SOC Analyst Report

Case ID: IR-2024-1023-DNS001

Date: October 16, 2024

Subject: Analysis of Suspicious DNS Traffic Patterns

Tool: Splunk

Analyst: ALI CHINASA JULIET

Executive Summary

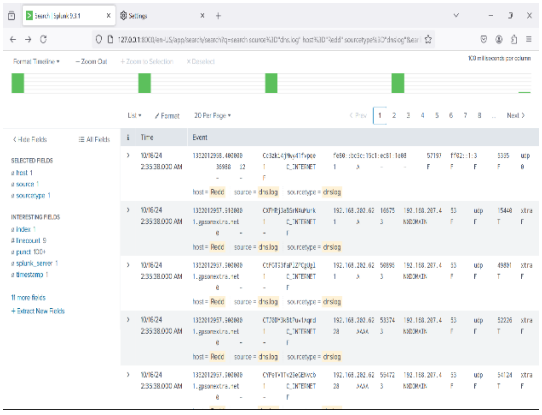
This report covers the analysis of DNS traffic logs extracted from a host named "Redd" using Splunk. The analysis reveals several DNS queries directed to various destination IPs, many of which returned NXDOMAIN responses, indicating failed resolution attempts. Additionally, PTR and A record queries were identified, pointing to both successful and failed DNS lookups. The investigation also involved VirusTotal and WHOIS lookups on notable IP addresses, particularly internal sources generating suspicious traffic, though no immediate malicious indicators were flagged. However, the volume and patterns of the traffic suggest potential issues worth further investigation, including data exfiltration and internal misconfigurations.

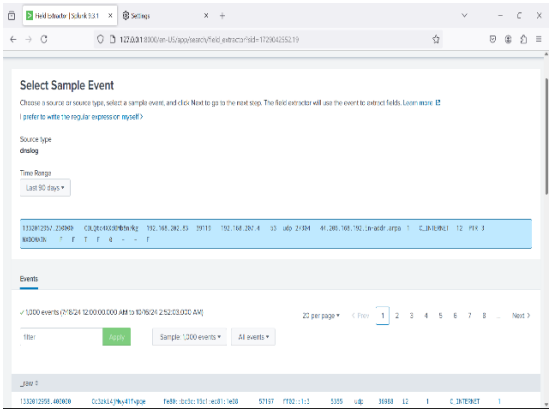
Overview

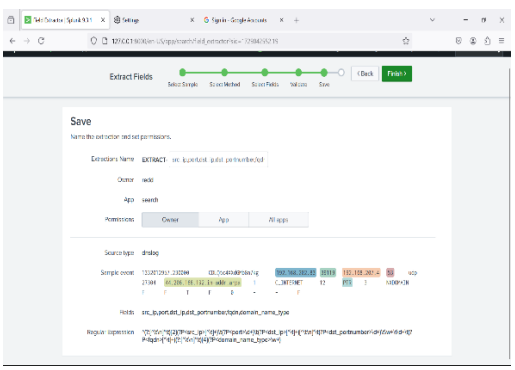
The investigation focused on DNS logs captured on October 16, 2024, around 2:35 AM. These logs were sourced from the host "Redd," using the dns.log as the event source and dnslog as the sourcetype. Several key fields—such as source and destination IP addresses, hostnames, and DNS record types (A, AAAA, and PTR)—were isolated using Splunk's field extraction capabilities. The majority of the DNS queries returned NXDOMAIN responses, raising concerns about the intent and origin of these failed lookups.

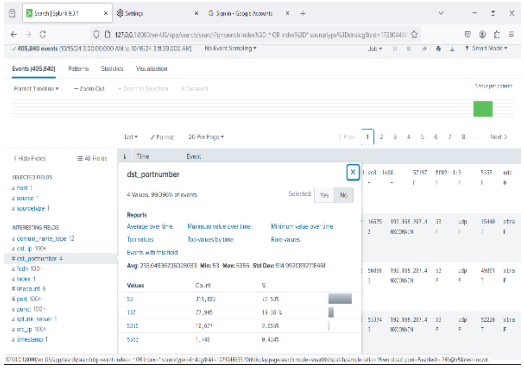
Analysis and Investigation

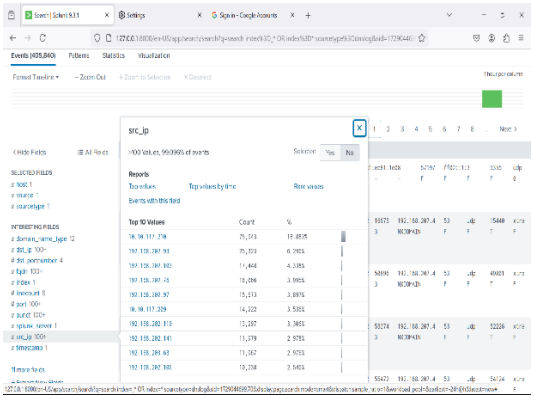
1. **DNS Queries:**
   The logs indicated frequent DNS queries to internal servers, such as 192.168.202.83 and 192.168.207.4. A significant number of these queries returned NXDOMAIN responses, meaning the requested domains could not be resolved. For instance, a query from 192.168.202.62 to 1.gpsonextra.net resulted in an NXDOMAIN response. The pattern of repeated failed lookups may suggest typos, failed access attempts to legitimate services, or more concerning behavior such as scanning for unavailable resources.

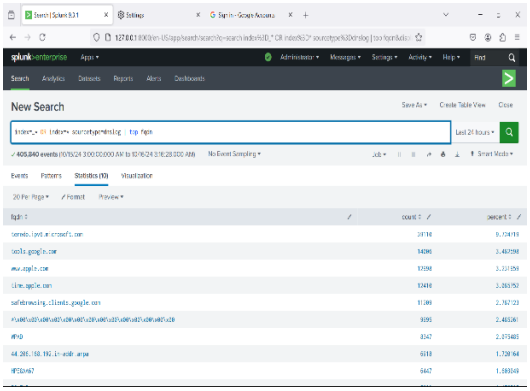


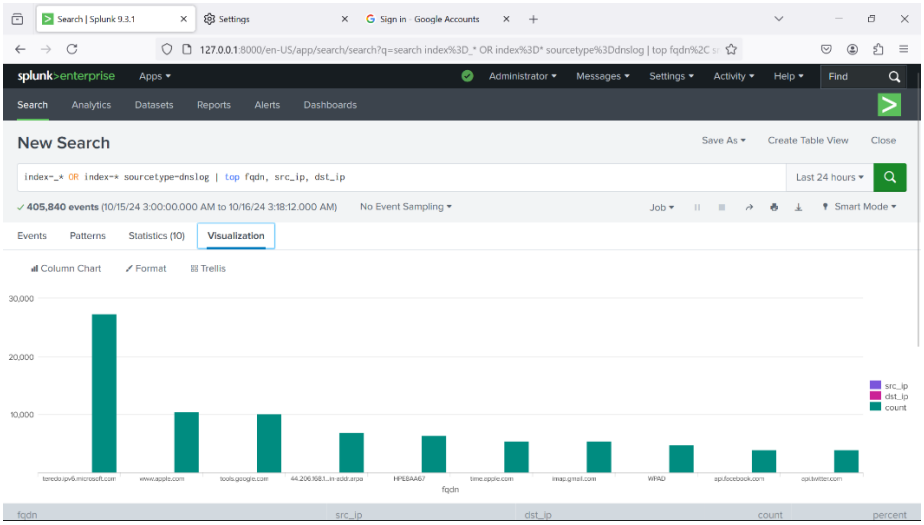



Extract Fields
Save


dst_portnumber

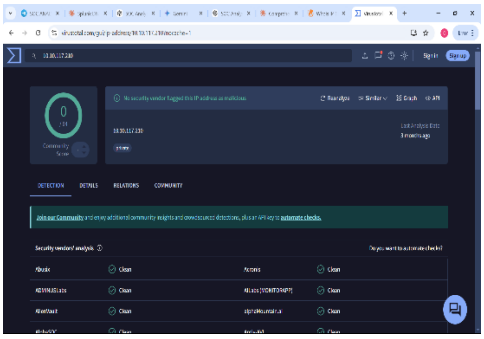

src_ip

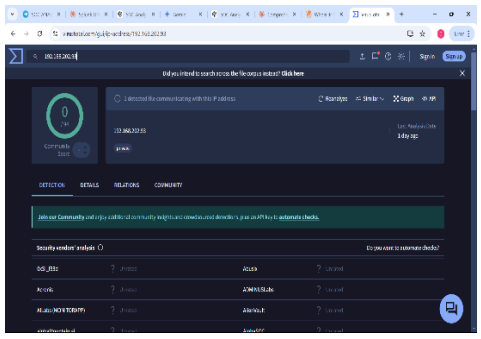

New Search

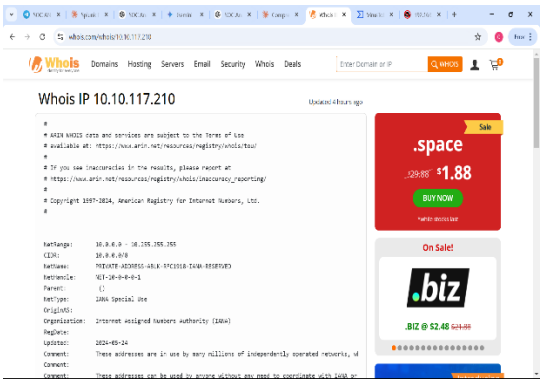

Search | Splunk 9.3.1
Settings
Sign in - Google Accounts
127.0.0.1:8000/en-US/app/search/search?q=search index%3D_* OR index%3D* sourcetype%3Ddnslog | top fqdn%2C
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
New Search
Save As
Create Table View
Close
index=_* OR index=* sourcetype=dnslog | top fqdn, src_ip, dst_ip
Last 24 hours
✓ 405,840 events (10/15/24 3:00:00.000 AM to 10/16/24 3:18:12.000 AM)
No Event Sampling
Job
Smart Mode
Events
Patterns
Statistics (10)
Visualization
Column Chart
Format
Trellis
30,000
20,000
10,000
src_ip
dst_ip
count
fqdn
fqdn
src_ip
dst_ip
count
percent

2. **Record Types:**
   Several different types of DNS records were queried, reflecting typical DNS activity but also raising some questions:
   - **A Record:** Standard IPv4 address lookups were prevalent.
   - **AAAA Record:** These queries attempted to resolve IPv6 addresses.
   - **PTR Record:** These reverse DNS lookups aimed to resolve IP addresses back to domain names, which may be used for internal network activity.
3. **Suspicious Internal Activity:**
   - **Host:** HPE8AA67 (192.168.202.76) was identified as generating a high volume of broadcast queries to the IP 192.168.202.255. These excessive queries to a broadcast address, with no known legitimate service registration, suggest possible internal scanning or misconfiguration. This host warrants immediate isolation for further analysis.
4. **Traffic Volume and Patterns:**
   - **Source IP 10.10.117.210** generated the highest volume of DNS queries, totaling 75,943 requests (18.88% of all DNS events).

     - **VirusTotal Analysis:** No malicious activity was associated with this IP.
     - **WHOIS Lookup:** The IP is internal (RFC1918), confirming that it belongs to the organization's private network.
     - Despite the clean findings, the unusually high traffic directed toward DNS servers and external services, such as Teredo tunneling, indicates the need for further scrutiny.







5. **External Service Queries:**

   - **Teredo.ipv6.microsoft.com:** This service, receiving 27,425 queries, is often used for IPv6 tunneling. Although VirusTotal flagged no malicious activity, the large volume of traffic to a tunneling service suggests the potential for data exfiltration or covert communications.
   - **Tools.google.com:** Another destination with a notable volume of queries (10,179), VirusTotal returned no malicious indicators. However, the frequency of these requests merits further monitoring to prevent any unauthorized data transfers through this service.

Conclusion

The DNS traffic logs reveal typical DNS query behavior, but the high volume of NXDOMAIN responses, unusual internal broadcast queries, and excessive traffic to tunneling services like Microsoft Teredo raise concerns. While VirusTotal and WHOIS investigations did not indicate direct malicious activity, the volume of DNS traffic—especially to external services—suggests that the host "Redd" or its associated queries may be involved in misconfigurations or more subtle, suspicious activity. Further monitoring and investigation of the unresolved queries and internal broadcast traffic are recommended to rule out any threats.

Recommendations

1. **Short-term Actions:**
   - Investigate the sources of repeated NXDOMAIN responses to determine whether they are misconfigurations or indicative of malicious behavior.
   - Isolate the host HPE8AA67 (192.168.202.76), which generated the suspicious broadcast queries, to prevent potential network scanning from continuing.
   - Block Teredo tunneling, as its use may facilitate unauthorized data transfers.

- Implement DNS query rate limiting to mitigate potential abuse from high-volume querying hosts.

2. **Long-term Recommendations:**
    - Strengthen DNS security by implementing query filtering policies to limit unnecessary and potentially malicious queries from internal hosts.
    - Deploy real-time DNS traffic monitoring with alerting for abnormal patterns, such as frequent NXDOMAIN responses or excessive traffic to specific external services.
    - Review and update the organization's cloud and DNS usage policies, especially in regard to tunneling services and cloud-based tools like AWS and Google services.
    - Segment internal networks more strictly to contain broadcast traffic and reduce the likelihood of lateral movement or scanning.

Lessons Learned

- **DNS Log Analysis as a Proactive Measure:** Routine analysis of DNS logs is essential for detecting anomalies like excessive NXDOMAIN responses or unusual queries to external services. Early detection of these anomalies can help identify potential threats or misconfigurations.
- **Field Extraction Enhances Efficiency:** Using Splunk's field extraction capabilities, such as isolating destination IPs (dst_ip), greatly improves the efficiency of investigations by allowing analysts to focus on specific patterns and behaviors.
- **Importance of Real-time Monitoring:** DNS traffic monitoring and real-time alerts for abnormal query patterns can provide crucial insights into potential malicious activity, allowing for quicker response times and mitigating the impact of any threats.

Report Status: Investigation Active
Next Review: 24 Hours
Distribution: SOC Team, Network Security Team, IT Management
Attachments:

- Full query logs
- VirusTotal reports
- WHOIS records