

**infoblox**<sup>®</sup>



**Infoblox  
Threat Intel**

# UNCOVER THE HIDDEN CYBER VILLAINS

DNS REVEALS ALL—ARE YOU READY  
TO SEE?



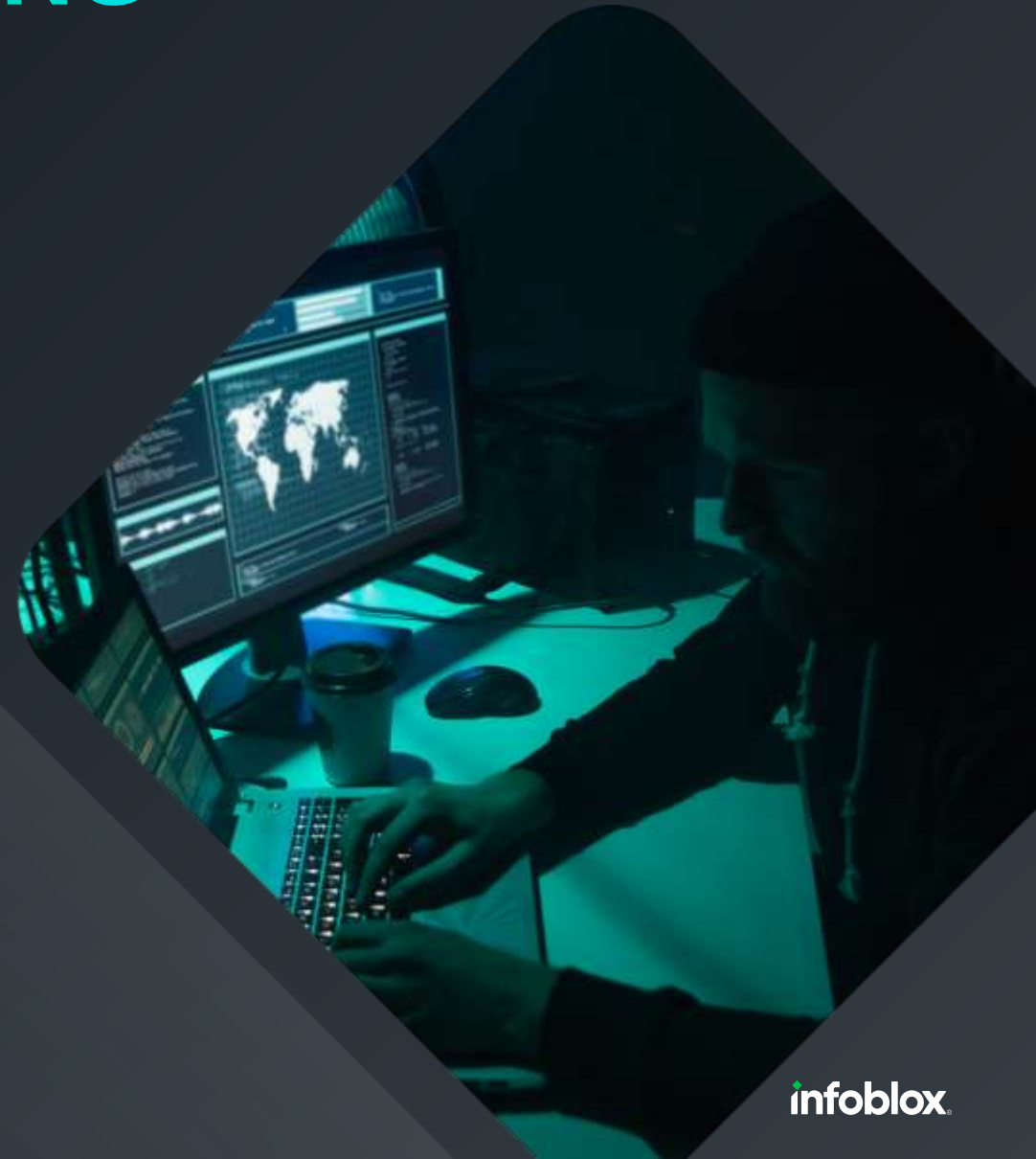
# THREAT LANDSCAPE EVOLVING

- Lookalike domain spear phishing attacks accounted for 66% of data breaches in 2023 (Source: Barracuda)

- DNS is exploited by the vast majority of malware due to insufficient DNS visibility and control

- Industrialization of attacks: Threat Actors register orchestrate attacks from malware infrastructure platforms

- It only takes one DNS query to compromise a network



“

**DNS** is the foundation of the Internet, and securing it is paramount to protecting our digital world.

Cricket Liu, EVP, Chief Evangelist and Senior Fellow

”

# DNS IS THE **BACKBONE** OF EVERY NETWORK

## **YOURS:**

Every Internet connections start with a DNS query

## **THEIRS:**

Threat actors rely on DNS to run malicious campaigns

## **DNS MTTRs**

**92%**

of malicious activity can be blocked using DNS

**60%**

of threats blocked before first DNS query occurs

**82%**

after the first query

Over

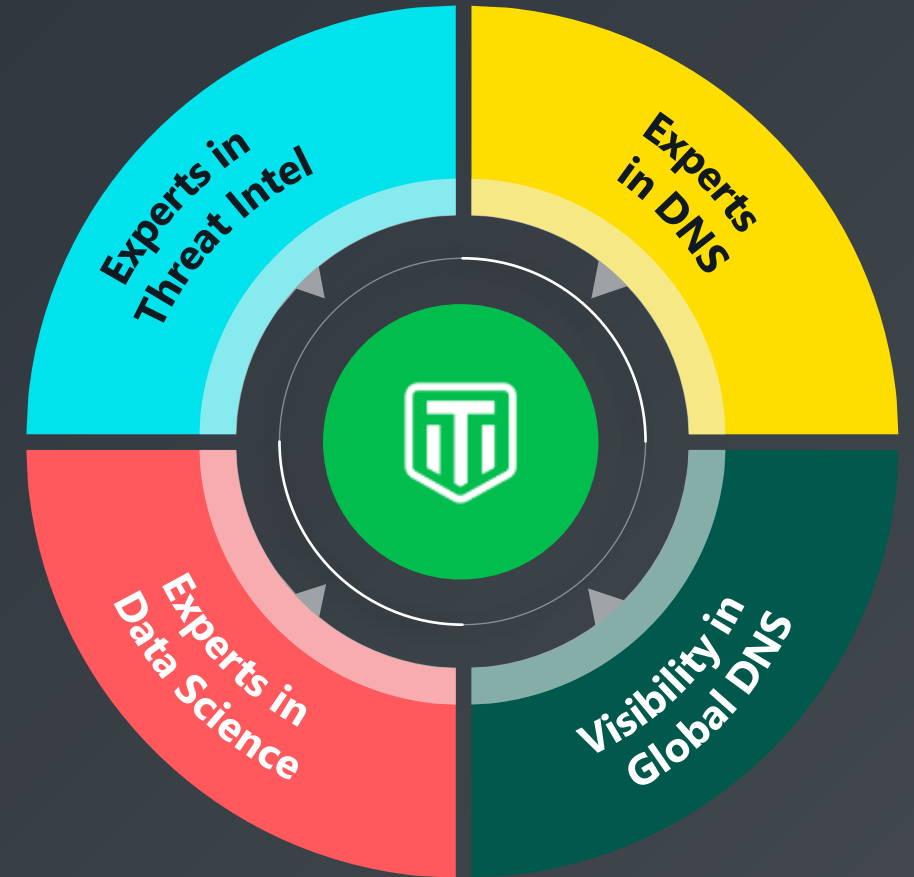
**3.5M**

new malicious and suspicious domains detected monthly

Sources: 1. 92% of malicious domains can be blocked by DNS: Neuberger, A. (2020, June 19). Our analysis highlighted that using secure DNS would reduce the ability for 92% of malware attacks both from command and control perspective, deploying malware on a given network. ExecutiveGov. <https://executivegov.com/2020/06/anne-neuberger-on-nsas-secure-dns-pilot-program/>. 2. TBD Krupa 3. Over 25 million malicious and suspicious domains identified: Renee Burton, Infoblox Threat Intelligence (2023, November 1). Report on the total number of domains identified by Infoblox over a 12-month period.

# WE ARE DOING THE HARD WORK TO UNCOVER ALL THE THREATS

- Unique approach to Threat Intel combines market leading DNS expertise with cutting-edge data science
- Focused on proactively blocking the malware infrastructure the campaigns rely on even before the campaign is even launched
- An Industrial scale solution to an industrial scale problem





**Infoblox  
Threat Intel**



**INFOBLOX  
DISCOVERED**



**DECOY DOG**



**PROLIFIC PUMA**



**SAVVY SEAHORSE**



**VEXTRIO VIPER**



**LOOPY LIZARD**



**MUDDLING MEERKAT**

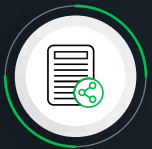
# Vextrio Viper

## Identify and Block Malware Distribution Prior to Discovery



### VexTrio network discovered by Infoblox Spring 2022

- Operating since at least Spring 2021
- Massive maze of dictionary generated domains (DDGA)
- Impacts 50% of enterprises
- Ignored by most vendors as “adware” or “nuisance-ware”
- Leverages anti-detection methods with low profiles
- Impossible to fully observe and protect against outside of DNS



Nozomi Networks published about **IoT Malware** in December 2022 **delivered by VexTrio** – months after Infoblox began blocking

Infoblox **identifies 100% of VexTrio** and other persistent malvertising networks by monitoring DNS.





DECOY DOG



PROLIFIC PUMA



SAVVY SEAHORSE



VEXTRIO VIPER



LOOPY LIZARD



MUDDLING MEERKAT

# What to know more?

---

Let's talk

# Hall 7A-321



ありがとう      köszönjük  
Cảm ơn      धन्यवाद  
terima kasih      gracias  
고마워요      teşekkür ederim  
Σας ευχαριστώ      obrigado  
Спасибо      grazie  
merci      THANK YOU!      谢谢      takk  
ขอบคุณ      شكرا      tack      danke  
bedankt      kiitos

