ENEA

Application Use Case

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 3000 protocols and extract more than 4500 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.

Key Facts

- Qosmos ixEngine is a DPI-based Software Development Kit that examines data packets crossing a network
- Over 3000 protocols classified and continuously updated, 4500 application metadata extracted
- Identifies protocols and applications based on flow pattern matching, session correlation, heuristics and statistical analysis
- Identifies key network protocols such as SMB, DHCP, and Industrial Control System (ICS) protocols
- Users can develop their own signature plugins
- Modular architecture (flow management, regular expression engine, http parsing, etc.)
- Portable architecture (x86, Cavium, ARM)

Benefits

- Accurately and rapidly detects network-based lateral movement to allow containment of attacks and immediate remediation
- Protocol information and metadata can be used to improve the results of user behavior analysis and machine learning
- Enables mitigation at each stage of the kill chain, improving the effectiveness of security solutions

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.

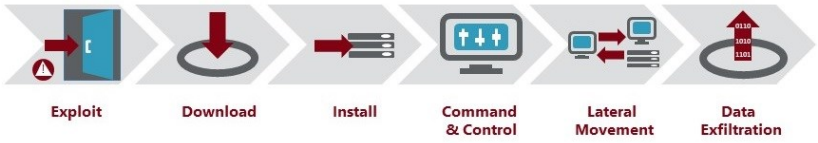

Figure 1: The Cyber Kill Chain

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

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

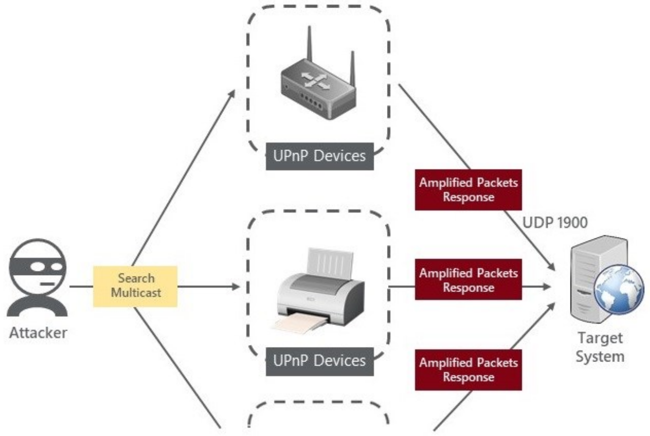
UPnP Devices
Amplified Packets Response
UDP 1900
Attacker
Search Multicast
Amplified Packets Response
Target System
UPnP Devices
Amplified Packets Response

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

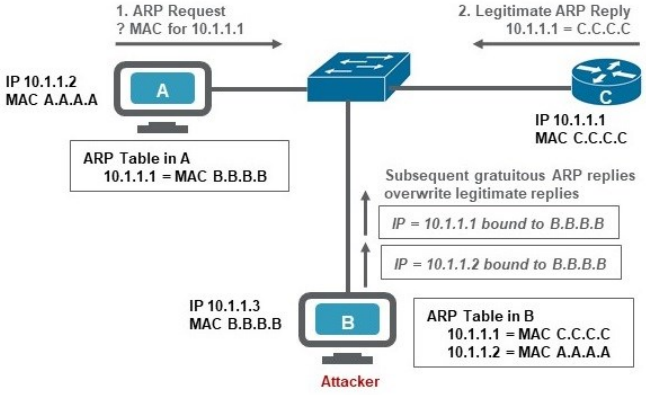

Figure 3: ARP spoofing attacks and ARP cache poisoning occur because ARP allows a gratuitous reply from a host even if an ARP request was not received. After the attack, all traffic from the targeted device flows through the attacker's computer and then to the router, switch, or host.

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.

Qosmos, a division of Enea, is the leader in IP traffic classification and network intelligence technology used in physical, SDN and NFV architectures. Qosmos ixEngine software development kit and components are embedded by vendors and integrators into their products sold to telcos, cloud service providers and enterprises. For more information: www.qosmos.com