uila

Uila's DPI Methods for Detecting Lateral Movement

Uila's Deep Packet Inspection Engine monitors network traffic in real-time, using it's built-in library of protocol and application metadata to distinguish between normal and anomalous behaviors. This allows lateral movement of traffic to be rapidly detected and the suspicious activity identified.

This DPI capability in addition with Uila's ability to identify thousands of latest Advanced Threats, make it a comprehensive security monitoring solution.

DPI Methods for Detecting Different Types of Network-based Lateral Movement

Lateral Movement using File-Share

How it works	Detection based on Uila DPI
Access to shared resources: • Remote folders • Network drives	Uila DPI software can detect traffic based on protocols such as: • Netbios/NBNS • Samba (SMB/CIFS)

uila

Lateral Movement using Remote Resources

How it works

1.Malware runs application
2.Accesses local resources & files
3. Transfers/modifies files
4. Installs agents

Examples: Remote Desktop, VNC, TeamViewer, Ammyy admin

Detection based on Uila DPI

Uila DPI can detect traffic based on protocols such as:

- RDP
- RFB
- TeamViewer
- Ammyy admin

Lateral Movement using Services/Server Scans

How it works

Malware identifies services of interest:

- Databases
- Web applications
- Remote access functionalities
- Network Services

Tools used: - NMAP: TCP (SYN, Ack, Fin/Ack), - UDP - SSDP (different than DDOS)

Detection based on Uila DPI

Uila DPI can detect traffic based on protocols such as:

- TCP connections (empty)
- UDP connections (empty)
- SSDP (including metadata)
- ICMP / ICMP6