The Terabit era and beyond

CSTSE 2019

Marco Gioanola, Services Architect
NETSCOUT Arbor

Guardians of the connected world since 2000

- Arbor Networks, founded in Ann Arbor, Michigan, born out of the Lighthouse Project at the University of Michigan, named in 2016 as one of the top 10 projects ever financed by the US’ Defense Advanced Research Projects Agency.

Global market leader in DDoS detection and mitigation

Part of NETSCOUT since 2015

ATLAS

Everything it learns, it remembers!

A global brain and memory, learning from the activity and interactions between identities and finding outliers.

Statistics:
- 400 Active SP Contributors
- ATLAS “sees” 1/3 of All Internet Traffic
- Ingests 140Tbps
- 200K Malware Samples per Day

ASNs: 44,570
Unique IPv4 Addresses: 2.63B
“Dark” IPv4 Addresses: 1.76M
Increase in size of DDoS attacks, 2005-2018

We can observe here a discernable increase in attack sizes and that attack sizes are still on the increase. Most interestingly, the following details on attack magnitude were reported:

- 17 Gbps was largest sustained attack reported
- 22 Mpps UDP flood was reported
- 14 Mpps SYN flood was reported

One hundred times increase.
DDoS Statistics

Frequency of attacks, «G7» countries
DDoS Statistics

Largest attack, «G7» countries
DDoS Statistics

Largest attacks, Germany
DDoS Statistics

Frequency of attacks, Germany

![Bar chart showing the frequency of DDoS attacks in Germany from February to January. The chart indicates the number of attacks per month, with the highest in February at 13.8k and the lowest in January at 8.01k.]
DDoS Statistics

Frequency of attacks longer than 3 hours, Germany
How did we get here?

Broadband trends

Weaponization

Botconomics

Internet of Things
Command, control, attack, steal

STOLEN PENCIL Campaign

As reported in a December 2018 blog post, ASERT discovered a campaign of probable DPRK origin targeting universities. ASERT saw massive credential theft across four universities, where all of the compromised targets were in the mechanical engineering field and focused on biomedical research. One victim was a member of a Pacific-region policy non-profit. ASERT research uncovered a far-reaching campaign resulting in ongoing collaboration with industry professionals around the world.

DPRK utilized a browser plugin in the STOLEN PENCIL campaign, going so far as to leave reviews on the plugin from compromised accounts in a likely effort to establish legitimacy.
Research – Technology – Services

NETSCOUT Threat Report
netscout.com/threatreport

Early Warning Service

DDoS attacks

Cloud / Edge protection

Stateless Threat Gateway

Data exfiltration
Command & Control traffic

Arbor Edge Defense

NETSCOUT Arbor

Arbor ASERT DDOS Notification
Below is your updated Arbor Threat Report. It details potential malicious attack activities that Arbor has identified and is directing at your company.
The DDoS Early Warning Service intends to provide targeted early warnings about potential DDoS attacks as identified by Arbor from threat communications. Armed with the information on the early warning periods, you may be able to take immediate actions to better prepare for mitigating the attacks.

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor

Arbor
Thank You.

Marco.Gioanola@netscout.com