Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

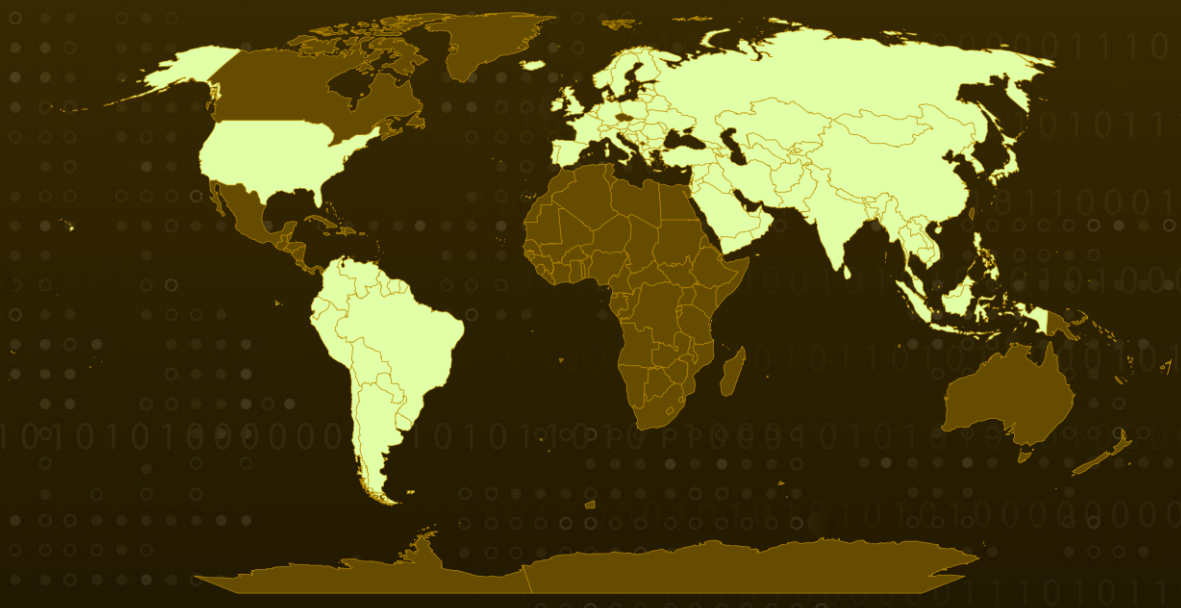
Unmasking Decoy Dog Malware Toolkit Hiding in DNS Traffic

Date of Publication	Admiralty Code	TA Number
July 27, 2023	A1	TA2023316

Summary

First appeared: April 2022
Attack Region: Worldwide
Malware: Decoy Dog, Pupy RAT
Targeted Regions: U.S., Europe, South America, and Asia
Targeted Industries: Technology, Healthcare, Energy, Financial
Attack: Decoy Dog, a sophisticated malware toolkit uses DNS for C2 communication, evading detection with its wildcard-type behavior and encryption methods. Its origin remains mysterious, and the malware's capabilities surpass traditional RATs like Pupy, making it highly elusive.

Attack Regions



Attack Details

#1

In April 2023, a sophisticated malware toolkit called Decoy Dog was discovered, using the domain name system (DNS) for command and control (C2) communication. Unlike conventional malware, Decoy Dog's C2 operations rely on DNS traffic, making it highly elusive and challenging to detect.

#2

Initially based on the Pupy open-source remote access trojan (RAT), Decoy Dog exhibits a level of sophistication beyond its predecessor. While Pupy is commonly used by penetration testers, Decoy Dog's capabilities go far beyond those of a typical RAT.

#3

Decoy Dog's behavior has raised serious concerns among security experts. The malware responds to all well-formed DNS requests, exhibiting a wildcard-type behavior that is unusual among most malware, which often tries to avoid detection. This deliberate and sophisticated approach has allowed Decoy Dog to evade identification and remain concealed for extended periods.

#4

The motives behind Decoy Dog's development remain unclear, as no specific victims have been identified. The malware has been traced to at least three different threat actors, adding to the mystery surrounding its purpose and potential targets.

#5

The malware's behavior also indicates a level of sophistication and intentionality that raises concerns about the motives behind its development. In a surprising twist, Decoy Dog responds to all well-formed requests, creating a DNS wildcard-type behavior, which goes against common malware evasion practices. This unique characteristic, among others, has allowed Decoy Dog to stay under the radar and operate undetected for extended periods.

#6

Due to its encryption methods, understanding the specific data being communicated by Decoy Dog has proven challenging. Nonetheless, researchers have been able to identify the types of messages sent and profile the overall communication behavior of the malware.

Recommendations

DNS Traffic Analysis: Invest in advanced DNS traffic analysis tools and systems that can monitor and detect anomalous DNS activities. Look for sudden spikes in DNS queries, unusual patterns, or wildcard-type responses, which may indicate the presence of Decoy Dog. Implementing robust DNS detection and response mechanisms can help identify and block malicious communications, mitigating the impact of the malware.

Network Segmentation: Implement proper network segmentation to limit the lateral movement of malware within the network. By dividing the network into smaller, isolated segments, organizations can contain the spread of Decoy Dog and prevent it from accessing critical systems and sensitive data. This segmentation also helps in isolating infected devices, allowing for more effective incident response and containment.

Robust Endpoint Security: Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place. A multi-layered approach to endpoint security can prevent malware like Decoy Dog from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

Potential MITRE ATT&CK TTPs

TA0010 Exfiltration	TA0011 Command and Control	TA0042 Resource Development	TA0043 Reconnaissance
TA0003 Persistence	TA0002 Execution	T1041 Exfiltration Over C2 Channel	T1583 Acquire Infrastructure
T1583.001 Domains	T1048 Exfiltration Over Alternative Protocol	T1001 Data Obfuscation	T1071.004 DNS
T1071 Application Layer Protocol	T1573 Encrypted Channel	T1203 Exploitation for Client Execution	T1573.002 Asymmetric Cryptography

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	ads-tm-glb[.]click, allowlisted[.]net, atlas-upd[.]com, cbox4[.]ignorelist[.]com, claudfront[.]net, hsdps[.]cc, j2update[.]cc, maxpatrol[.]net, nsdps[.]cc, rcmsf100[.]net
IPV4	13[.]248[.]169[.]48, 156[.]154[.]132[.]200, 194[.]31[.]55[.]85, 5[.]199[.]173[.]4, 5[.]252[.]176[.]63, 5[.]252[.]176[.]22, 5[.]252[.]179[.]18, 67[.]220[.]81[.]190, 69[.]65[.]50[.]194, 69[.]65[.]50[.]223, 70[.]39[.]97[.]253, 83[.]166[.]240[.]52
SHA256	4996180b2fa1045aab5d36f46983e91dadeebfd4f765d69fa50eba4edf310acf, ab8e333ef9bc5c5a7d1ed4cab08335861e150b0639d3d0ca4c30b7def5cdccde, ad186df91282cf78394ef3bd60f04d859bcacccbcdcbfb620cc73f19ec0cec64, 6c8f413111f1abfee788dad4ee7cca37e0c2597cca66d155af958c535faf55cc, 0375f4b3fe011b35e6575133539441009d015ebecbee78b578c3ed04e0f22568, 6c8f413111f1abfee788dad4ee7cca37e0c2597cca66d155af958c535faf55cc
Telfhash	t1fde0f101c9395f39ecd16430b41041a59107c73c904087309fb8d0e8d87e0077129f3f

References

https://insights.infoblox.com/resources-whitepaper/infoblox-whitepaper-decoy-dog-is-no-ordinary-pupy-distinguishing-malware-via-dns

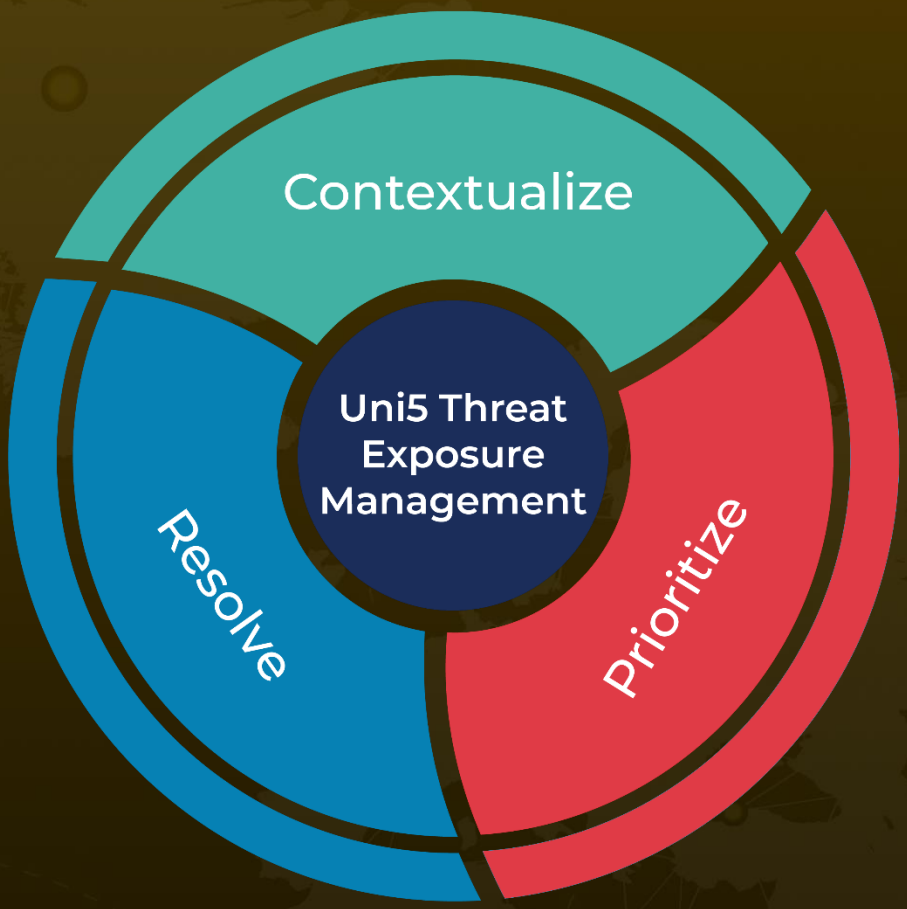
https://blogs.infoblox.com/cyber-threat-intelligence/decoy-dog-is-no-ordinary-pupy-distinguishing-malware-via-dns/

https://www.infoblox.com/company/news-events/press-releases/infoblox-uncovers-dns-malware-toolkit-urges-companies-to-block-malicious-domains/

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

July 27, 2023 • 5:30 AM

More at www.hivepro.com