Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ACTOR REPORT

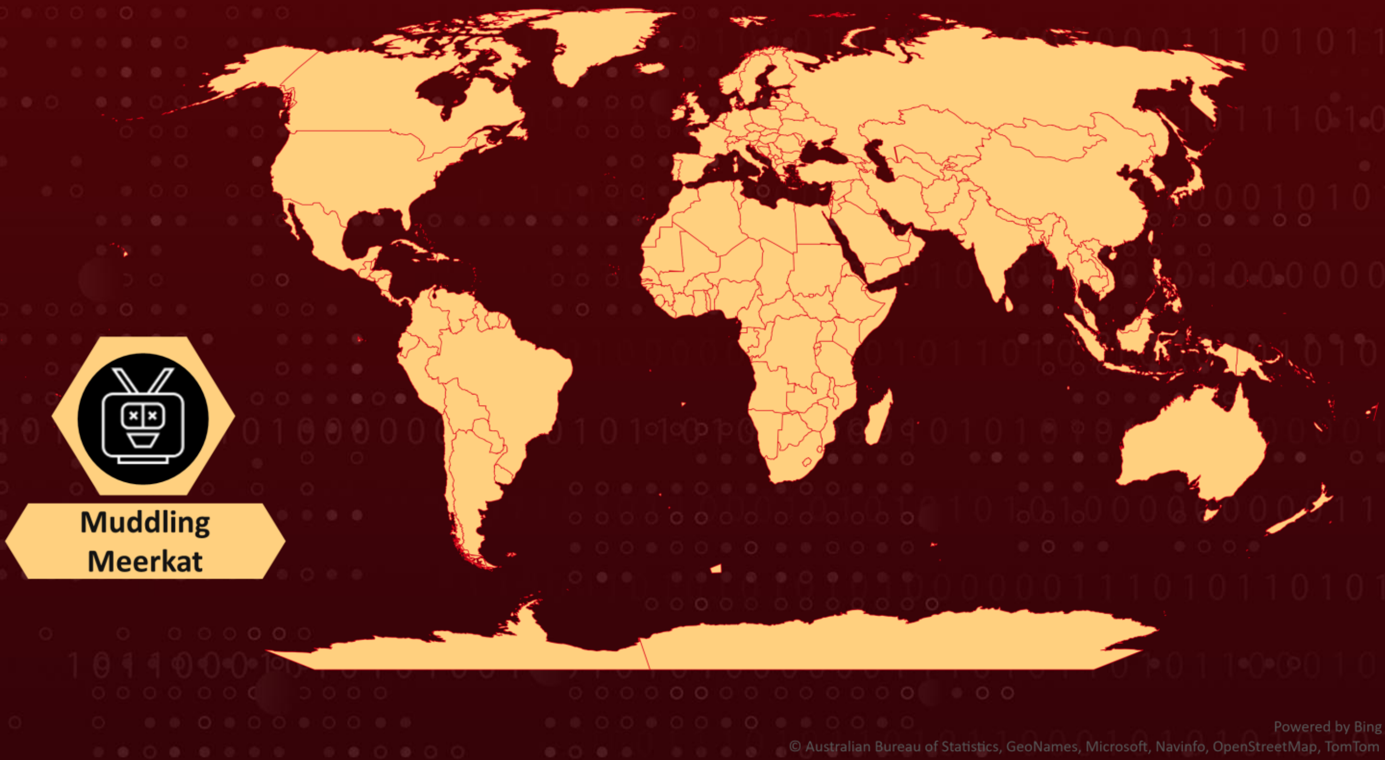
The Enigmatic 'Muddling Meerkat' Poses a Nation-State DNS Puzzle

Date of Publication	Admiralty code	TA Number
April 30, 2024	A1	TA2024168

Summary

First Appearance: October 2019
Threat Actor: Muddling Meerkat
Target Industries: All
Target Region: Worldwide

Actor Map


Muddling Meerkat
Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Actor Details

#1 Muddling Meerkat, an entity associated with the People's Republic of China, has been identified for its sophisticated operations involving DNS manipulation and Slow Drip DDoS attacks. These activities, closely linked with the Chinese Great Firewall (GFW), demonstrate a high level of proficiency in DNS dynamics and manipulation techniques.

#2 Operating since at least October 2019, Muddling Meerkat exerts control over the GFW to conduct various campaigns. These campaigns involve generating substantial query volumes through open DNS resolvers, injecting false MX records from Chinese IP addresses, and utilizing "super-aged" domains to evade detection. The operations typically span one to three days and may involve discrete components, resulting in varied DNS patterns over time.

#3 Muddling Meerkat employs three main types of activities: querying MX records of a target domain, querying MX records of random hostnames, and querying A records of random hostnames. These queries, characterized by the use of short hostnames and the prevalence of A records for IPv4 addresses, distinguish Muddling Meerkat's tactics from other Slow Drip attacks.

#4 The Global Firewall (GFW) plays a pivotal role in Muddling Meerkat's operations, injecting false responses to DNS queries originating from specific data collections. These false responses, originating from Chinese IP addresses, aim to impede analysis efforts and cause confusion. The GFW can inject responses without noticeable performance impacts, providing false answers instead of commonly expected responses.

#5 Muddling Meerkat's operations involve querying MX records for random subdomains of target domains, a departure from typical DNS attack patterns. The volume of MX queries remains consistent across multiple target domains, resembling Slow Drip DDoS attacks but with significantly lower volumes.

#6 These operations disrupt the internet by dispatching DNS queries to various destination IP addresses, including open resolvers within Chinese IP space. The involvement of the GFW and collaboration with operators indicate a coordinated effort to manipulate DNS responses for specific domains, although the motives behind these operations remain unclear. Muddling Meerkat's activities highlight the evolving of cyber threats and the intricate methods employed by state-sponsored actors to achieve their objectives.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
Muddling Meerkat	China	All	All
	MOTIVE		
	-		

Recommendations

Deploy DNS Monitoring Tools: Invest in DNS monitoring tools or platforms that provide real-time visibility into DNS traffic across your network. These tools should be capable of analyzing DNS queries and responses, identifying anomalies, and flagging suspicious activities.

Enable Logging and Analysis: Ensure that DNS servers and monitoring tools are configured to log DNS queries and responses for analysis. Analyzing DNS logs can help identify patterns of malicious activity and provide valuable insights into potential threats.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0043 Reconnaissance	TA0040 Impact	T1594 Search Victim-Owned Websites
T1584 Compromise Infrastructure	T1584.002 DNS Server	T1584.003 Virtual Private Server	T1584.001 Domains
T1584.005 Botnet	T1595 Active Scanning	T1595.002 Vulnerability Scanning	T1596 Search Open Technical Databases
T1593 Search Open Websites/Domains	T1498 Network Denial of Service		

Indicator of Compromise (IOCs)

TYPE	VALUE
Domain	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, gogo[.]com, zbo6[.]com, id[.]com, mv[.]com, nef[.]com, ntl[.]com, tv[.]com, 7ee[.]com, gb[.]com, tunk[.]org, q29[.]org
IPv4	183[.]136[.]225[.]45, 183[.]136[.]225[.]14

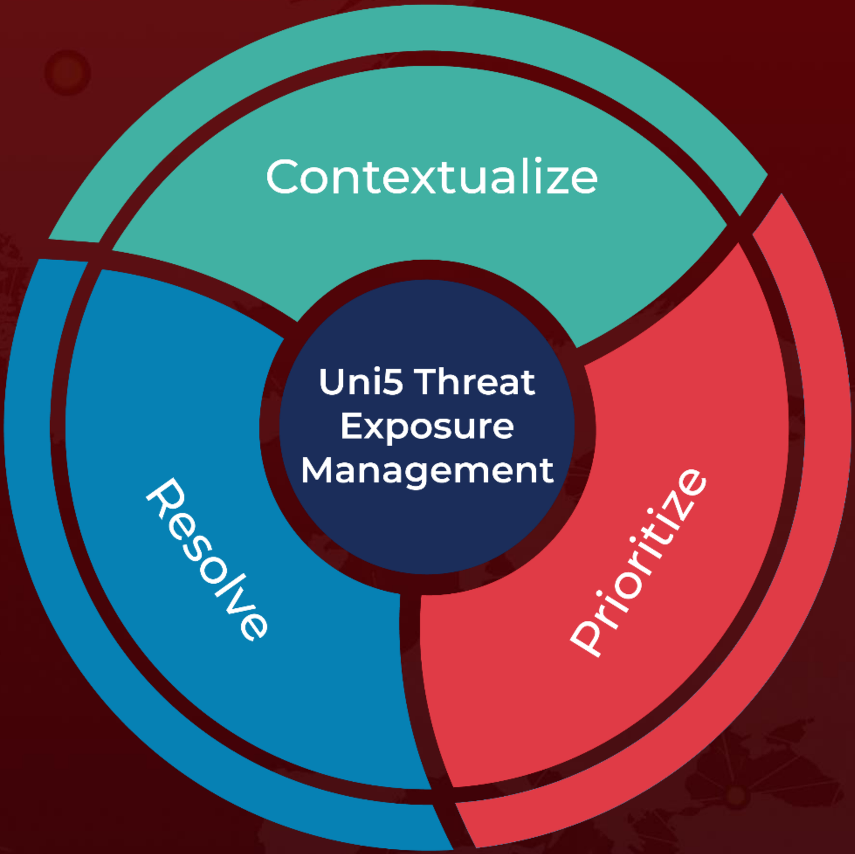
References

https://insights.infoblox.com/resources-report/infoblox-report-muddling-meerkat-the-great-firewall-manipulator?

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

April 30, 2024 • 7:30 AM

© 2024 All Rights are Reserved by HivePro

More at www.hivepro.com