PLIXER

WHITE PAPER

Understanding and Navigating the "Decoy Dog" Exploit.

DECOY DOG

Watch out for this DNS attack

In the rapidly evolving cyber threat landscape, the "Decoy Dog" exploit has emerged as a significant concern. This, coupled with the recent EfficientIP and IDC Global DNS Threat Report, highlights a broader vulnerability: in 2020, 79% of organizations faced DNS attacks, with the average cost per attack nearing USD $924,000.

The shift to cloud-based DNS, though designed to improve flexibility and user experience, has inadvertently increased security threats, with 50% of companies reporting cloud service downtimes—a 22% rise from 2019. (1)(2)

North America remains particularly vulnerable, with the average DNS attack cost pegged at USD 1,073,000. However, there's a silver lining: a growing number of organizations are recognizing the importance of DNS security.

But the challenge persists, as many still undervalue its significance, underscoring an urgent need for prioritizing DNS security measures to fortify their cyber security stance.

While specific technical details remain under exploration, understanding its potential impact, propagation methods, and mitigation strategies is crucial. This paper aims to shed light on the key elements of the "Decoy Dog" exploit, emphasizing its significance by highlighting its potential impacts on companies: substantial financial losses due to compromised data, erosion of customer trust in brand integrity, and potential regulatory repercussions with associated legal costs.

NATURE OF THE EXPLOIT

Decoy Dog was initially discovered in April 2023 and is suspected to be used in ongoing nation-state cyber attacks. Decoy Dog is a malware toolkit that uses the domain name system (DNS) for command-and-control (C2) operations. Decoy Dog responds to replays of previous DNS queries and wildcard DNS requests, which doubles the number of resolutions seen in passive DNS.

While the complete mechanics of "Decoy Dog" are under investigation, it is essential to comprehend:

- The cyber threat actor, Decoy Dog, has showcased a sophisticated approach to malware propagation by harnessing the advanced capabilities of the Pupy Remote Access Tool (RAT).

- Pupy, recognized for its ability to operate entirely in-memory and utilize encrypted DNS for covert communications, serves as a powerful tool in Decoy Dog's arsenal.

- Domains like claudfront[.]net, atlas-upd[.]com, and cbox4[.]ignorelist[.]com have been identified as part of their communication infrastructure, aiding in masking their activities.

• Using Pupy's features like reflective DLL injection, Decoy Dog can seamlessly inject malicious payloads without leaving traces on the disk.

• Additionally, the strategic use of nonces and Security Parameter Indexes (SPIs) in Pupy ensures that the malware's communications are not just covert, but also secure.

• Leveraging these combined strengths, Decoy Dog may further exploit software vulnerabilities or employ phishing techniques to spread their malware, while domains like the aforementioned ones assist in maintaining a steady and clandestine connection to compromised systems.

PROPAGATION METHOD

Based on the information provided, the malware toolkit named "Decoy Dog" represents a sophisticated cyber security threat targeting enterprise networks globally. Its propagation method centers around its command-and-control (C2) capabilities, which are linked to a Russian IP address. This toolkit uses the DNS (Domain Name System) as its C2 channel, enabling the malicious actors to gain control over internal devices within an organization. The insidious nature of this toolkit is emphasized by the fact that its C2 communications are hard to detect, especially since they involve only a minute amount of data queries within vast pools of DNS data.

When such communications are viewed in isolation, they are extremely challenging to identify. However, complete visibility is the key; leveraging conversation metadata like NetFlow and IPFIX along with DNS integration and intelligence is vital to pinpointing such covert activities. The RAT, which is based on an open-source project named Pupy, has remained active and undetected since April 2022.

This has allowed it to embed itself within the DNS infrastructure and continue its operations for an entire year before detection.

MITIGATION STRATEGIES

To safeguard against the threats presented by Decoy Dog, organizations should adopt a multifaceted mitigation approach. This includes:

• First and foremost, a robust endpoint detection solution is essential. This system should be primed to recognize and neutralize Pupy-related executables, which are Decoy Dog's primary payloads. By leveraging known indicators of compromise, it can swiftly isolate affected systems and prevent further infiltration.

• Additionally, enhancing user awareness is vital. Regular training sessions can educate staff on the nuances of phishing and spear-phishing campaigns, which are frequently used by advanced threats like Decoy Dog. Ensuring that users can swiftly identify and report potential threats significantly narrows the window of vulnerability.

• Finally, deploying a Network Detection and Response (NDR) tool that ingests and analyzes network-wide conversations is crucial. When enhanced with DNS transactional information, such tools can pinpoint anomalies or suspicious domain query patterns, enabling timely detection of C2 communications or DNS tunneling attempts associated with Decoy Dog.

CONCLUSION

The cybersecurity landscape is constantly shifting, wi th advanced threats like Decoy Dog demonstrating the evolving nature of cyber risks. Utilizing DNS-based techniques, Decoy Dog's propagation method takes advantage of vulnerabilities, particularly in the increasingly adopted cloud-based DNS systems. This is even more concerning when considering that cyberattacks on DNS servers are on the rise, with nearly 79% of organizations experiencing DNS attacks in 2020.

Command and control (C2) attacks represent one of the most insidious threats in the cyber security landscape, and recent developments have only intensified concerns. A notable example is the emergence of malware like Decoy Dog, which, through its ingenious utilization of DNS-based techniques, underscores the vulnerabilities present even in sophisticated defense mechanisms. These DNS-centric methods, particularly when they exploit cloud-based DNS attacks, are a testament to the evolving creativity of cyber adversaries.

The National Institute of Standards and Technology (NIST) provides a comprehensive definition of C2, highlighting its pivotal role in executing the mission of ensuring security. (3) As these systems are crucial for planning, directing, and controlling organizational forces against cyber threats, their compromise can lead to catastrophic outcomes. MITRE ATT&CK® research, for instance, delineates 16 potent techniques that attackers can employ to this end, ranging from data obfuscation to protocol tunneling. The ramifications of a successful C2 attack are profound. Adversaries can not only siphon off invaluable data but also lay the groundwork for even more devastating attacks, using the compromised system to initiate operations such as DDoS attacks. The Log4j vulnerability stands as a prime example of how attackers can exploit a singular vulnerability to unravel an entire C2 system. Coupled with malware like Decoy Dog, exploiting DNS vulnerabilities, the stakes have never been higher.

Such compromises don't just pose technological challenges—they can lead to financial losses, erode reputation, and result in legal consequences.

The financial toll of such breaches is alarming, with the global average cost of a data breach in 2023 reaching a historic high of $4.45 million. In the U.S., breaches have an even steeper price tag, with an average cost of $9.44 million. As these threats continue to grow, so too does the demand for enhanced visibility and intelligence in cyber security measures. It's imperative for organizations to not only recognize these significant threats but also invest in sophisticated tools and strategies that offer better threat detection and response capabilities. As our dependence on digital infrastructures grows, safeguarding against malware like Decoy Dog and its ilk remains paramount. (4)

SUMMARY

While the technological landscape continually evolves, bringing about new tools like Decoy Dog and revealing vulnerabilities in systems like DNS, the protection of the C2 system remains a paramount concern. Organizations must adopt a holistic security strategy, encompassing both technical and organizational measures, to counter these advanced threats. By fostering a culture of security, staying updated with the latest threat vectors, and instilling the importance of robust security postures, organizations can stand resilient against the ever-looming threat of C2 attacks.

Sources:
(1) Infoblox Threat Intelligence Group. (2023, April 20). Dog Hunt: Finding Decoy Dog Toolkit via Anomalous DNS Traffic. Infoblox Cyber Threat Intelligence.
(2) Teyton, B., & Fouchereau, R. (2023, June). IDC DNS Threat Report 2020. EfficientIP.
(3) NIST. (n.d.). C2. National Institute of Standards and Technology.
(4) Pro Writers. (2023, June). Cost of a Data Breach—Stats Your Clients Should Consider.

ABOUT PLIXER

Plixer gives you visibility and context of every network transaction so you can better understand what's happening in your IT environment. Our 20+ years of network monitoring and management solutions help us provide innovative solutions that help you secure and optimize your digital enterprise. Supercharge your business defense with AI-powered visibility and insight that goes beyond traditional NDR.

sales@plixer.com

plixer.com

68 Main St Ste 4
Kennebunk, ME 04043

PLIXER