ultraviolet

CONFIDENTIAL

THREAT REPORT:

Leveraging DNS tunneling to Track and Scan Targets

Services Performed By:
UltraViolet Cyber
Omar Silva
(915)234-0541
info@uvcyber.com

Published Date:
05/29/2024

Contents

1 Executive Summary

In a constantly evolving digital landscape, adversaries are continuously devising new tactics and techniques to bypass security measures and compromise victim networks. A known documented method threat actors have been observed leveraging is DNS tunneling to establish stealthy and resilient communication channels, facilitating malicious activities such as data exfiltration to a C2 server. A recent case study performed by Palo Alto Unit 42 revealed that threat actors have now begun leveraging DNS tunnelling in the initial phases of an attack for scanning campaign efficiency and tracking a victim's network. This data is based upon three distinct DNS tunneling campaigns which utilize unique methods to gather intel while still evading detection. (Wang et al., 2024[i])

2 Technical Analysis

Leveraging DNS tunneling can be effective against a target network due to its ability to exploit the inherent trust and ubiquity of DNS traffic, evade traditional security measures, and blend in with legitimate traffic to operate stealthily. Data gathered by PA Unit 42 provides further insight on how threat actors are now utilizing DNS tunneling to scan network infrastructure and track victim activities, helpful in facilitating attacks. One identified campaign nicknamed "TrkCdn," focuses on tracking victim interactions with phishing email content. According to Unit 42, this campaign targeted 731 potential victims using 75 IP addresses for nameservers and resolving 658 attacker-controlled domains. Through encoded subdomains, threat actors monitor when targets open phishing emails, enabling them to refine their strategies and deliver malicious payloads effectively. "In this application of DNS tunneling, an attacker's malware embeds information on a specific user and that user's actions into a unique subdomain of a DNS query," the researchers explained. "This subdomain is the tunneling payload, and the DNS query for the FQDN (Fully Qualified Domain Name) uses an attacker-controlled domain".[1] For

[1] Wang, S., Duan, R., & Liu, D. (2024b, May 13). Leveraging DNS tunneling for tracking and scanning. *Unit 42*. https://unit42.paloaltonetworks.com/three-dns-tunneling-

tracking purposes, attackers can then query DNS logs from their authoritative nameservers and compare the payload with the hash values of the email addresses to monitor campaign performance. Similarly, a campaign nicknamed "SpamTracker" utilizes a tracking mechanism in a comparable manner to "TrkCdn" by leveraging DNS tunneling to track spam delivery. The intent being to lure victims to click on the links behind which threat actors have concealed their payload in the subdomains.

The final campaign identified as "SecShow", utilizes DNS tunneling to perform reconnaissance on a network infrastructure. By embedding IP addresses and timestamps into DNS queries, adversaries can map network configurations and identify exploitable weaknesses. This campaign generally targets open resolvers thus victims mainly come from education, high tech and government fields, where open resolvers are commonly found. This can be useful for threat actors in the initial phases of an attack as they can acquire useful information about the network while remaining undetected. Adversaries within this specific campaign typically perform reflective attacks which is a technique that leverages DNS to spoof source IP addresses and send forged queries to DNS servers. This technique allows them to identify vulnerabilities and can be the first step for DNS spoofing, DNS cache poisoning or DNS amplification attacks.

3 What UltraViolet Cyber is Doing

- UltraViolet Cyber regularly updates our IOC database to ensure alerting is up to date
- Monitoring commands that are associated with malicious activity from threat actors
- Closely monitoring anomalies within network logs to detect malicious DNS behavior

4 What Customers Can Do

- Unit 42 researchers recommend that organizations control the service range of resolvers to accept necessary queries only and promptly update the resolver software version to prevent N-day vulnerabilities
- Keep systems, software, and network devices patched and updated
- Blocking or limiting unnecessary DNS queries can help reduce the attack surface for DNS tunneling

campaigns/#:~:text=In%20scanning%2C%20adversaries%20employ%20DNS,Content%20Delivery%20Networks%20(CDN).

5 References

[1] Liu, S. W., Ruian Duan, Daiping. (2024, May 13). Leveraging DNS Tunneling for Tracking and Scanning. Unit 42. https://unit42.paloaltonetworks.com/three-dns-tunneling-campaigns/?web_view=true

Muncaster, P. (2024, May 14). Hackers Use DNS Tunneling to Scan and Track. Infosecurity Magazine. https://www.infosecurity-magazine.com/news/dns-tunneling-scan-track-victims/

Application Layer Protocol: DNS, Sub-technique T1071.004 - Enterprise | MITRE ATT&CK®. (n.d.). Attack.mitre.org. https://attack.mitre.org/techniques/T1071/004/

---

[i] Wang, S., Duan, R., & Liu, D. (2024, May 13). Leveraging DNS tunneling for tracking and scanning. *Unit 42*. https://unit42.paloaltonetworks.com/three-dns-tunneling-campaigns/#:~:text=In%20scanning%2C%20adversaries%20employ%20DNS,Content%20Delivery%20Networks%20(CDN).