China-Linked 'Muddling Meerkat' Hijacks DNS to Map Internet on Global Scale

Date: 30th April 2024 | Severity: High

Summary

A previously undocumented cyber threat dubbed Muddling Meerkat has been observed undertaking sophisticated domain name system (DNS) activities in a likely effort to evade security measures and conduct reconnaissance of networks across the world since October 2019. Cloud security firm Infoblox described the threat actor as likely affiliated with the People's Republic of China (PRC) with the ability to control the Great Firewall (GFW), which censors access to foreign websites and manipulates internet traffic to and from the country. The moniker is reference to the "bewildering" nature of their operations and the actor's abuse of DNS open resolvers – which are DNS servers that accept recursive queries from all IP addresses – to send the queries from the Chinese IP space.

Attack Vectors

Muddling Meerkat conducts active operations through DNS by creating large volumes of widely distributed queries that are subsequently propagated through the internet using open DNS resolvers. Their operations intertwine with two topics tightly connected with China and Chinese actors: the Chinese Great Firewall (GFW) and Slow Drip, or random prefix, distributed denial-of-service (DDoS) attacks.

The target domains are the domain used in the queries, so it is not necessarily the target of an attack. It is the domain used to carry out the probe attack. These domains are not owned by Muddling Meerkat.

Indicator of compromise

INDICATOR TYPE	INDICATORS		
Domain	• pq5bo[.]kb[.]com • uff0h[.]kb[.]com • biuti[.]kb[.]com • 8jxg1x[.]kb[.]com • 8p0[.]kb[.]com • 4u[.]com • kb[.]com • oao[.]com • od[.]com • boxi[.]com • zc[.]com	• s8[.]com • f4[.]com • b6[.]com • p3z[.]com • ob[.]com • eg[.]com • kok[.]com • gogo[.]com • aoa[.]com • q29[.]org	• gogo[.]com • zbo6[.]com • id[.]com • mv[.]com • nef[.]com • ntl[.]com • tv[.]com • 7ee[.]com • gb[.]com • tunk[.]org

IP addresses	• 0183[.]136[.]225[.]45 • 183[.]136[.]225[.]14

Recommendation

- Actively seek out and eliminate open resolvers in their networks.
- Do not use domains that you do not own for Active Directory or DNS search domains.
- Incorporate DNS detection and response (DNSDR) into your security stack.
- Report Muddling Meerkat activity to the community.

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Links

- https://thehackernews.com/2024/04/china-linked-muddling-meerkat-hijacks.html
- https://blogs.infoblox.com/threat-intelligence/a-cunning-operator-muddling-meerkat-and-chinas-great-firewall/