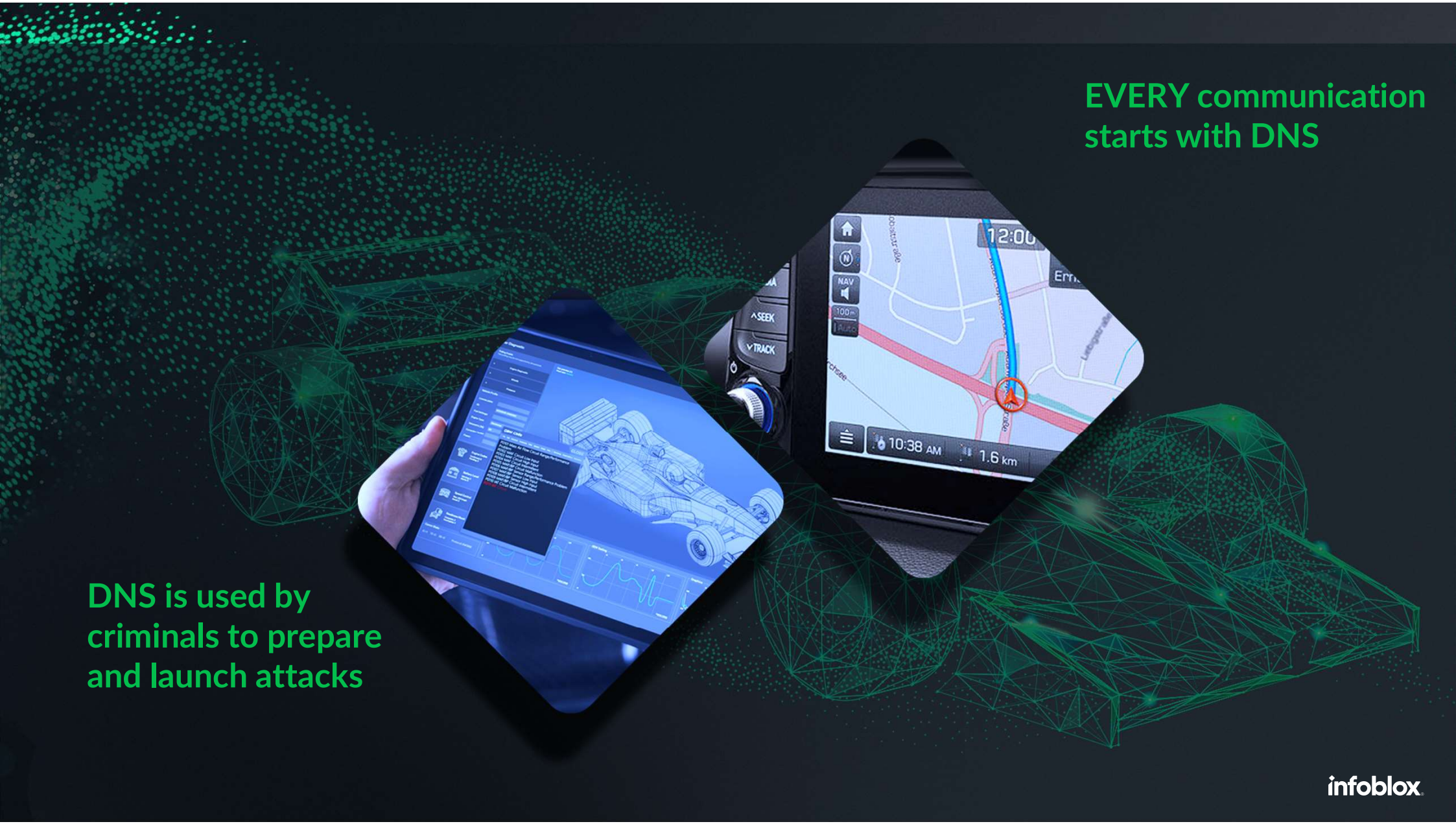
infoblox®

DNS in Zero Trust

"NEVER WALK WITH STRANGERS"

NEVER TALK TO UNTRUSTED DOMAINS


DNS is not just a component
IT'S THE BACKBONE
infoblox


EVERY communication starts with DNS
DNS is used by criminals to prepare and launch attacks
SEEK
TRACK
NAV
10:38 AM
1.6 km
infoblox

What is the Domain Name System doing?

Translating Names (Domains) into Numbers (IP-addresses)

But DNS can do more for you ....

Imagine

Your phone book would not show the numbers of the bad guys and girls ....

Geriet Wendler --> 030 1234567890

Let us order a Pizza

How can the intelligent phonebook DNS help you to order a healthy pizza?

Every communication starts with DNS

Where to find my applications?

Where can I find the phishing site?

Where can I find this service?

Where do I find my C2 Server ?

Where do I find my Data Exfil Endpoint?

Some attacks only work with DNS

Where can I update my Endpoint Security?

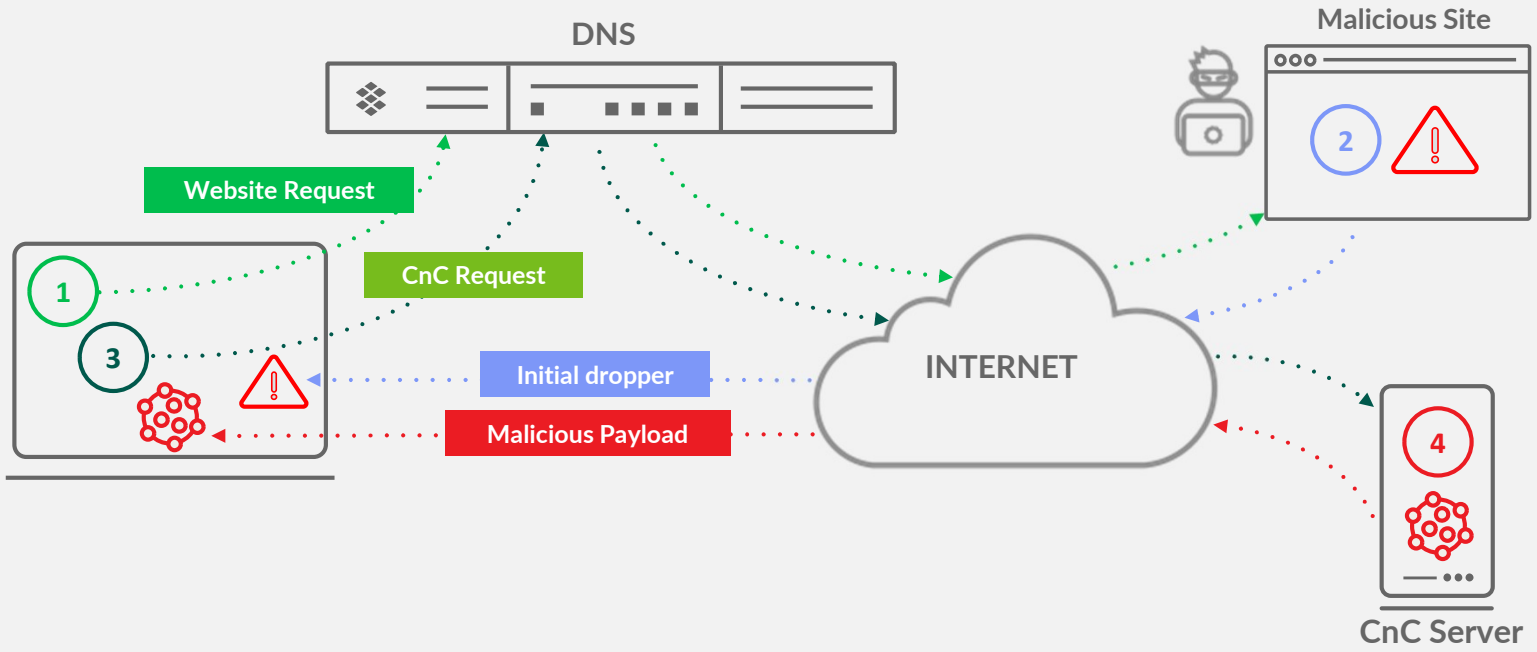
DNS Tunneling

Code Infiltration (e.g. DNS Messenger)

Daten Exfiltration via DNS (with/without Web Proxy)

Typical role of DNS in an attack

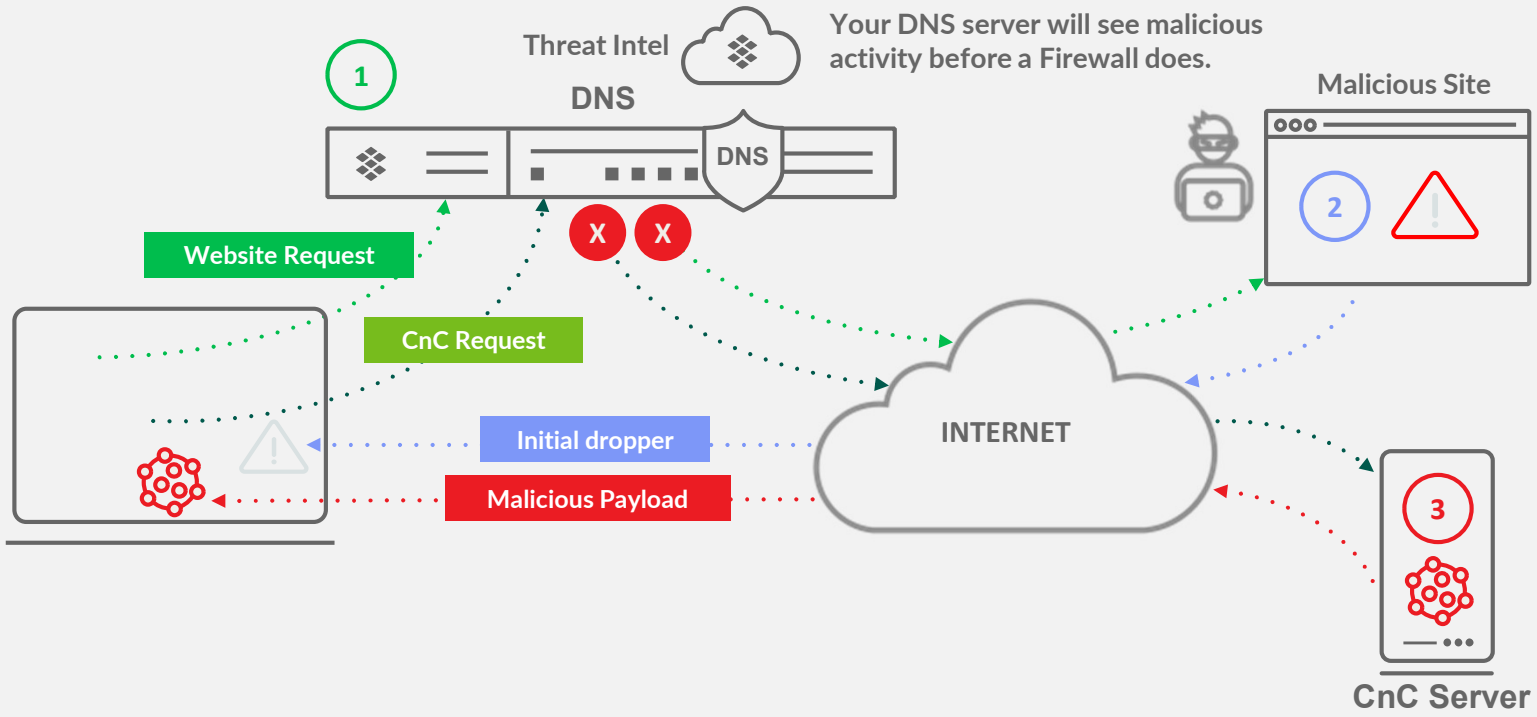
1. User directed to malicious site
2. Website delivers initial exploit
3. Exploit contacts Command and Control (CnC) server
4. Malicious payload downloaded



DNS is used for all outbound traffic requests

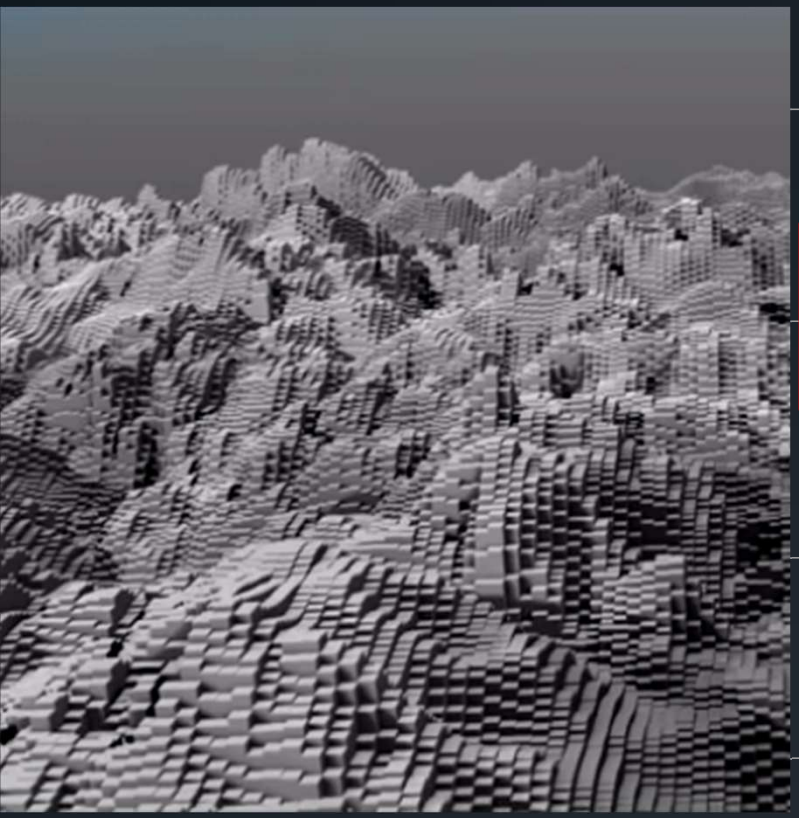
Secure DNS as first line of defense

1. Curated threat intelligence for DNS
2. Connection to malicious website blocked at DNS
3. If already infected, system blocked from connecting to CnC at DNS



Secure DNS breaks the attack chain from the start

Threat Landscape Evolving Rapidly



- Counterfeit domains and persistent malware in smishing bypass defenses
- On an average, 200,000 net domains are created every day
- New top-level domains resemble file extensions (e.g., ZIP, MOV) confusing users
- Researchers flag around 80 million domains as malicious every six months

Sources: * Infoblox * Palo Alto Networks ** Akamai

infoblox

Current XDR Approaches Use Malware Centric Approach

EDR

Monitors end user devices

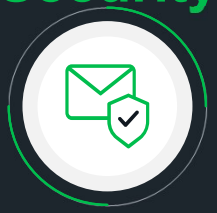
NDR

Monitors communication within the network to detect threats

ITDR

Detects threats to all services and privileged accounts on a company's network

Email Security

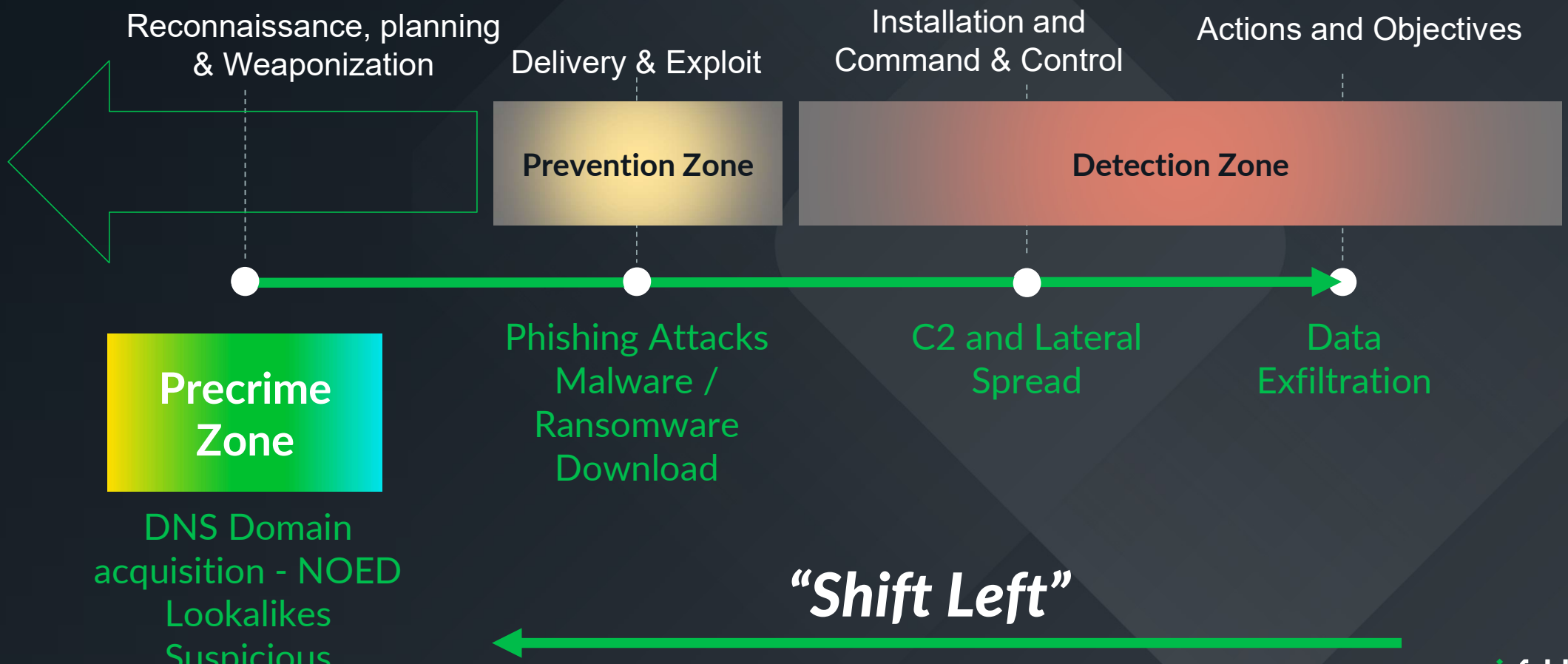


Protects email-based communications

Point solutions, don't track adversary infrastructure, use a malware centric approach

infoblox.

BEHAVIOUR AND DOMAIN EARLY DETECTION, SHIFT LEFT AT CYBER KILL CHAIN

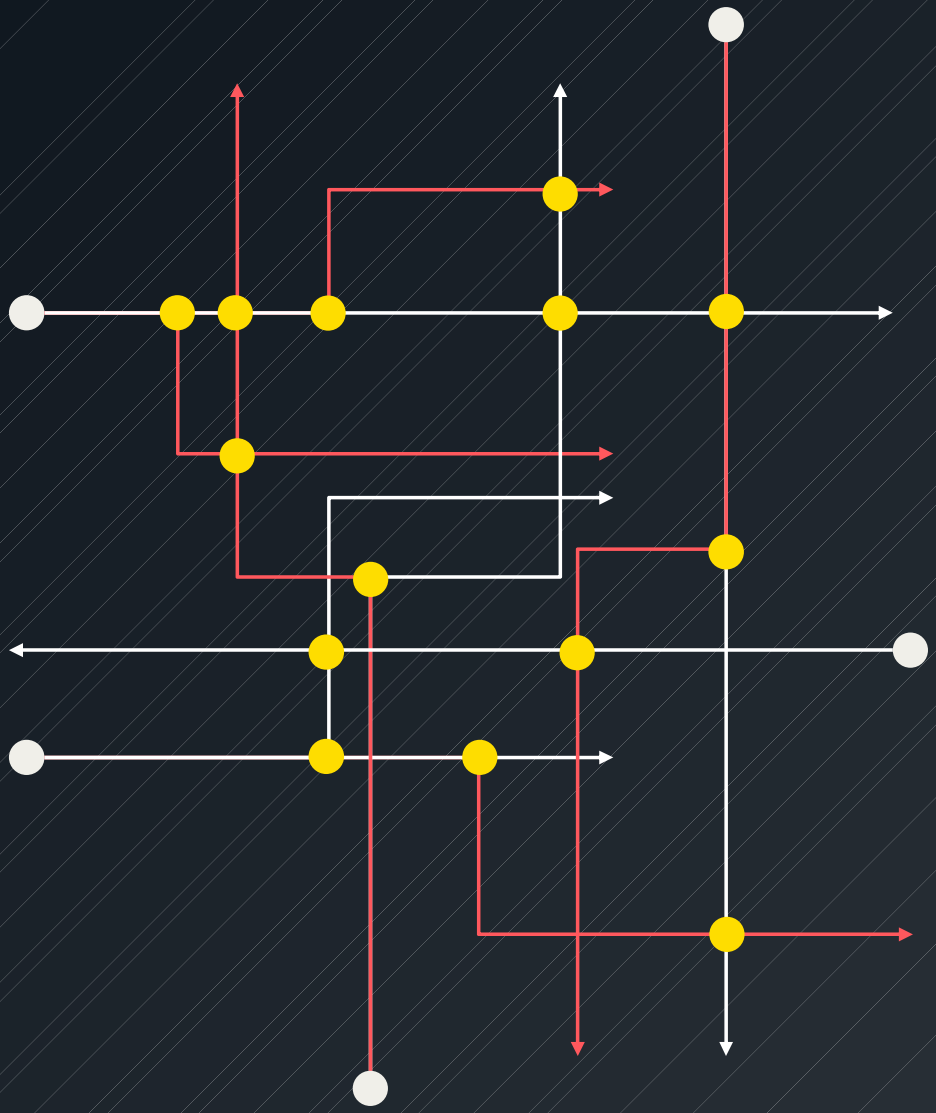


infoblox

infoblox

PROACTIVE DETECTION

WHAT HAPPENS BEFORE THE ZERO DAY



Adversary Infrastructures

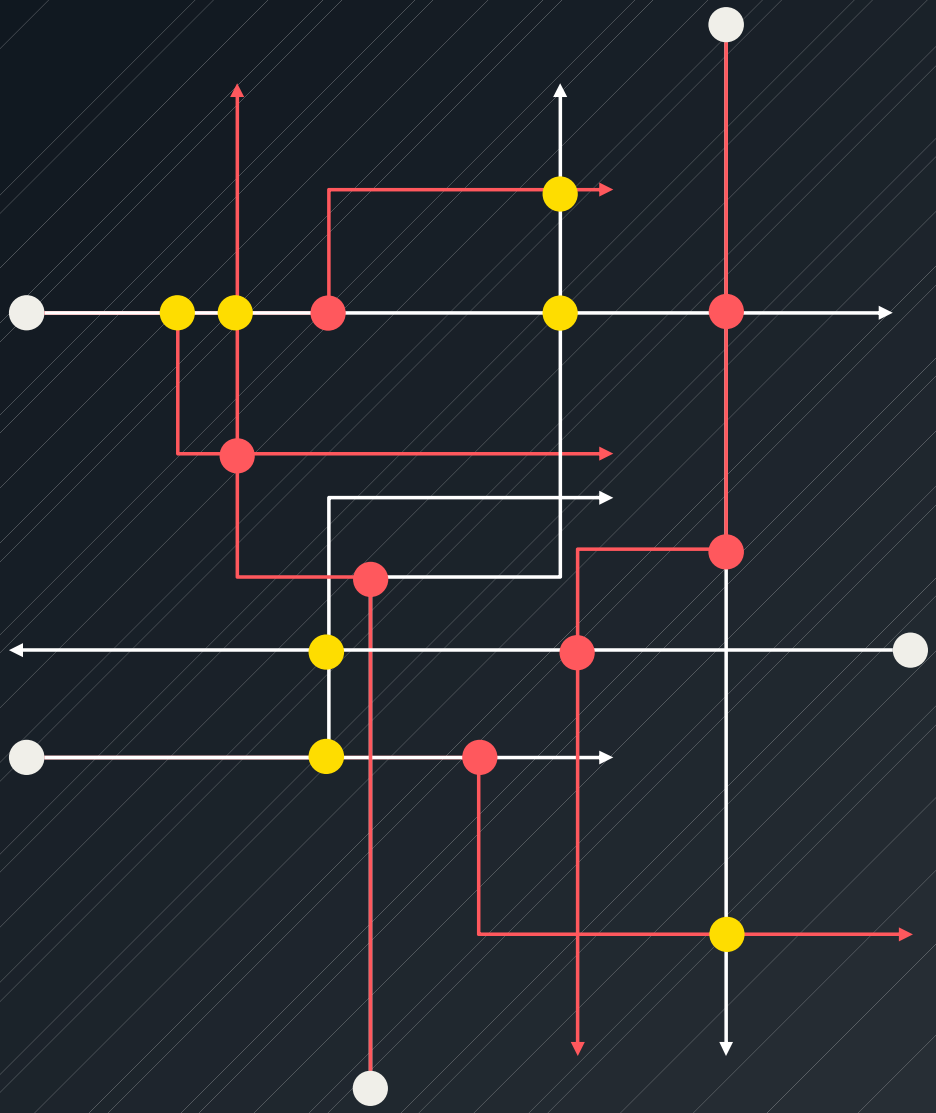
Traffic flows in multiple directions

Malicious traffic flows in the same way

Traffic Distribution Systems are used in both good and malicious traffic

DNS is used and reused in the Distribution Systems

infoblox



Adversary Infrastructures

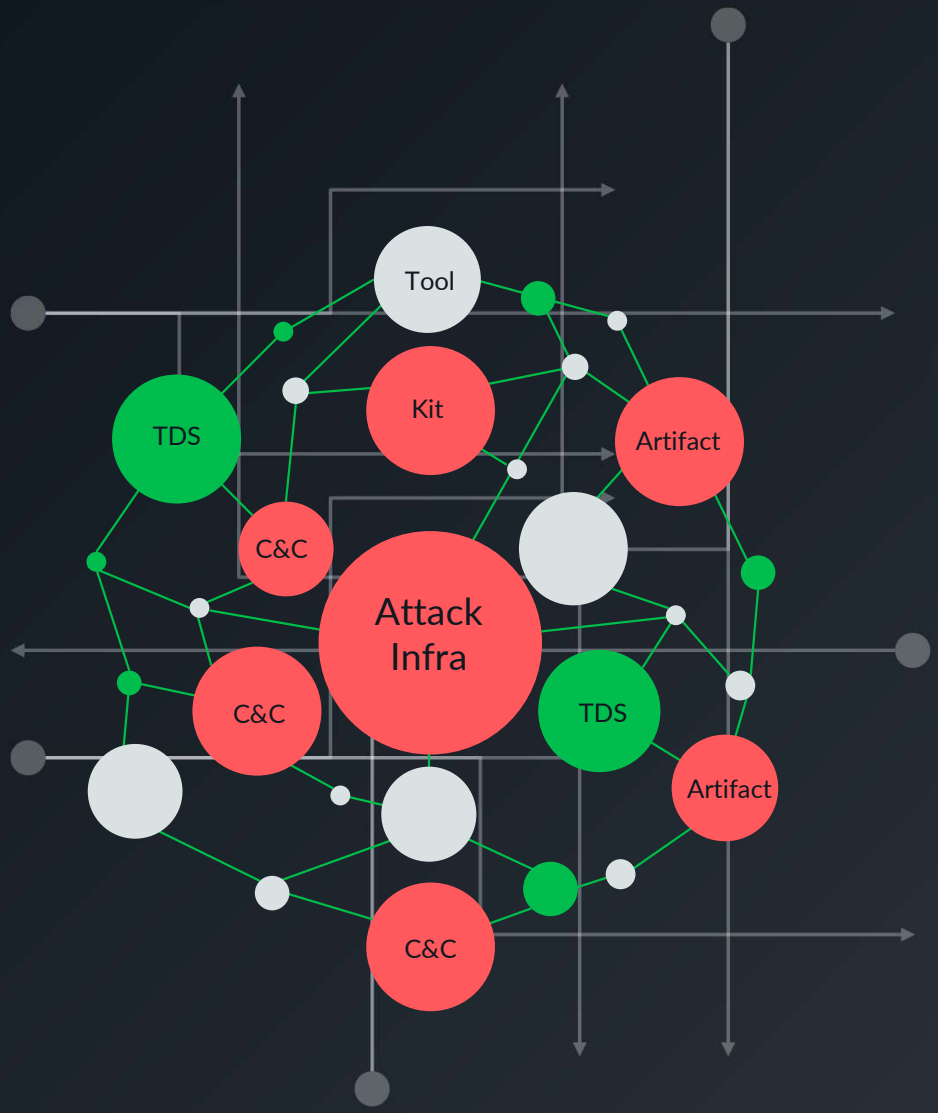
Traffic flows in multiple directions

Malicious traffic flows in the same way

Traffic Distribution Systems are used in both good and malicious traffic

DNS is used and reused in the Distribution Systems

infoblox



Adversary Infrastructures

Traffic flows in multiple directions

Malicious traffic flows in the same way

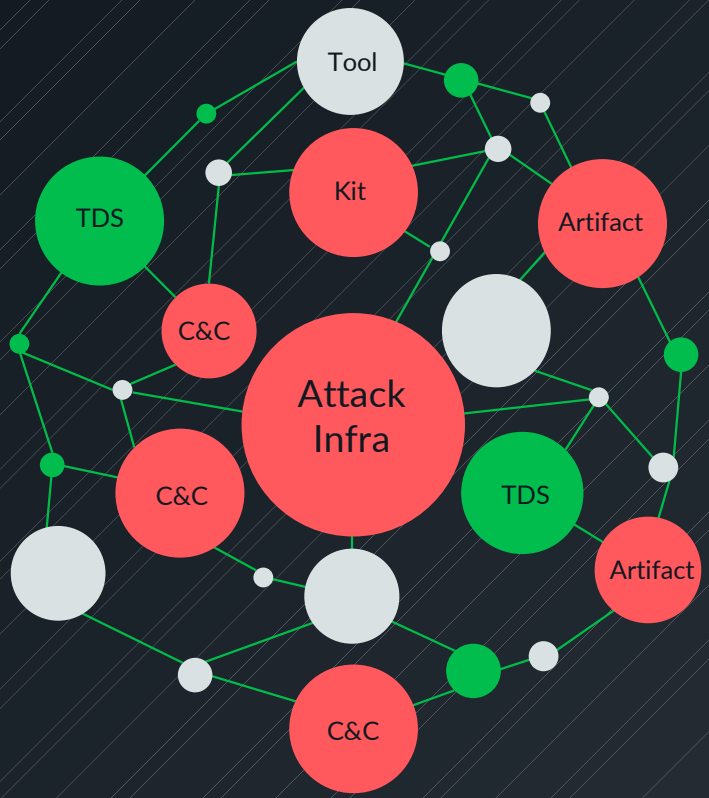
Traffic Distribution Systems are used in both good and malicious traffic

DNS is used and reused in the Distribution Systems

By analyzing massive DNS data we can identify the TDS that are used in different attacks

infoblox

Adversary Infrastructures



Traffic **flows** in multiple directions

Malicious traffic flows in the same way

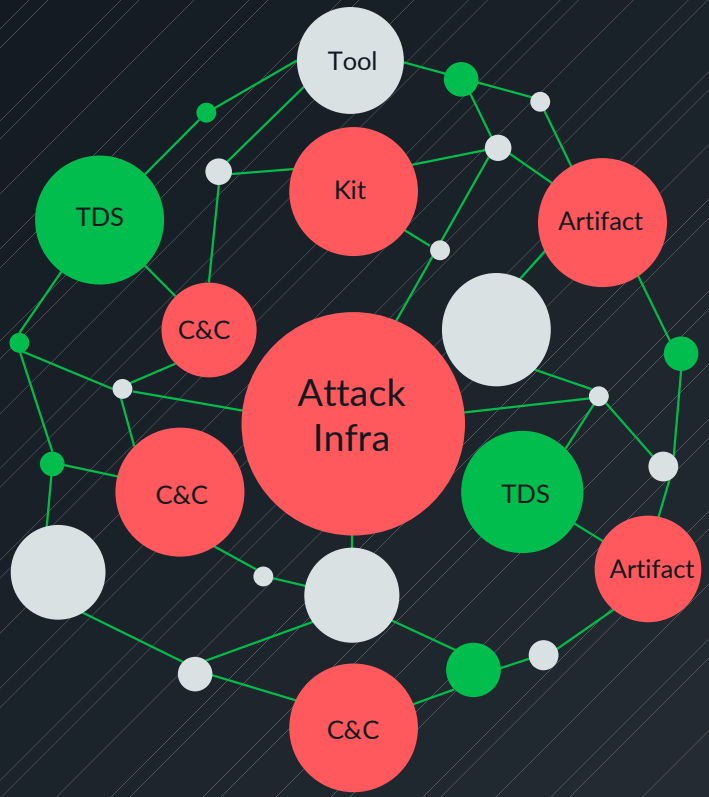
Traffic **Distribution** Systems are used in both good and malicious traffic

DNS is used and **reused** in the Distribution Systems

By analyzing massive DNS data we can identify the TDS that are **used** in different **attacks**

And build a real **MAP** of all the domains involved in the **Adversary Infrastructure**

infoblox



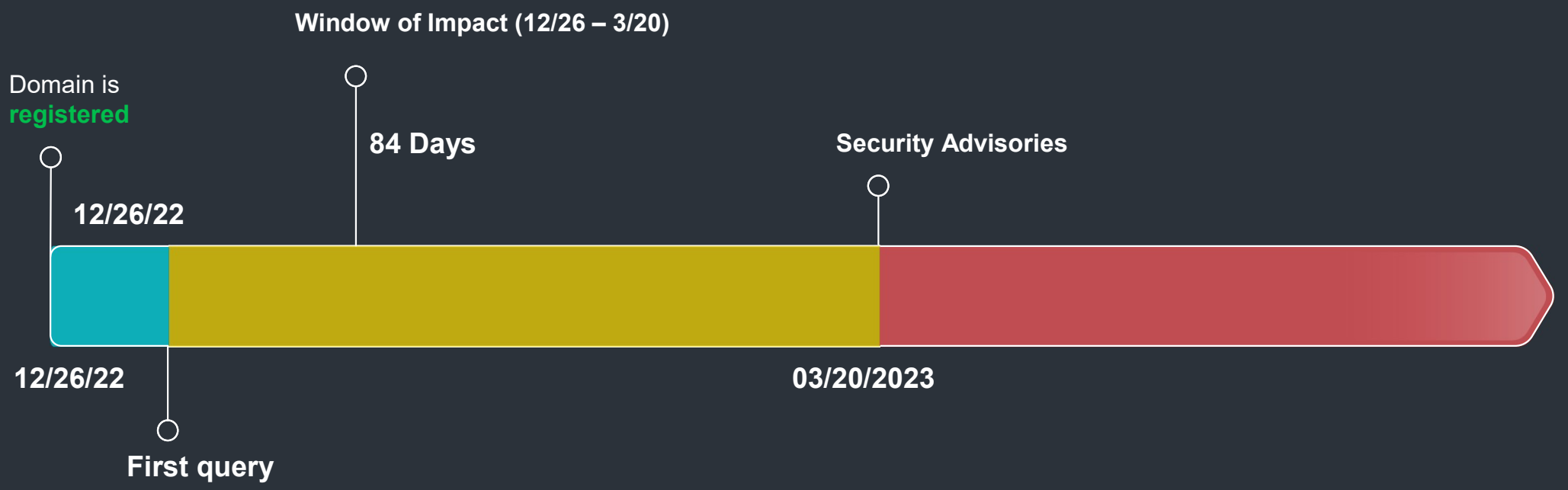
To Prevent the Threat

BEFORE THE ATTACK

infoblox

Domain Lifecycle

Example IoC: pbxphonenetwork[.]com



Example 1: Lumma C2 – dogshanter[.]xyz Domain

SUSPICIOUS Domain Detected & Blocked

8/3/2023

MALICIOUS Domains Released in OSINT

9/28/2023

Blocked 56 Days Earlier Than OSINT Malicious

8/1/2023

WHOIS Domain is Registered

https://blogs.infoblox.com/cyber-threat-intelligence/dns-early-detection-cobalt-strike-dns-c2/

Example 2: Lumma C2 – ocmtancmi2c4t[.]life

SUSPICIOUS Domain Detected & Blocked

7/10/2023

MALICIOUS Domains Released in OSINT - Estimated

9/28/2023

Blocked 80 Days Earlier Than OSINT Malicious

7/7/2023

WHOIS Domain is Registered

infoblox

DNS IS THE HEART OF NETWORKING

Every network connection starts with a DNS query—nothing runs without it

DNS's place on the network enables it to identify threats before any other security control

Establish Secure DNS as Zero Trust control point

infoblox


DNS is not just a component
IT'S THE BACKBONE
Transform DNS into your security strong point
infoblox

Ask ChatGPT

What is the role of DNS in Zero Trust?

In essence, DNS serves as a foundational component of Zero Trust architecture, enabling organizations to establish a secure and adaptive access control framework that aligns with the principles of least privilege and continuous verification. By integrating DNS with other security technologies and best practices, organizations can enhance their overall security posture and mitigate the evolving threat landscape effectively.

infoblox

THANK YOU

Geriet Wendler | gwendler@infoblox.com