Contribution ID: **49** Type: **not specified**

Identifying Suspicious Network Activities in Grid Network Traffic: Finding the needle in a stack of needles

Tuesday, 7 March 2017 16:00 (30 minutes)

In this presentation we will share our experience with analysing a year of grid network flow data. The network flow data provides only limited information regarding the nature of network traffic that traveled through the network segments. Therefore researchers need to come up with additional methods of anomaly detection, data enrichment and cross-referencing in order to effectively identify 'true-positives': a subset network flows which could be of some interest to security officers: from denial of service attacks, to malware operations, network scanning and attacker's lateral movements. In this study having access to other network data feeds (such as honeypot networks) and full packet payload monitoring, so we demonstrate how such sources could be effectively leveraged in identifying and verifying suspicious network activities.

Summary

A quick summary of the presentation:

Visibility

Data subsets by Protocol

Analyzing Traffic Direction (internal/external/incoming/outgoing flows)

Outgoing connections using high-risk protocols

Identifying Local Assets

Threats

Identifying Recon activities :Scans, Bruteforce sessions

Anomalies: TCP and UDP

High-risk flows

Identifying C2 calls

Lateral spreading and worming activities

Exfiltration

Infrastructure abuse

DDOS

DDOS and DNS traffic sessions

DDOS and SSDP

Exploring 'bad' SNMP

'bad' NTP traffic

Conclusions and Future research

Primary author: Mr YAROCHKIN, Fyodor (Academia Sinica)

Presenter: Mr YAROCHKIN, Fyodor (Academia Sinica)

Session Classification: Network, Security, Infrastructure & Operations II

Track Classification: Networking, Security, Infrastructure & Operations