infoblox.

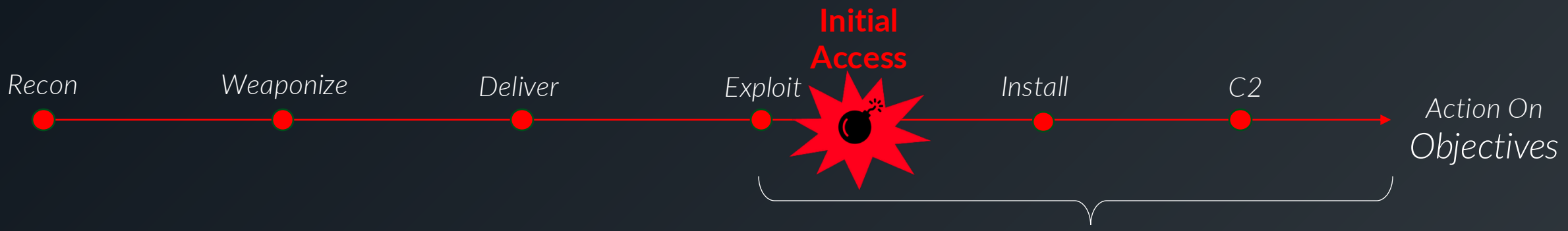
Seeing Ahead:
Turning DNS Data into a Predictive Defense

Brad Ford

infoblox. | Cybersecurity Sales Specialist

TRADITIONAL CYBERSECURITY CONTROLS

Cyber Kill Chain



Traditional Intel Sources

Sandboxing, Honeypot, IR
Forensics, OSINT, DRPS

Reactive Intel

Understand the last malicious payload

infoblox

THE NEED FOR PREDICTIVE ANALYSIS

”Anticipate and prevent attacks before they occur”

Malicious AI breaks controls

AI allows actors to intensify attacks and simplify evasion
88% of AI generated malware renders False Negatives (1)

Adversaries move to new targets

Threat actors look at any exposed asset to reach their goals
46% of stolen corporate logins are from non-managed devices (2)

Professional evasion and deception

Specialized ecosystems evade traditional controls.
82% of customers had DNS queries into malicious adtech (3)

(1) AI Could generate 10K malware variants, evading detection in 88%. The Hacker News, December 23, 2024.
(2) Verizon DBIR 2025
(3) Infoblox Threat Intel

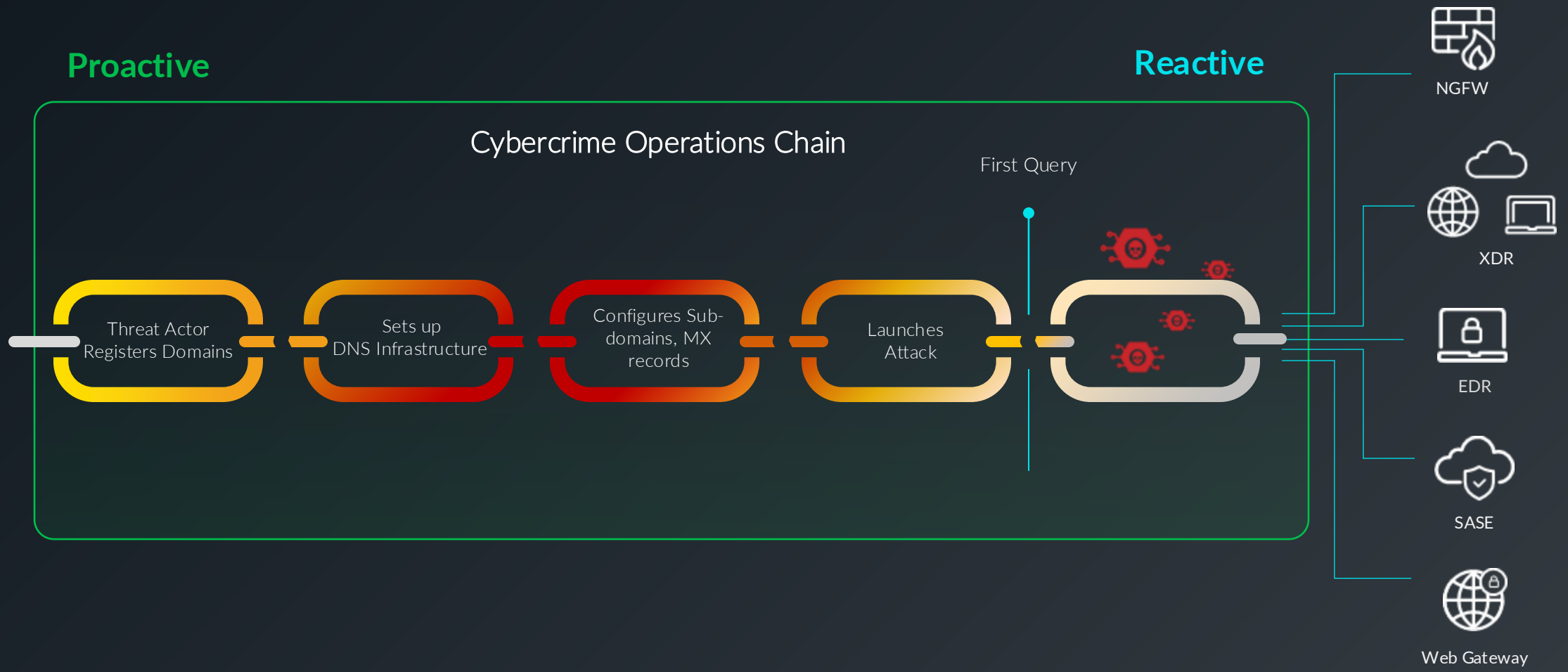
infoblox.

infoblox.

WHY DNS BASED THREAT INTEL?

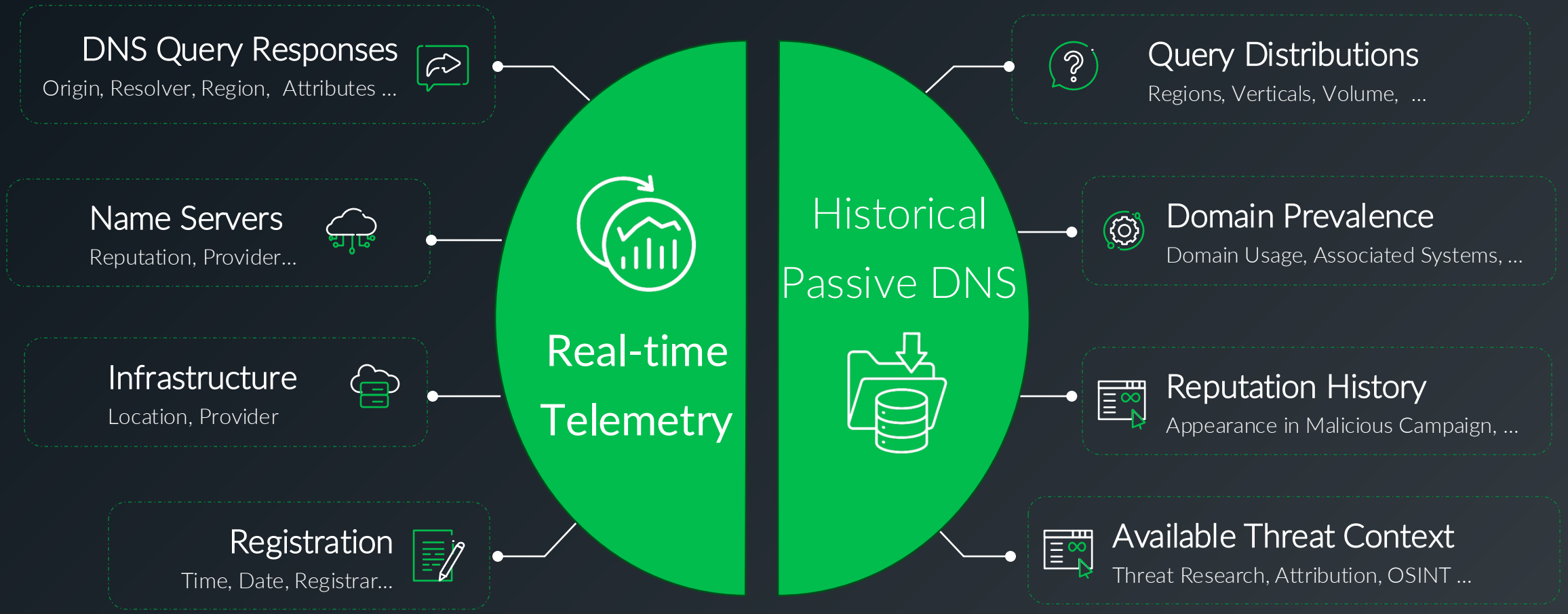
DISRUPTING THREAT ACTORS WITH DNS

DNS GETS MULTIPLE INSIGHTS INTO A THREAT – AND CHANCES TO DISRUPT IT



infoblox.

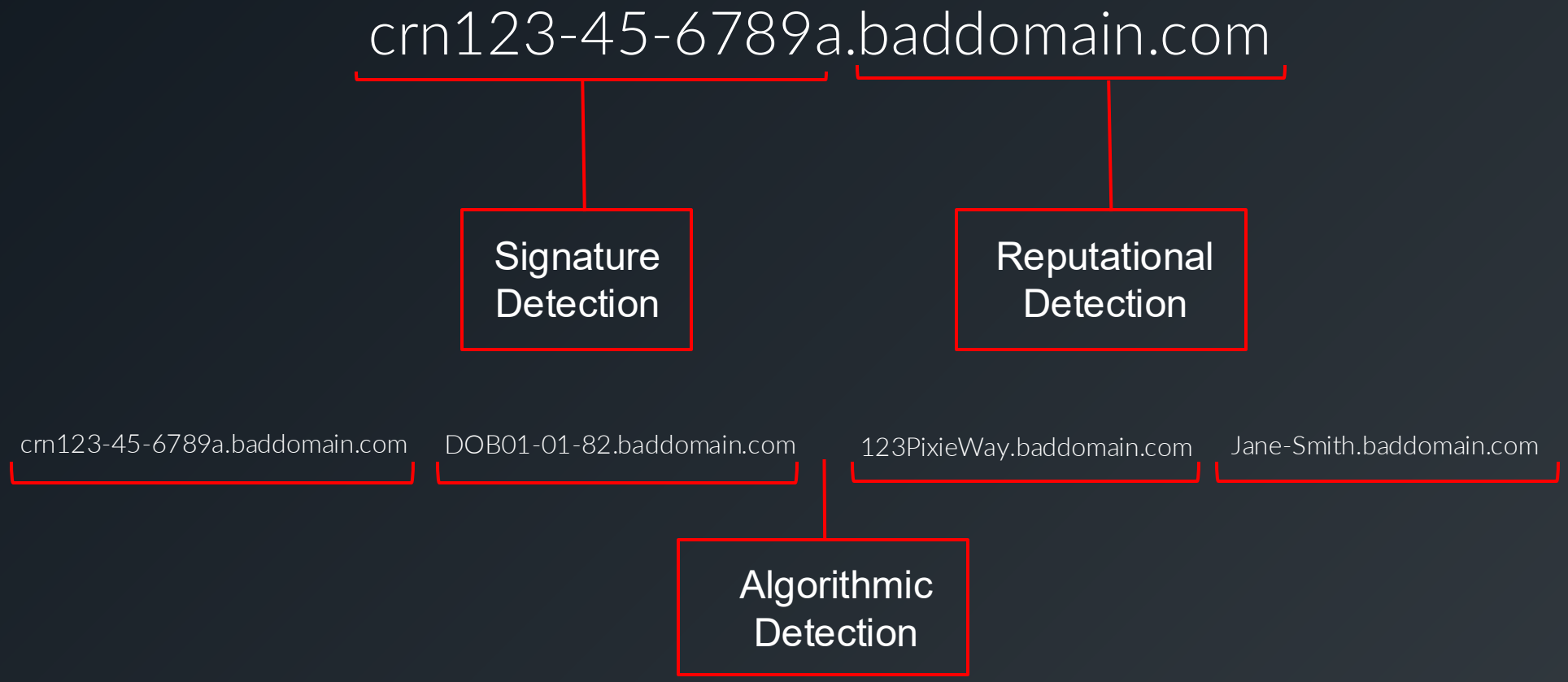
WHAT INSIGHTS CAN WE GET FROM DNS?



infoblox

DETECTION BEYOND SIGNATURES AND REPUTATION

COUNTERMEASURES FOR SOPHISTICATED TECHNIQUES



infoblox.

infoblox.

WHY DNS BASED SECURITY CONTROLS?

Almost every internet connection starts with a DNS query

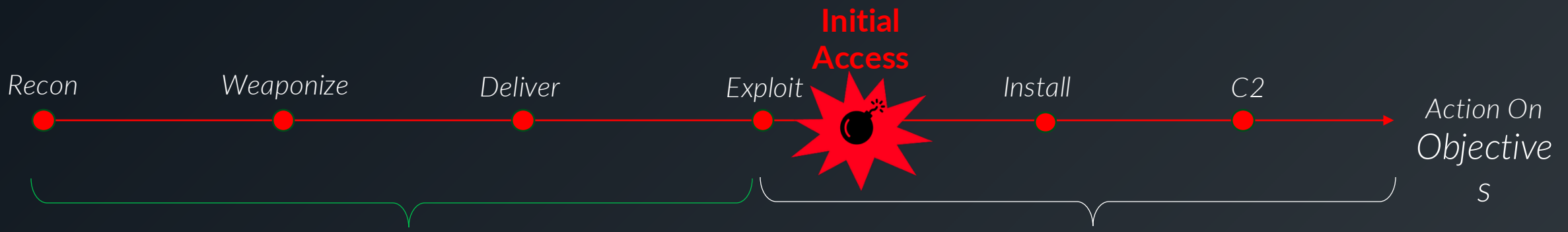
WHAT CAN DNS DISRUPT?

Initial Infection

On-Going Communication

DISRUPT AND BLOCK EARLIER

Cyber Kill Chain



Pre-Attack Telemetry

Domain Registration, Service Activation, Infrastructure, Reputation and More

Uncover Actor Logistics

Traditional Intel Sources

Sandboxing, Honeypot, IR Forensics, OSINT, DRPS

Reactive Intel

Understand the last malicious payload

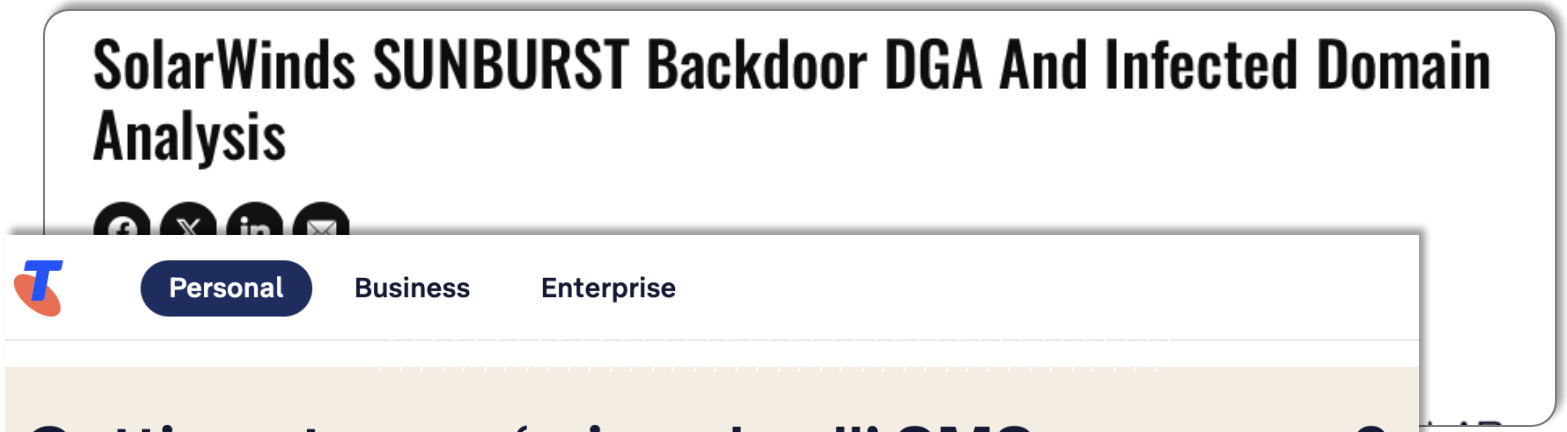
infoblox

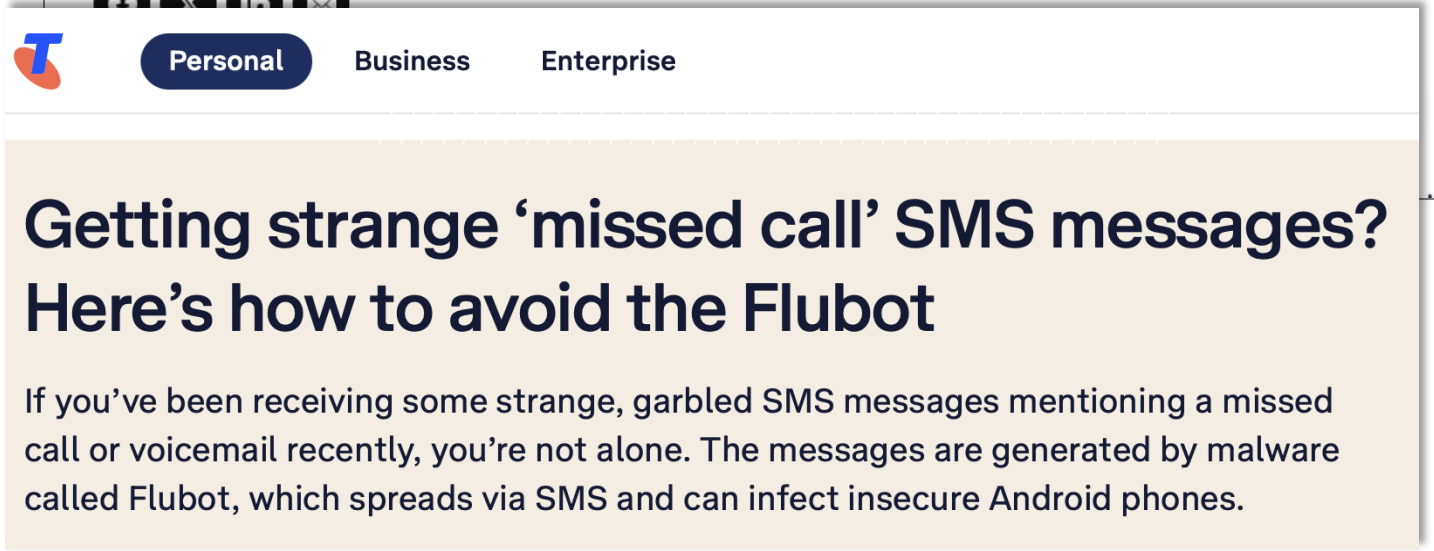
infoblox.

HOW DNS IS BEING ABUSED

HOW DNS IS BEING ABUSED

MALWARE, C2, DGAs, DoH





infoblox.

C2 OVER DNS *OVER HTTPS (DOH)*

FLUBOT

- Android banking trojan - Dec 2020
- Masquerading as a courier delivery service app or a voicemail app
- Domain Generation Algorithm (DGA) to resolve IP of C2 server
- Time-based DGA generates 5,000 domain names, all 15 characters long using“.ru”, “.su” or “.cn” TLDs
- DNS over HTTPS (DoH) used to establish C2 communication

What you see:

```
https://cloudflare-dns.com/dns-query?name=798f300c.2.1.4NLIV5GLKFX6Z2JE6TPBEUMKPRKKSGHUEYFGIQNSS4HOR3GFQO6PGCMI5YJKBSB.IK5XFEVIV3EC2C2MNEJKUPNWNU27SU3WACGD4YARQ.yacwryqiccwhlvm[.]ru&type=TXT
```


https://blog.f-secure.com/flubot_doh_tunneling/

infoblox.

HOW DNS IS BEING ABUSED

DNS TUNNELLING, DATA EXFILTRATION

securityaffairs

B1TXOR20 LINUX BOTNET USE DNS TUNNEL AND LOG4J EXPLOIT

BLEEPINGCOMPUTER

NEWS ▾ TUTORIALS ▾ VIRUS REMOVAL GUIDES ▾ DOWNLOADS ▾ DEALS ▾

Home > News > Security > Windows POS malware uses DNS to smuggle stolen credit cards

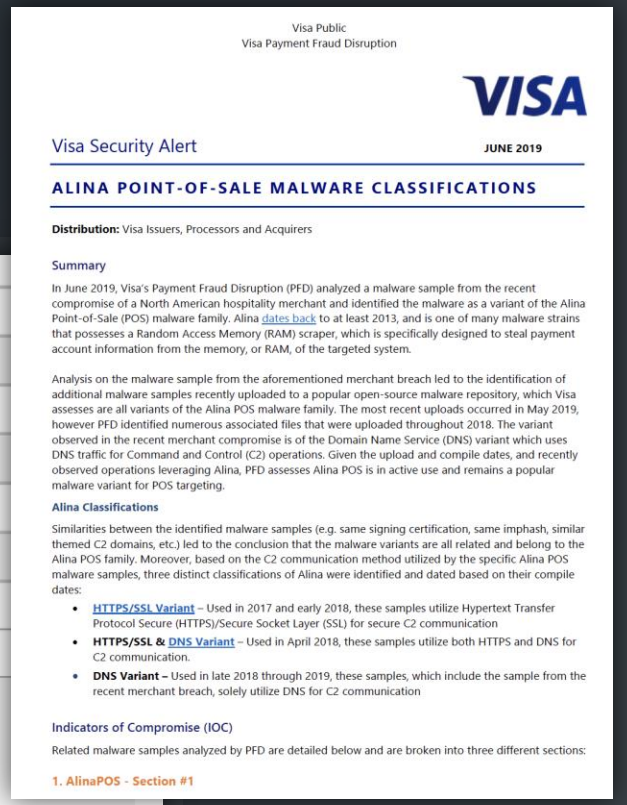
Windows POS malware uses DNS to smuggle stolen credit cards

infoblox.

DATA EXFILTRATION OVER DNS

ALINA POS

File Name	bcastdvs.exe / OneDriveUi.exe
Source	Virus Total
MD5	d000bd7c56811eec4067a4b7401bcb38
SHA1	f5e89c72f62ea9a51161b2e1407c719903308e41
SHA256	c55b2f3b67108a58c4cb81c3550115956cb07139e39a37ce9eb57ff4fb41d832
SSdeep	3072:VV3QHwn7YMzN5bkFxuy3U7qzxyeeiY5ddfkiuy41wROrHB1O5NVyT8:D7f3kFwzqz8e/YHPuLTzOfVyg
Note	Alina POS Malware (DNS Variant)
Sample	4
DNS Request(s)	zuzn4v_EkO7l5OX86-SH-umQm5DjxNney8bG.analytics-akadns[.]com yczA8vzDkO7l5OX86-SH-umQm5D53svY3g.analytics-akadns[.]com yczA8vzDkO7l5OX86-SH-umQm5D6w8TN.analytics-akadns[.]com yczA8vzDkO7l5OX86-SH-umQm5CQ2sXZhM_Sz5CQmZycmZ2dkpmTkpOemJ2cl5.iYm5uYmpuampqampqbk5mam5qampqampKdnZqamg.analytics-akadns[.]com



Visa Public
Visa Payment Fraud Disruption

VISA

Visa Security Alert — JUNE 2019

ALINA POINT-OF-SALE MALWARE CLASSIFICATIONS

Distribution: Visa Issuers, Processors and Acquirers

Summary

In June 2019, Visa's Payment Fraud Disruption (PFD) analyzed a malware sample from the recent compromise of a North American hospitality merchant and identified the malware as a variant of the Alina Point-of-Sale (POS) malware family. Alina dates back to at least 2013, and is one of many malware strains that possesses a Random Access Memory (RAM) scraper, which is specifically designed to steal payment account information from the memory, or RAM, of the targeted system.

Analysis on the malware sample from the aforementioned merchant breach led to the identification of additional malware samples recently uploaded to a popular open-source malware repository, which Visa assesses are all variants of the Alina POS malware family. The most recent uploads occurred in May 2019, however PFD identified numerous associated files that were uploaded throughout 2018. The variant observed in the recent merchant compromise is of the Domain Name Service (DNS) variant which uses DNS traffic for Command and Control (C2) operations. Given the upload and compile dates, and recently observed operations leveraging Alina, PFD assesses Alina POS is in active use and remains a popular malware variant for POS targeting.

Alina Classifications

Similarities between the identified malware samples (e.g. same signing certification, same imphash, similar themed C2 domains, etc.) led to the conclusion that the malware variants are all related and belong to the Alina POS family. Moreover, based on the C2 communication method utilized by the specific Alina POS malware samples, three distinct classifications of Alina were identified and dated based on their compile dates:

- HTTPS/SSL Variant – Used in 2017 and early 2018, these samples utilize Hypertext Transfer Protocol Secure (HTTPS)/Secure Socket Layer (SSL) for secure C2 communication
- **HTTPS/SSL & DNS Variant** – Used in April 2018, these samples utilize both HTTPS and DNS for C2 communication.
- **DNS Variant –** Used in late 2018 through 2019, these samples, which include the sample from the recent merchant breach, solely utilize DNS for C2 communication

Indicators of Compromise (IOC)

Related malware samples analyzed by PFD are detailed below and are broken into three different sections:

1. AlinaPOS - Section #1

`yczA8vzDkO7l5OX86-SH-umQm5CQ2sXZhM_Sz5CQmZycmZ2dkpmTkpOemJ2cl5.iYm5uYmpuampqampqbk5mam5qampqampKdnZqamg.analytics-akadns[.]com`

encoded data in subdomain

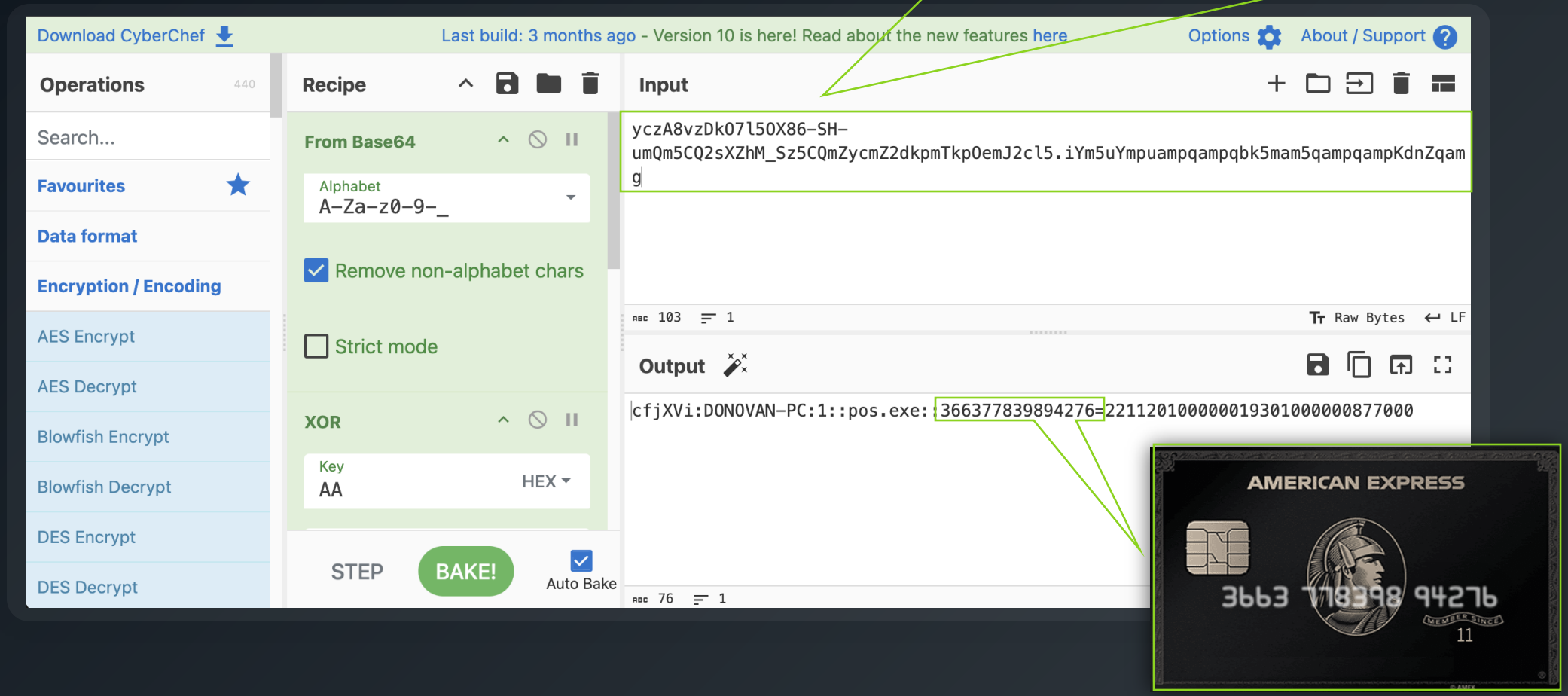
actor controlled domain

 https://usa.visa.com/dam/VCOM/global/support-legal/documents/visa-security-alert-alina-pos-malware.pdf

infoblox

DNS QUERIES BYPASSING PERIMETER CONTROLS

yczA8vzDkO7l5OX86-SH-umQm5CQ2sXZhM_Sz5CQmZycmZ2dkpmTkpOemJ2cl5.iYm5uYmpuampqampqbk5mam5qampqampKdnZqamg.analytics-akadns[.]com



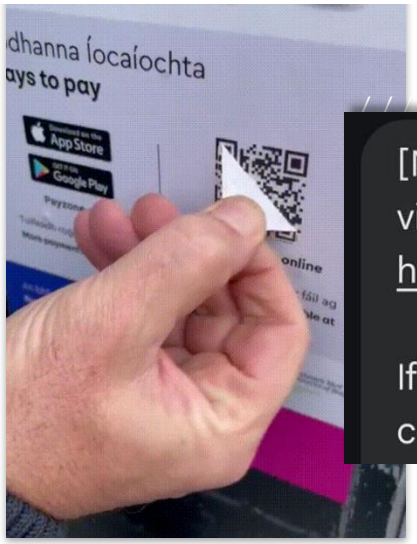
infoblox

HOW DNS IS BEING ABUSED

PHISHING, LOOKALIKES

TECHNOLOGY / NEWS

NZ Police warn against elaborate QR code attacks: don't panic, but beware where the scans want to take you



[NZTA] Overdue Notice:Please log
view your toll invoice:
https://bit.ly/6ll1q?TMc=ISZO5cjNz

If you fail to pay,we will submit it t
court within 15 working days or so.

Scam Alert ⚠

Watch out for this scam message pretending to be from NZ Post. If received, don't click any links and delete immediately.

iMessage
Today 2:22 PM

New Zealand Post Office: Your package has arrived at the warehouse and has been suspended for delivery due to a missing home number in the package. Please update:
https://nzpost.

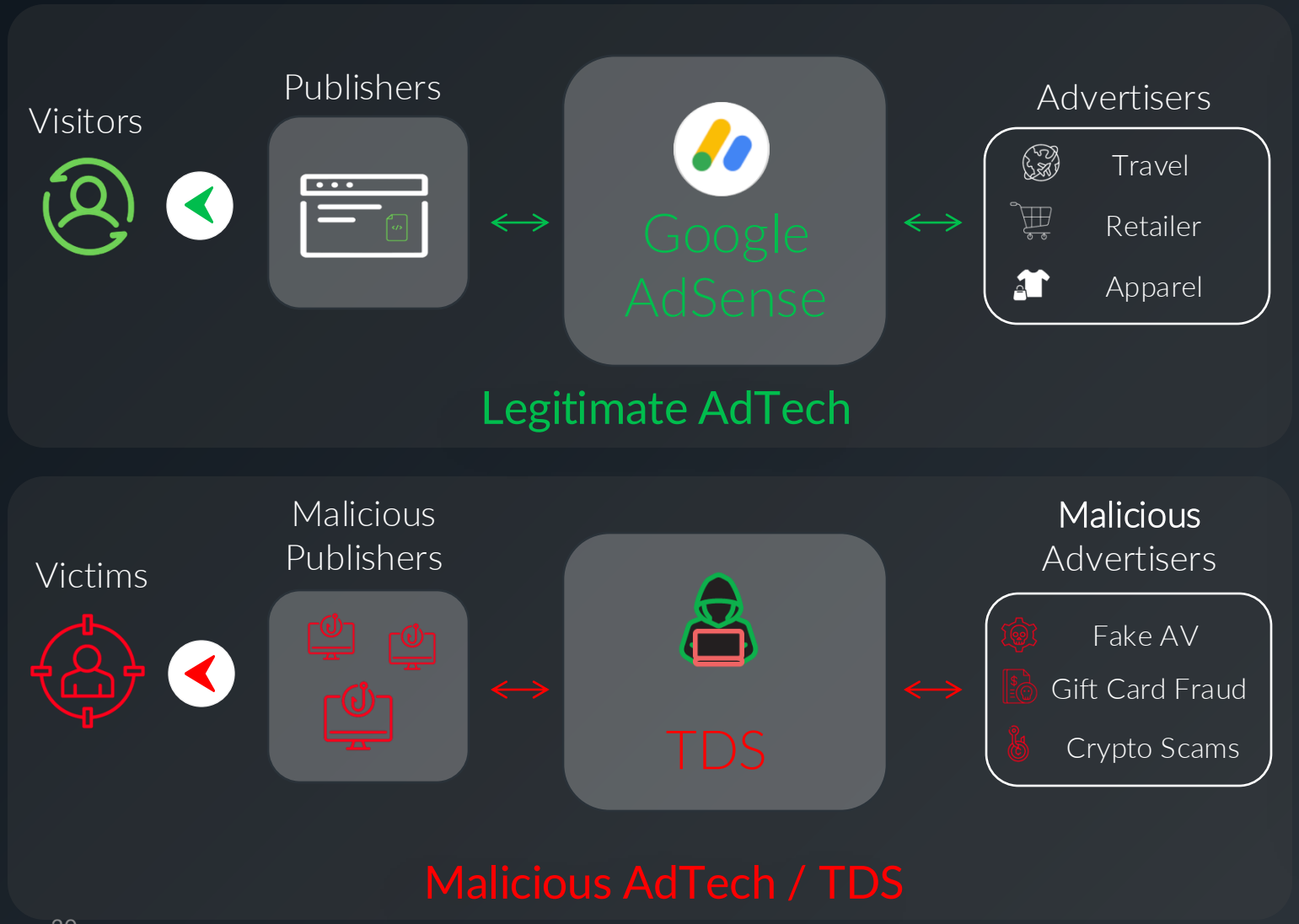
infoblox.

HOW DNS IS BEING ABUSED

ADTECH, TRAFFIC DISTRIBUTION SYSTEMS (TDS)

infoblox.

TRAFFIC DISTRIBUTION SYSTEM (TDS)



Attackers can't use Google AdSense

So they use a malicious TDS to deliver the right content to the right audience while remaining undetected

Operating since 2015, Vextrio Viper registered 80k+ unique domains, using Dictionary DGAs and rotates 100's of domains per day

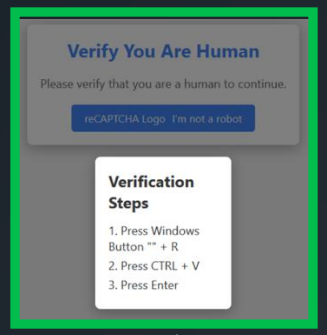
Infoblox tracks ~100 malicious TDS clusters in near real time

infoblox.

USING TDS TO DELIVER INFOSTEALER MALWARE

1 Visit compromised site

2 Fake CAPTCHA



Download & launch obfuscated code

(EDR Bypass)

3 Information Stealer

Victim

1 Initial Landing Domains

Thehartfford[.]com
Onlinetesco[.]com
Verizoninterprise[.]com

2 Profile and Redirect Traffic

Based on OS, GEO, CounterIntel, Trackers, Cookies, etc

Decoy Site
Benign Content

3 Weaponised Domains

Privacy-shield[.]online
Passpass[.]online
Sbrowse[.]me
Stealth-browse[.]cc
Guard-mate[.]online

Access Brokers harvesting credentials via Lummastealer

Affiliate

Operating Actor - Vane Viper

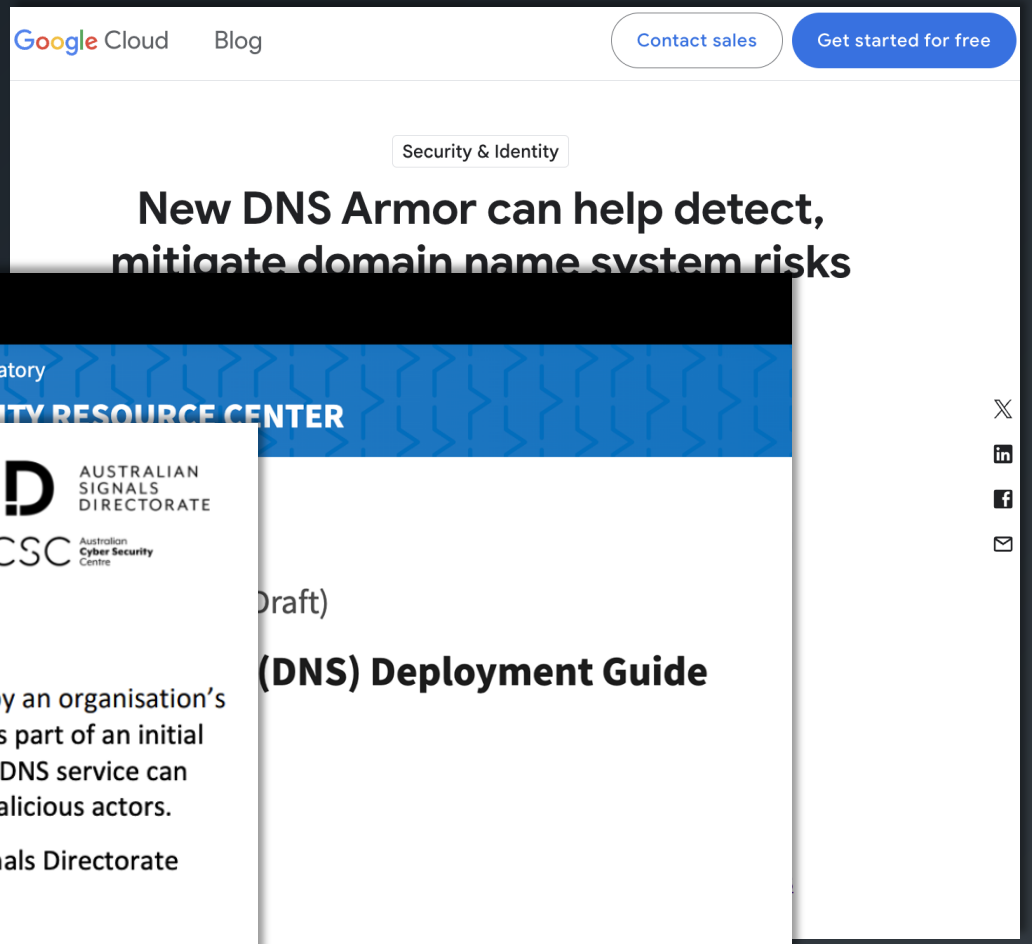
infoblox

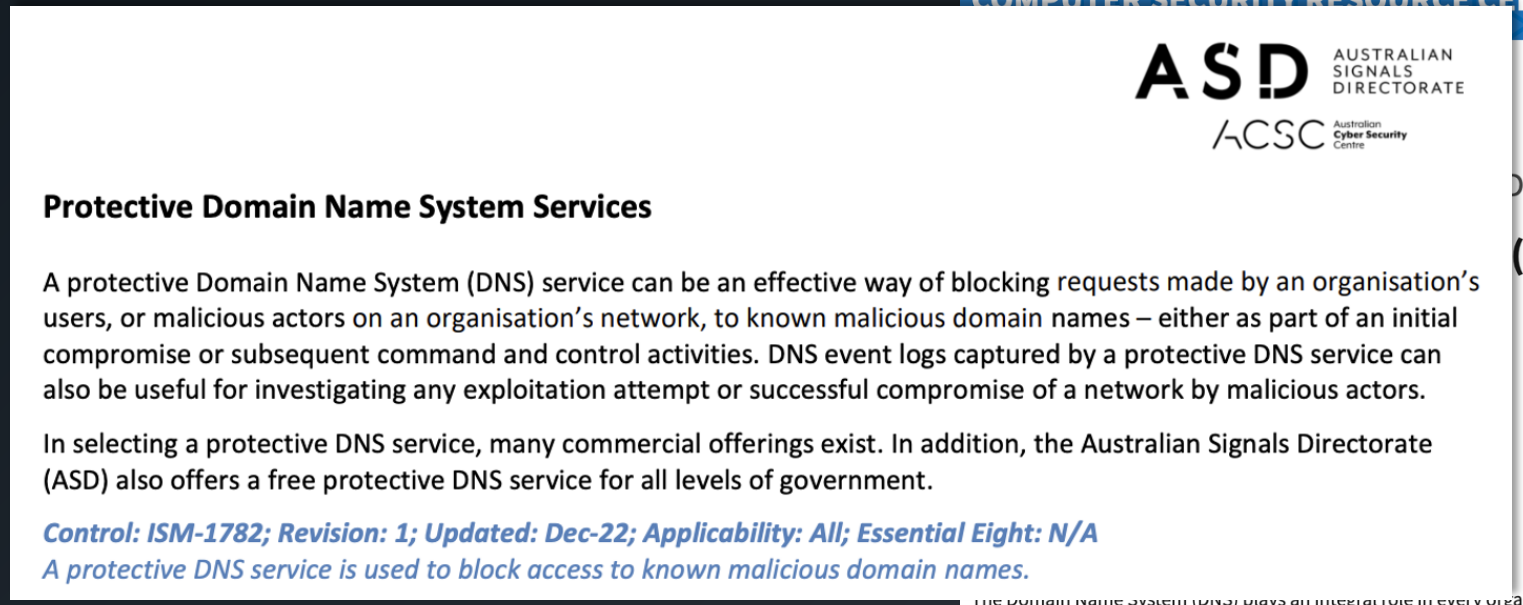
infoblox

PROTECTIVE DNS (PDNS) BECOMING IMPERATIVE

INCREASED ADOPTION OF PDNS

- GCP DNS Armor – other CSPs to follow
- NIST– PDNS included in Special Publication
- ASD – Inclusion of PDNS in ISM





infoblox.

LEARN, VALIDATE AND EVALUATE

STEPS TO BETTER UNDERSTAND HOW DNS IS BEING ABUSED IN YOUR NETWORK TODAY!

DNS SECURITY WORKSHOP

Customer enablement initiative, 2-4 hours to educate on how DNS is used by threat actors and better understand the role of DNS in modern cyber threats

DNS SECURITY ASSESMENT

Real Time customer DNS traffic analysis, to detect insights into potential malicious DNS activity like attacks, threats, content and brand reputation

DNS SECURITY AUDIT

Quick review by using simple DNS queries to assess a company's DNS security posture and identify potential gaps including data exfiltration and infiltration

Thank you