ENEA
Qosmos Division

Protecting Against Malware: Using DPI Inside Security Solutions to Detect Lateral Movements

by Erik Larsson, SVP Marketing, Enea and
Belgacem Hlali, Senior Global Technical Account Manager, Qosmos Division, Enea

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

This white paper looks at attack techniques, the vulnerability of an attack during the lateral movement phase, the ability of DPI to detect infiltration during this phase and different techniques for doing so.

No Organization is Immune from Malware Attacks

One of the worst nightmares for a network administrator is knowing that despite all the security technology in place and all the efforts made to protect a network, infiltration still happens. For 87% or organizations, it happens at least once a year. For 20% of organizations, it happens at least 100 times a year. More worrying still, 9% of organizations are unsure whether any incidents actually occurred[1].

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

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.

44% of respondents in a survey carried out by SDxCentral for their 2017 SDx Infrastructure Security Report[2] indicated that lack of visibility was one of their major challenges.

The length of time currently required to analyze the data travelling across a network means that most of today's cyber security solutions are unable to defend networks against 0-day attacks.

The Vulnerability of Lateral Movements

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.

DPI software can be used to monitor network traffic and analyze 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.

Since lateral movement typically accounts for the longest period in an attack timeline, it presents a window of opportunity during which DPI can detect the suspicious activity and alert the security system so that action can be taken before any damage is done.

Typical Techniques Used by Malware During Lateral Movement

For host-based techniques, DPI is of limited added value in detecting the threat. These include:

- Token stealing / credential stealing, Pass-the-hash
- PowerShell
- Network sniffing

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

ENEA
Qosmos Division

How DPI Detects Different Types of Network-based Lateral Movement

Lateral Movement using File Shares

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

Lateral Movement using Remote Resources

How it works	Detection based on DPI
1. Malware runs application **2.** Accesses local resources/files **3.** Transfers/modifies files **4.** Installs agents Examples: Remote Desktop, VNC, TeamViewer, Ammyy admin	DPI software can detect traffic based on protocols such as: - RDP - RFB - TeamViewer - Ammyy admin

Lateral Movement using Services/Servers Scan

How it works	Detection based on DPI
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)	DPI software can detect traffic based on protocols such as: - TCP connections (empty) - UDP connections (empty) - SSDP (including metadata) - ICMP / ICMP6

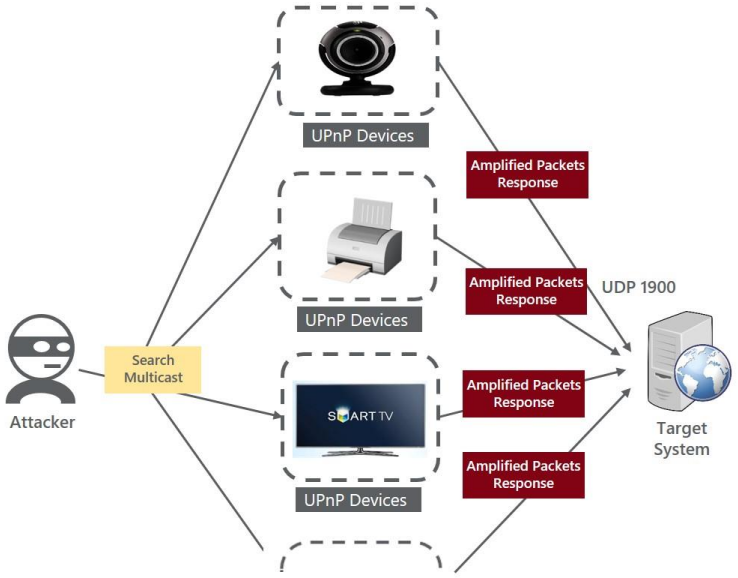
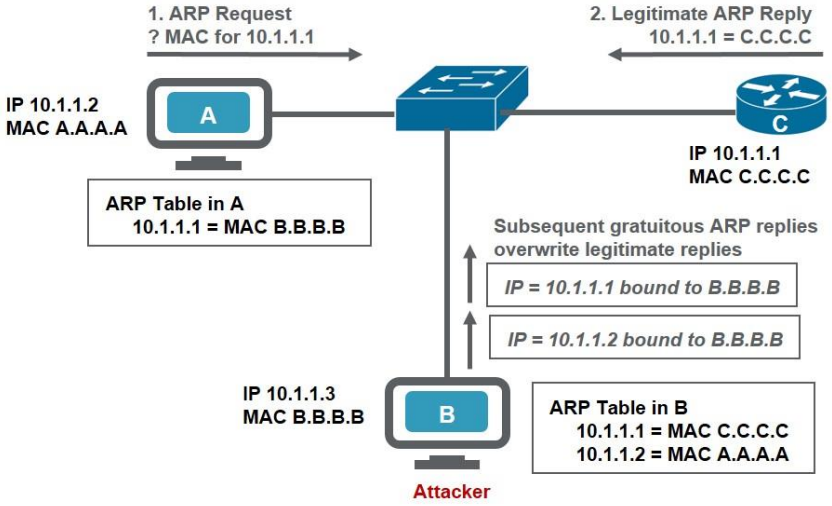


Figure 2: SSDP Flood - DPI software can detect traffic based on SSDP protocols

Lateral Movement using ARP spoofing/poisoning (man-in-the-middle)

How it works	Detection based on DPI
Malware redirects traffic of a specific host/user: - Gratuitous ARP - Modified ARP request Tools used: - ARPspoof - ARPoison - Subterfuge	DPI software can detect ARP traffic and extract useful metadata such as MAC addresses



ARP spoofing attacks and ARP cache poisoning can occur because ARP allows a gratuitous reply from a host even if an ARP request was not received. After the attack, all traffic from the device under attack flows through the attacker's computer and then to the router, switch, or host.

ENEA
Qosmos Division

Conclusion

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.

Enea's Qosmos ixEngine® is a Software Development Kit that can identify more than 3,000 protocols, including key network protocols such as SMB, DHCP, and Industrial Control System (ICS) protocols. Qosmos ixEngine can also extract additional protocol information in the form of metadata (recognizing up to 4500), further improving effectiveness of cybersecurity solutions.

Enea's Qosmos Division has a distinguished background working with cybersecurity vendors, whom successfully use Qosmos ixEngine inside their products, across a wide range of applications.

1. 2017 Incident Response Survey by the SANS Institute
   https://www.sans.org/reading-room/whitepapers/analyst/show-on-2017-incident-response-survey-37815

2. 2017 SDx Infrastructure Security Report - The Rise of Software-Defined Security (SDS)
   https://www.sdxcentral.com/articles/announcements/sdx-infrastructure-security-report-available/2017/09/

For additional content on how to use DPI to detect cyber attacks during the lateral movement phase, please go to: http://www.qosmos.com/dpi-for-lateral-movement-detection/

About the Authors

Erik Larsson is Senior Vice President of Marketing at Enea, where he drives product marketing, demand generation, branding and communication. Erik's views on high-tech trends are regularly featured in articles, blog posts, webcasts, video interviews, and industry events.

Belgacem Hlali is Senior Global Technical Account Manager at the Qosmos Division of Enea. He has over 17 years' experience in the architecture, design and development of IP technologies with specific expertise in Deep Packet Inspection, Networking and IP Security.

To contact the authors or for more information: http://www.qosmos.com/company/contact-us/

About the Qosmos Division of Enea

The Qosmos Division of Enea is a pioneer in Deep Packet Inspection technology for physical, SDN and NFV architectures. Qosmos ixEngine®, the company's DPI engine, is the de facto industry-standard for IP classification and metadata extraction. Security solution vendors and integrators use Qosmos to gain application visibility, accelerate product development and strengthen capabilities of new solutions. They benefit from Qosmos technical expertise in the development and integration of DPI technologies in their products and from continuous protocol signature updates, ensuring that their solutions always provide the most accurate network analysis available on the market. For more information on Qosmos technology and DPI in security solutions, please visit: http://www.qosmos.com/cybersecurity/overview/