Deep Packet Inspection for Lateral Movement Detection: Enabling Faster, More Accurate Detection of Network Infiltration

Leveraging Deep Packet Inspection (DPI) software can help organizations detect possible cyber attacks as they carry out lateral movements. Qosmos ixEngine examines the data part of every packet that passes an inspection point. With the ability to recognize over 3200 protocols and extract more than 5000 metadata, it is able to immediately detect non-compliant protocols and traffic types that could indicate the presence of a virus, spam, malware, ransomware or other malicious activity.

### The Challenge

Despite the advanced level of cyber security technology in place and all the efforts made by administrators to protect their networks, no organization is immune from malware attacks. Malware will try to penetrate a network through email phishing, a compromised external drive, an infected personal device, an IT misconfiguration or an unknown exploit. Once it has gained entry to the network, the attack typically evolves through the different stages of the cyber kill chain. It carries out early reconnaissance, creates a state of persistence, seeks access to the outside world through a Command & Control server, and then initiates a series of lateral movements (access to resources, propagation, privileges, etc.), until it reaches its final goal of data exfiltration, data destruction, or demand for ransom.

![Figure 1: The Cyber Kill Chain](image)

To avoid the consequences of such an attack it is necessary to detect the malware as rapidly as possible. However, distinguishing potential threats from legitimate traffic requires the management and analysis of huge amounts of data often complicated by the high number of false positives. The time required to do this means that many current cybersecurity solutions only detect infiltrations when it’s too late and most are unable to defend networks against 0-day attacks.

### The Solution

During the lateral movements phase, an attack generates specific types of network traffic as it searches the network and gathers valuable information for exfiltration. It is here that it becomes most vulnerable to detection.

Qosmos ixEngine monitors network traffic, analyzing flows in real-time, using an extensive library of protocol and application metadata to distinguish between normal and abnormal activity. As a result, lateral movements are rapidly detected and the suspicious activity identified. An alert is sent to the system’s cybersecurity software along with intelligence on the activity, allowing the malware to be immediately located and propagation of the attack halted.
Techniques used by Malware during Lateral Movement

For host-based techniques (Token stealing / credential stealing, Pass-the-hash, PowerShell, Network sniffing,...), DPI is of limited added value in detecting the threat.

However, for network-based techniques, DPI is highly effective in detecting the lateral movement:

- File shares
- Remote desktop, VNC, TeamViewer, Ammyy Admin
- Port scan
- Windows Management Instrumentation (WMI)
- Active directory & admin shares
- ARP spoofing

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

Lateral Movement using File Shares

<table>
<thead>
<tr>
<th>How it Works</th>
<th>Detection Based on DPI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access to shared resources: - Remote folders - Network drives</td>
<td>DPI software can detect traffic based on protocols such as: - Netbios/NBNS - Samba (SMB/CIFS)</td>
</tr>
</tbody>
</table>

Lateral Movement using Remote Resources

<table>
<thead>
<tr>
<th>How it Works</th>
<th>Detection Based on DPI</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Malware runs application 2. Accesses local resources/files 3. Transfers/modify files 4. Installs agents Examples: Remote Desktop, VNC, TeamViewer, Ammyy admin</td>
<td>DPI software can detect traffic based on protocols such as: - RDP - RFB - TeamViewer - Ammyy admin</td>
</tr>
</tbody>
</table>

Lateral Movement using Services/Servers Scan

<table>
<thead>
<tr>
<th>How it Works</th>
<th>Detection Based on DPI</th>
</tr>
</thead>
<tbody>
<tr>
<td>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)</td>
<td>DPI software can detect traffic based on protocols such as: - TCP connections (empty) - UDP connections (empty) - SSDP (including metadata) - ICMP / ICMP6</td>
</tr>
</tbody>
</table>

DPI software is highly effective in accurately detecting network-based lateral movement, while allowing rapid containment of attacks and remediation. The protocol information and metadata can be used to improve the results of user behavior analysis and machine learning, and to enable mitigation at each stage of the kill chain, improving the effectiveness of security solutions.