SPLUNK COMMAND AND CONTROL 2025/12/16

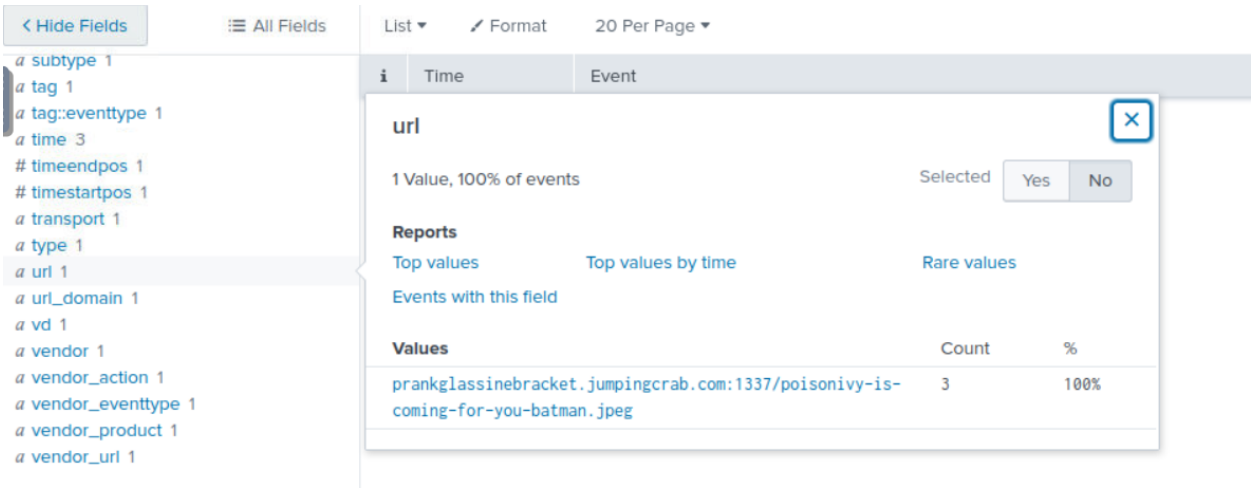
Command and Control:

The attacker uploaded the file to the server before defacing it. While doing so, the attacker used a Dynamic DNS to resolve a malicious IP. Our objective would be to find the IP that the attacker decided the DNS.

To investigate the communication to and from the adversary's IP addresses, we will be examining the network-centric log sources mentioned above. We will first pick fortigate_utm to review the firewall logs and then move on to the other log sources.

STEP 1: This attack used dynamic DNS to resolve to the malicious IP. What fully qualified domain name (FQDN) is associated with this attack?

Search Query: index=botsv1 sourcetype=fortigate_utm"poisonivy-is-coming-for-you-batman.jpeg"



To find this I looked used the mentioned search query and scrolled through the left panel to find the 'uri' field and clicked on it to find our value – '**prankglassinebracket.jumpingcrab.com**'

Conclusion Summary

In the Command and Control phase, the investigation focused on identifying how the attacker communicated with external infrastructure after compromising the server. By analysing FortiGate firewall logs in Splunk, evidence of Dynamic DNS usage was uncovered. The attacker leveraged a malicious domain, **prankglassinebracket.jumpingcrab.com**, to resolve and communicate with the command-and-control IP. This finding confirms the attacker's use of Dynamic DNS to maintain control and conceal their infrastructure during the attack lifecycle.