From Vulnerability to Vanguard
Reinventing DNS Security

Brad Ford

infoblox | Cybersecurity Sales Specialist

Why Threat Actors Like Domains

infoblox

DNS IS OMNIPRESENT

Domains provide:
Credibility,
Authenticity,
& Stealth

Spam
Use reputation of stolen domain to distribute emails

Phish
Mimic sites to extract credentials

Deceive
Trick users into high-risk actions

Evade
Hide behind complex mesh of domain names and redirections

90% of successful cyber-attacks start with a link or webpage that looks legitimate - *CISA 2024*

infoblox

HOW DNS GETS ABUSED

MALWARE, C2, DGAs, DoH

SolarWinds SUNBURST Backdoor DGA And Infected Domain Analysis

Personal Business Enterprise

Getting strange 'missed call' SMS messages? Here's how to avoid the Flubot

If you've been receiving some strange, garbled SMS messages mentioning a missed call or voicemail recently, you're not alone. The messages are generated by malware called Flubot, which spreads via SMS and can infect insecure Android phones.

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

Personal Business Enterprise

Getting strange ‘missed call’ SMS messages? Here’s how to avoid the Flubot

If you’ve been receiving some strange, garbled SMS messages mentioning a missed call or voicemail recently, you’re not alone. The messages are generated by malware called Flubot, which spreads via SMS and can infect insecure Android phones.

What you see:

```
https://cloudflare-dns.com/dns-
query?name=798f300c.2.1.4NLIV5GLKFX6Z2JE6TPBEUMKPR
KKSGHUEYFGIQNSS4HOR3GFQO6PGCMI5YJKBSB.IK5XFEVIV3EC
2C2MNEJKUPNWNU27SU3WACGD4YARQ.yacwryqiccwhlvm[.]ru
&type=TXT
```

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

HOW DNS GETS ABUSED

DNS TUNNELLING, DATA EXFILTRATION

securityaffairs

B1TXOR20 LINUX BOTNET USE DNS TUNNEL AND LOG4J EXPLOIT

BLEEPINGCOMPUTER

Search

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

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
```

$\underbrace{\texttt{yczA8vzDkO7l5OX86-SH-umQm5CQ2sXZhM\_Sz5CQmZycmZ2dkpmTkpOemJ2cl5.iYm5uYmpuampqampqbk5mam5qampqampKdnZqamg}}_{\text{encoded data in subdomain}}.\underbrace{\texttt{analytics-akadns[.]com}}_{\text{actor controlled domain}}$

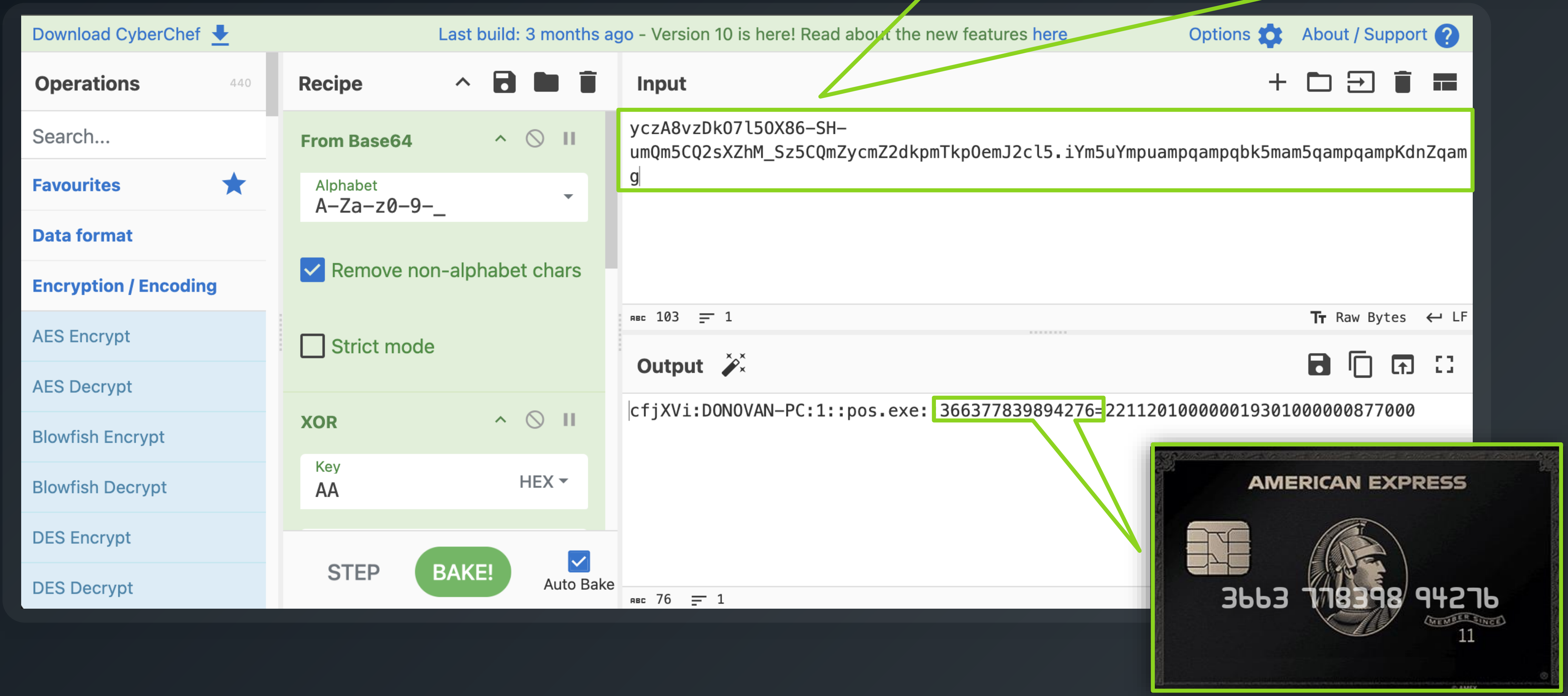
https://usa.visa.com/dam/VCOM/global/support-legal/documents/visa-security-alert-alina-pos-malware.pdf

infoblox

DATA EXFILTRATION OVER DNS

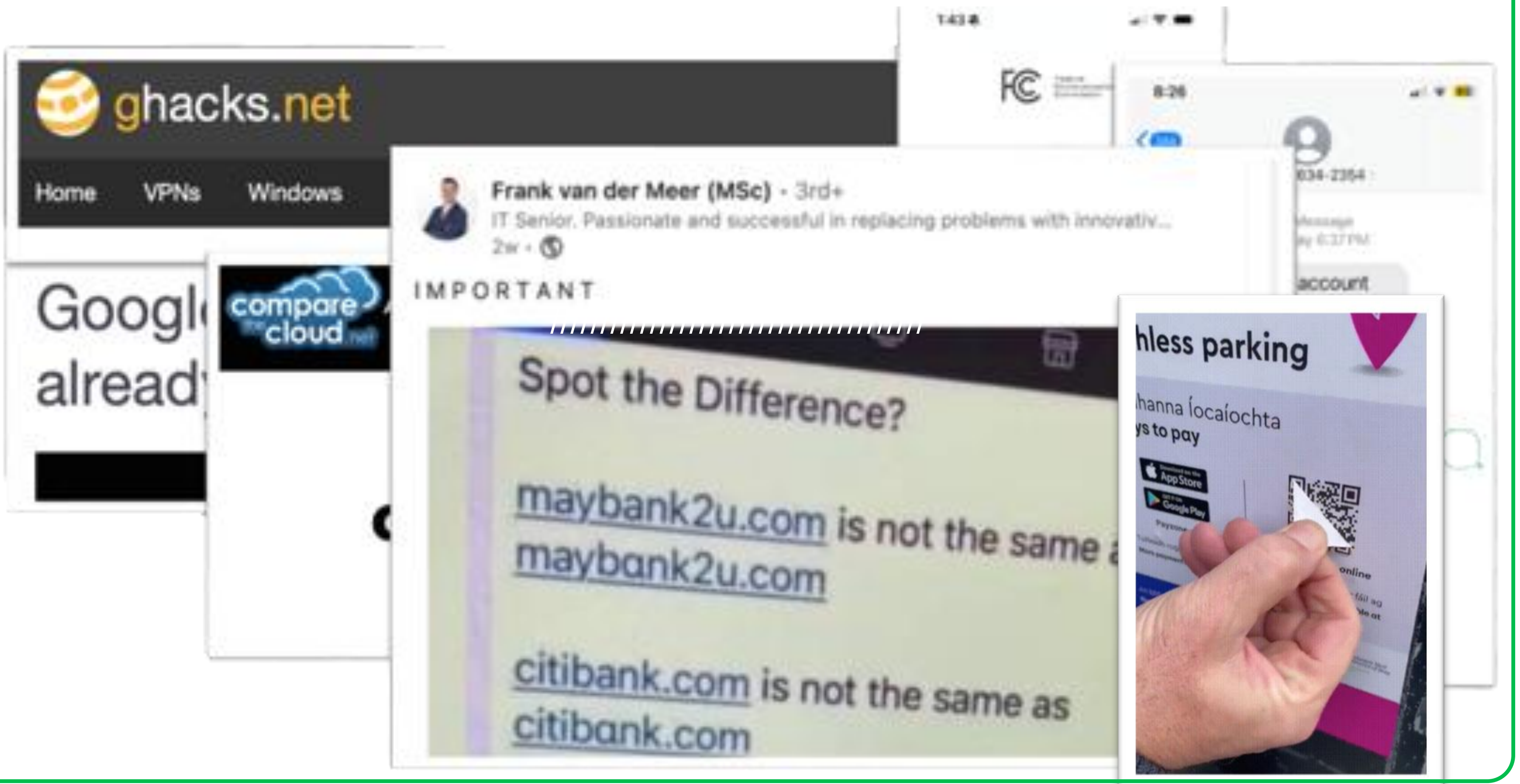
DNS QUERIES BYPASSING PERIMETER CONTROLS

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



HOW DNS GETS ABUSED

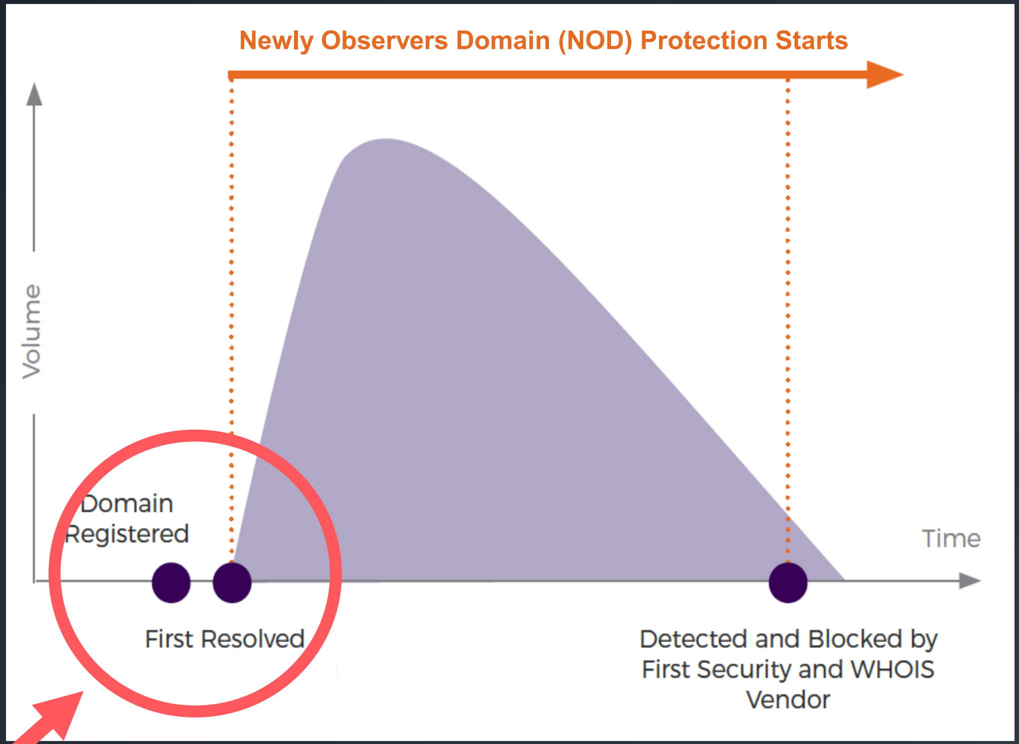
PHISHING, LOOKALIKES



NEW DOMAIN CHALLENGE

‘ZERO-HOUR PROTECTION AGAINST QUICK-STRIKE ATTACKS’

- Attacker registers many domains in advance
- Strategic timing and parking of domains
- Uses a domain for malicious purposes for a few hours or a day and then switches
- Lag between domain registration and propagation in DNS infrastructure/WHOIS

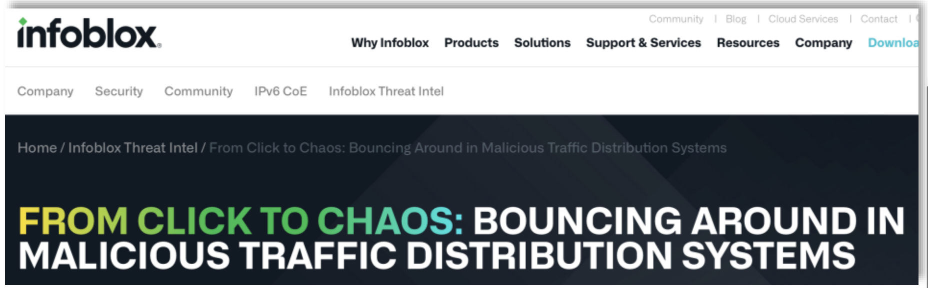


Gap being exploited!

infoblox

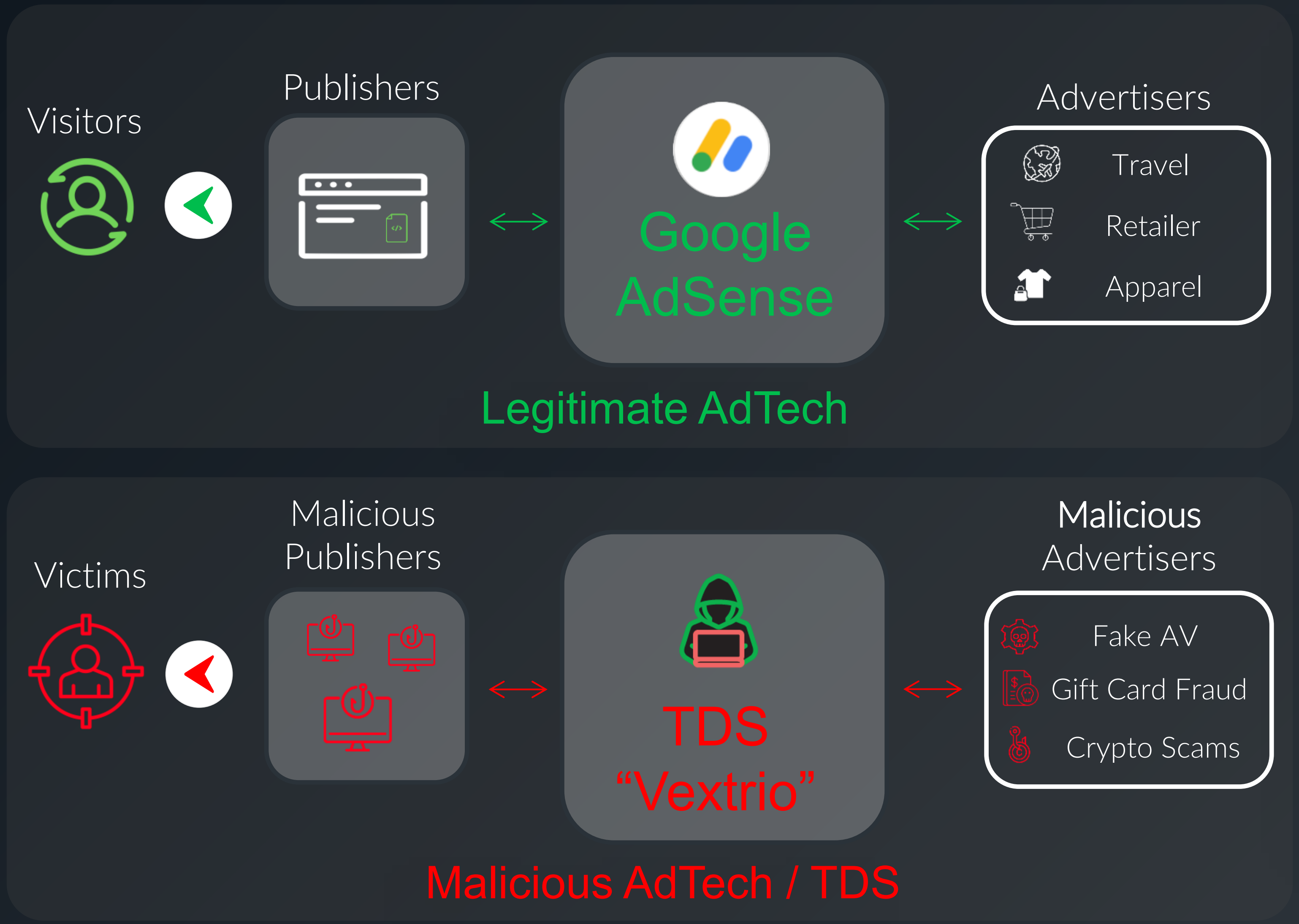
HOW DNS GETS ABUSED

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, including Vextrio Viper

infoblox

TRACKING TRAFFIC DISTRIBUTION SYSTEMS (TDS)

What

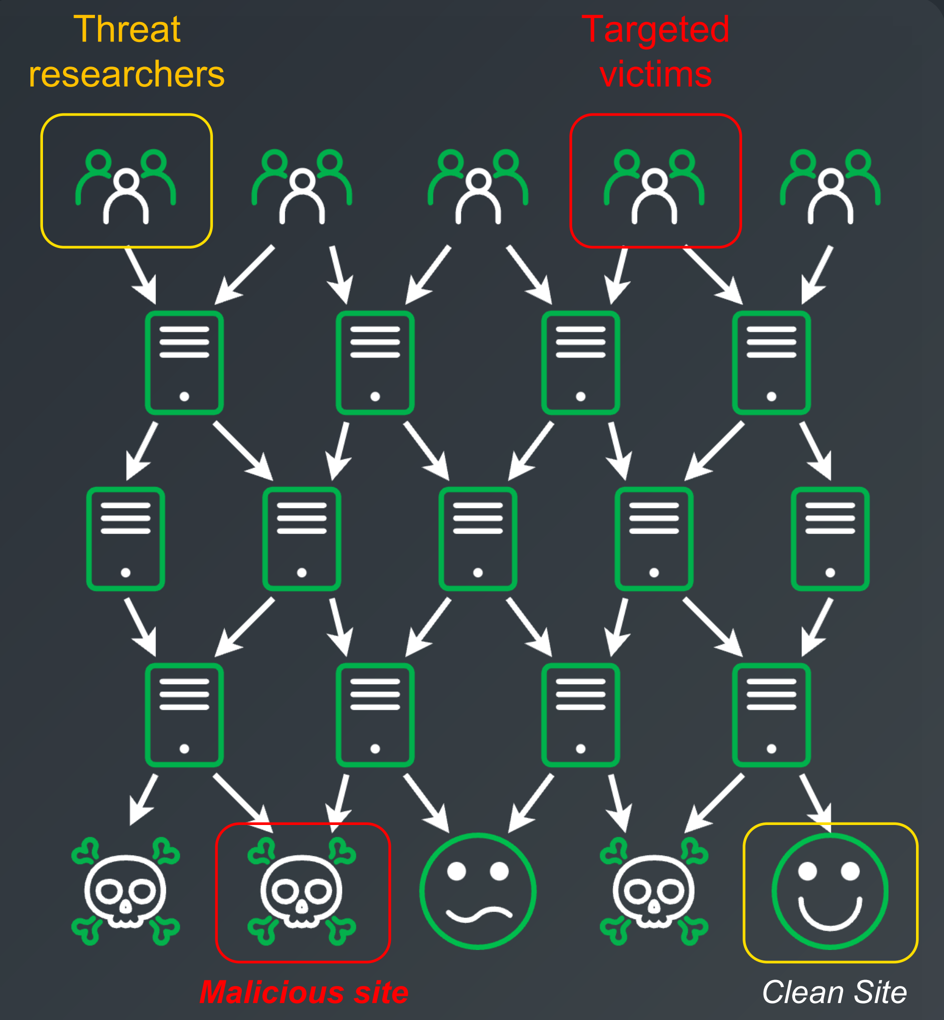
- “CLOAKING” system
- Redirections via DNS Infrastructure
- Available For Lease (6 USD/Day per site)

Why

- HIDE Malicious Sites from Threat Researchers
- Target “IDEAL” Victim

Danger

- Bypass Security Controls
- Fast Changing via Domain Rotation
- Hard to Take Down. Lifespan of +5 Years.



infoblox

HOW DNS GETS ABUSED

ABUSE OF HIGH REPUTATION DOMAINS

STEP 1

Legit site owner decommissions cloud app, forgets CNAME Record

CNAME Entry

ahbazuretestapp.cdc.gov

Cloud provider removes internal CNAME records

ahbdotnetappwithsqldb. azurewebsites.net

DECOMMISSIONED CLOUD APP

13.75.34.176

STEP 2

Actor reuses domain with cloud provider, and deploys malicious content

CNAME Entry

ahbazuretestapp.cdc.gov

Cloud provider reactivates internal CNAME records pointing to malicious content

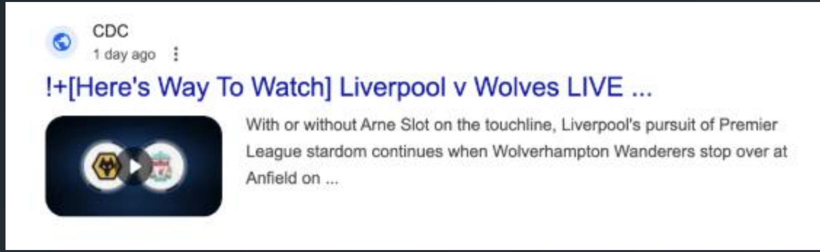
ahbdotnetappwithsqldb. azurewebsites.net

MALICIOUS CONTENT (E.g. Video)

13.75.38.212

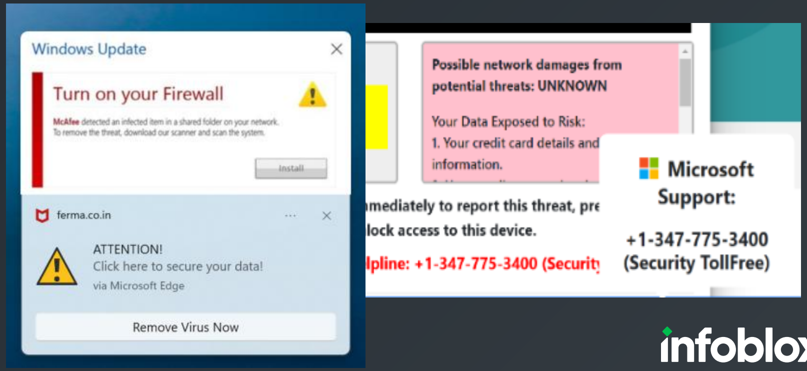
STEP 3

Search engines discover high-reputation domains (cdc.gov) with actor content



STEP 4

Visitors are tricked into actor content and rerouted into malicious advertisements, scams



infoblox

DANGLING CNAMES

Indicator	Data Type	Threat Class	Threat Property	Detected	Data Provider
[redacted].tmca-digital.com.au	HOST	Policy	Policy_DanglingRecord	2025-07-17T10:40:55.622Z	Infoblox
[redacted].tmca-digital.com.au	HOST	Policy	Policy_DanglingRecord	2025-07-17T10:40:55.622Z	Infoblox
[redacted]tity.tmca-digital.com.au	HOST	Policy	Policy_DanglingRecord	2025-07-17T10:40:55.622Z	Infoblox
[redacted]a.vic.gov.au	HOST	Policy	Policy_DanglingRecord	2025-07-16T10:40:41.605Z	Infoblox
[redacted].fmgl.com.au	HOST	Policy	Policy_DanglingRecord	2025-07-16T10:40:41.604Z	Infoblox
[redacted].vic.gov.au	HOST	Policy	Policy_DanglingRecord	2025-07-17T10:40:55.622Z	Infoblox
[redacted]integritylife.com.au	HOST	Policy	Policy_DanglingRecord	2025-07-17T10:40:55.621Z	Infoblox

infoblox Dossier™

Threat Research Portal

[redacted].vic.gov.au

First Seen: 07/16/2025 *Last Active Threat Detection: 07/16/2025 (Active)*

- Current DNS
- **Related Domains**
- Related URLs
- Related IPs
- Related File Samples

Related Domains will show domains that have been tied to this indicator based on many possible associations such as malware that uses multiple domains.

DOMAIN	LAST REPORT	SOURCE	CNAME
[redacted].vic.gov.au.	07/19/2025	PDNS	[redacted].cloudapp.azure.com.

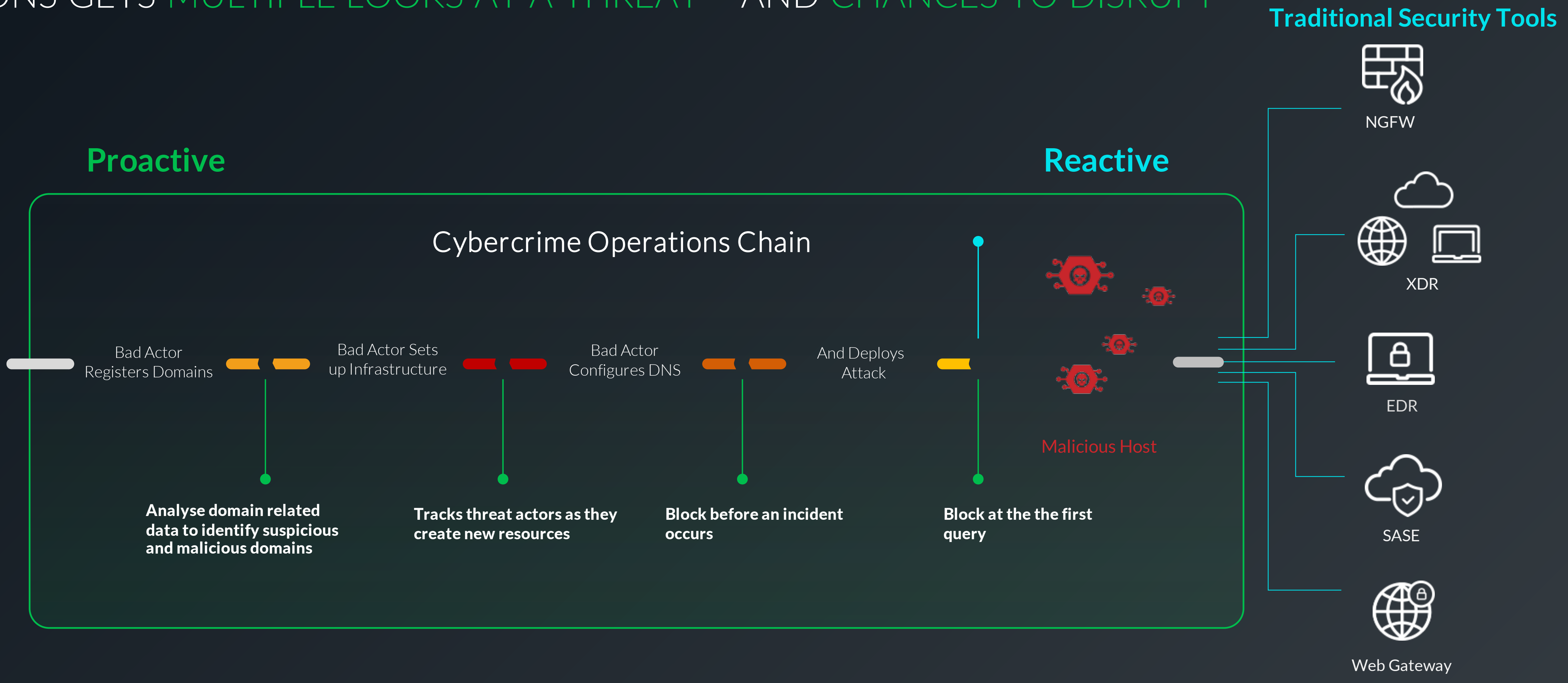
infoblox

Using the Domain Name System for Threat Detection & Response

infoblox

DISRUPTING THREAT ACTORS WITH DNS

DNS GETS MULTIPLE LOOKS AT A THREAT – AND CHANCES TO DISRUPT



DNS BASED THREAT INTEL

USING DNS FOR THREAT HUNTING – DNS MINUTIAE PATTERNS

Registration
Time, Date, Registrar…

Query Distributions
Regions, Verticals, Volume …

DNS Responses
Resolver, Region, Variety …

Name Features
Similarity, Usage of Known Brands

Name Servers
Location, Reputation, …

Hosting
Domain Provider, Location, …

Domain History
Appearance in Malicious Campaign

Domain Prevalence
Domain Usage, Associated Systems, …

DETECTION BEYOND SIGNATURES AND REPUTATION

COUNTERMEASURES FOR SOPHISTICATED TECHNIQUES

crn123-45-6789a.baddomain.com

Signature Detection

Reputational Detection

crn123-45-6789a.baddomain.com

DOB01-01-82.baddomain.com

123PixieWay.baddomain.com

Jane-Smith.baddomain.com

Behavioral Detection

infoblox

HIDDEN CHALLENGE OF PROTECTIVE DNS

Just blocking at the DNS layer is simple!

Source and apply threat intel **designed for DNS**

Analyse DNS queries and responses for **ALL** record types

User and device **attribution** – who, what, where?

COUNTRIES, GOVERNMENTS AND PRIVATE SECTOR ARE ADOPTING PROTECTIVE DNS (PDNS)

ASD INFORMATION SECURITY MANUAL (ISM)

Australian Government
Australian Signals Directorate

Protective Domain Name System Services

A protective Domain Name System (DNS) service can be an effective way of blocking requests made by an organisation's users, or malicious actors on an organisation's network, to known malicious domain names – either as part of an initial compromise or subsequent command and control activities. DNS event logs captured by a protective DNS service can also be useful for investigating any exploitation attempt or successful compromise of a network by malicious actors.

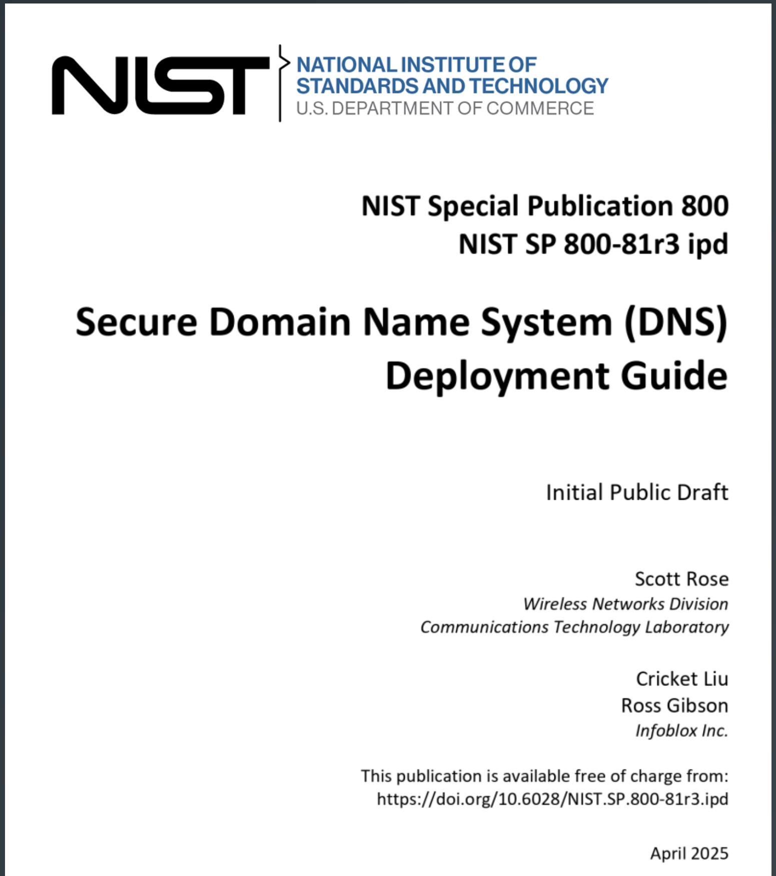
In selecting a protective DNS service, many commercial offerings exist. In addition, the Australian Signals Directorate (ASD) also offers a free protective DNS service for all levels of government.

Control: ISM-1782; Revision: 1; Updated: Dec-22; Applicability: All; Essential Eight: N/A
A protective DNS service is used to block access to known malicious domain names.

https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism

infoblox

NIST SPECIAL PUBLICATION - PROTECTIVE DNS


NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Special Publication 800
NIST SP 800-81r3 ipd

Secure Domain Name System (DNS) Deployment Guide

Initial Public Draft

Scott Rose
Wireless Networks Division
Communications Technology Laboratory

Cricket Liu
Ross Gibson
Infoblox Inc.

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-81r3.ipd

April 2025

Three Pillars for Best Practices

Employing Protective DNS

Protecting DNS Protocol

Protecting DNS Service and Infrastructure

https://csrc.nist.gov/pubs/sp/800/81/r3/ipd

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 teach customers how DNS is used by malware, understand the role of DNS in modern cyber threats
- DNS SECURITY ASSESTMENT; Real Time customer traffic analysis (captured data), 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 DNS security posture and identify potential gaps including data exfiltration and infiltration

Thank you

infoblox®