

Blog: nsfocusglobal.com/blog/

LinkedIn @nsfocus

Twitter @NSFOCUS_Intl

Facebook @nsfocus

NSFOCUS Website:

www.nsfocusglobal.com

EVENT LOOK BACK

An NSFOCUS Cloud DPS customer with their servers located in Hong Kong SAR has encountered a series of mass DDoS attacks lasted for four days, from June 20th to 24th.

The attackers managed to create several spikes including the biggest one reaching 399.2 Gbps and followed by another at 360 Gbps. It is noticeable that both the above mentioned two main spikes started in the night after 20:30 so it seems that attacker does understand the busy hours of customer's business and make it on purpose.

UDP flood is the major type of the attacks and occupies over 99% of the traffic.

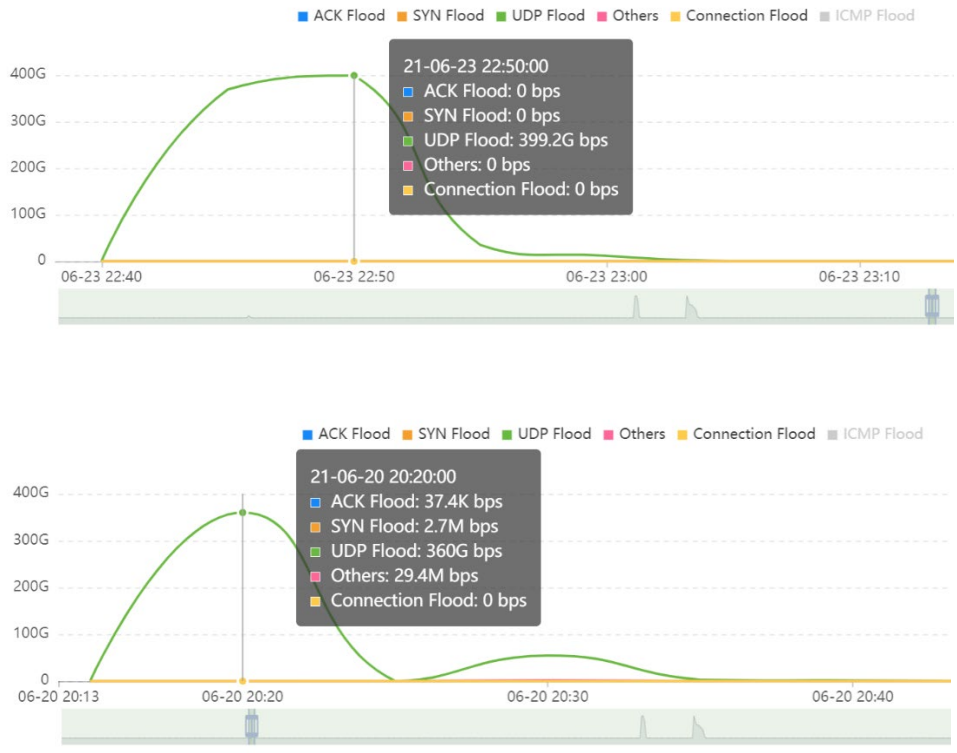

Fig 2: Spike at 360Gbps

NSFOCUS
SECURITY MADE SMART AND SIMPLE

EFFORT AND RESULT

At the very beginning when the customer connected to NSFOCUS Cloud DPS one month ago, NSFOCUS SOC experts studied the customer traffic characteristics and applied a set of optimized protection policies to maximize the mitigation effect.

Thanks to the always-on mode, the attacks were mitigated at zero seconds automatically at its arrival and mitigation status was proactively monitored by NSFOCUS 24/7 SOC. Traffic samples were also captured instantly to check and verify that it was the current policy that worked and optimization could be done when necessary.

In this event, NSFOCUS Cloud DPS managed to mitigate more than 99.8% of malicious traffic and only few megabits reached to the customer, services were not affected.

For more information, please contact:

U.S.

Tel: + 1 408-907-6638

EMEA

Tel: +44 (0) 20 3882 7025

LATAM

Tel: +55 11 3521-7124

Email: contato@nsfocusglobal.com

APAC

Email: apmarketing@nsfocusglobal.com

GCR:

Email: gcrmarketing@nsfocusglobal.com