DDoS Attack by NTP Amplification

NetVizura

Challenge

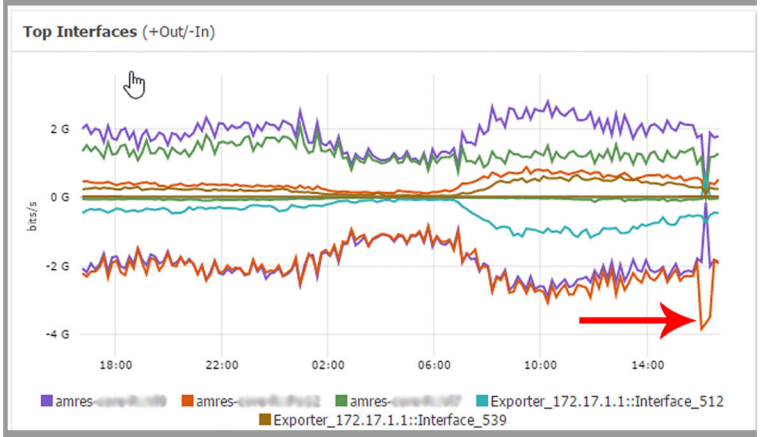
Cyber attacks have become part of our everyday life and we have all heard in the news how some person, large enterprise or government was targeted. They are extremely damaging because they can put our customers' trust into question, threaten long-term reputation, lower our income or accrue additional penalties.

NTP amplification is a specific type of DDoS (Distributed Denial of Service) attack where public NTP (Network Time Protocol) servers are saturated with UDP (User Datagram Protocol) traffic. In addition to that, packet requests sent often causes a disproportionate server response and thus amplify it's effect. Preventing NTP amplification attacks is challenging because responses from the NTP servers actually represent a legitimate traffic. However, quick and effective reaction is possible by provisioning server with extra resources and filtering unwanted traffic.

AMRES (Academic Network of Serbia) regularly experiences such attacks aimed at bringing down its websites and other resources available over Internet. In that sense, NetVizura NetFlow Analyzer plays an indispensable alerting, investigation and reaction role to quickly recover its public services.

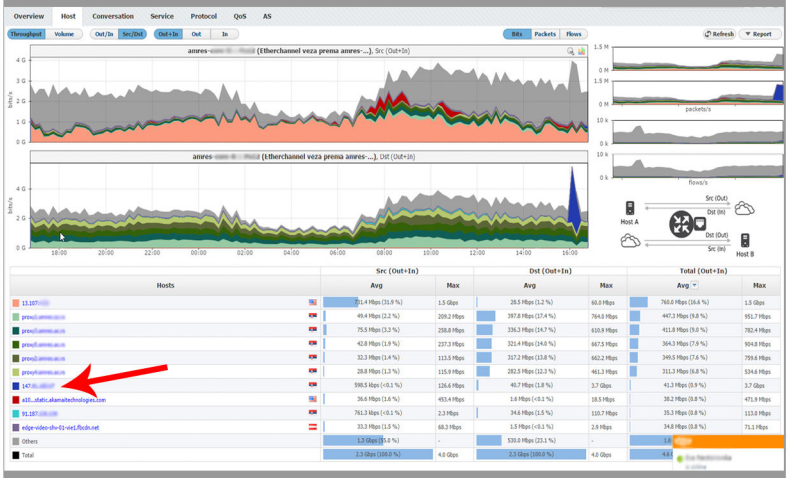
Solution

Top Interfaces 1.



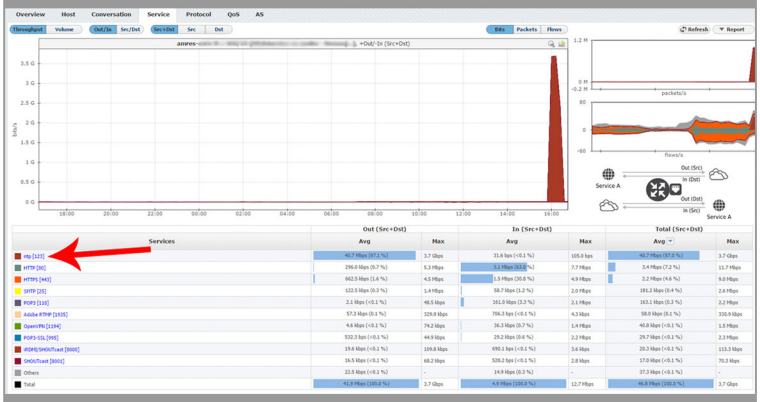
Sudden traffic increase on interface amres- brings down other interfaces on the same router

Interface Hosts 2.



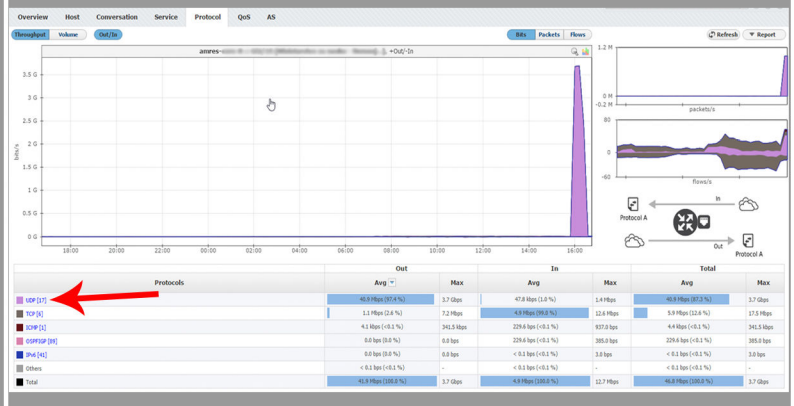
High bits and packets from multiple source IPs (Others) reaching destination IP 147.

Interface Services 3.



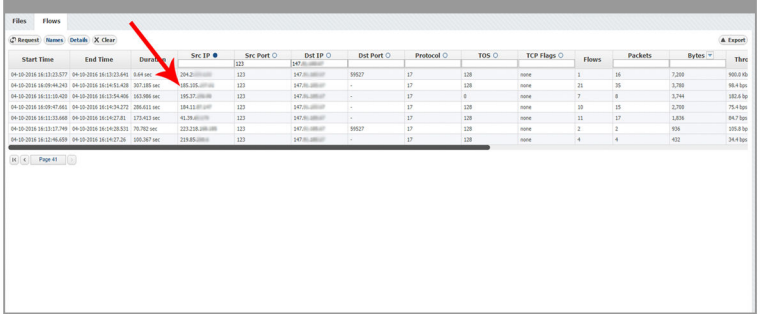
NTP service (port) used

Interface Protocols 4.



UDP protocol used

Raw Data Flows 5.



List of source IPs using NTP port (123) and reaching destination IP 147.

NetVizura

Conclusion

DNS and NTP are convinient for the attackers, because small query packets can get an answer 200x bigger, which, combined with IP spoofing, can lead to easier realisation of DDoS attack.

In this example, we have shown the most commonly used protocols for conducting amplification attack - the ones that are generaly used for typical network flow. This complicated spliting and identification of legitimate NTP traffic and traffic generated as a part of amplification attack.

In this case, NTP DDoS attack was extremely heightened, as a result of the huge number of Hosts operating and generating answer to a false query.

Despite these challenges, by using visual tools that NetFlow Analyzer provides, it was easy to identify the target of this attack and quickly make necessary recovery actions.