

Everything You Need to Know About DNS Attacks

Live Date: May 23, 2023

Sponsored by



DARKReading

ON24 Webinar Logistics

Optimize your experience today

- **Enable pop-ups** within your browser
- **Turn on your system's sound** to hear the streaming presentation
- **Questions?** Submit them to the presenters at anytime on the console
- **Technical problems?** Click “Help” or submit a question for assistance

Featured Presenters

Our knowledgeable speakers today are:



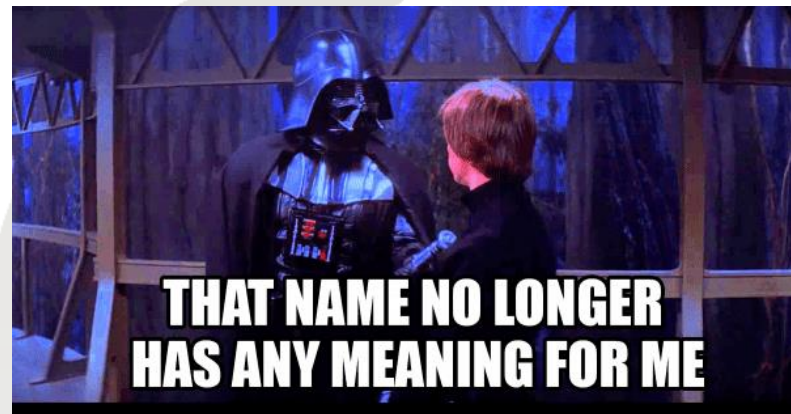
Jonathan Care
Advisor
Lionfish Tech
Advisors



Srikrupa Srivatsan
Director of Product
Marketing
Infoblox



Becky Bracken
Editor
Dark Reading



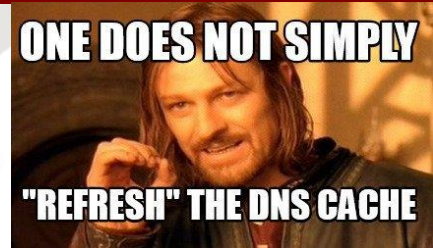
Everything You Need to Know About DNS Attacks

Jonathan Care, Lionfish Tech Advisors

No servers could be reached



What is DNS, anyway?



- Domain name system (DNS) is a protocol that translates a domain name, such as **jonathan.care**, into an IP address such as **35.241.62.186**.
- When users type the domain name **jonathan.care** into a browser, a DNS resolver (a program in the operating system) searches for the numerical IP address or **jonathan.care**. Here is how it works:
 - The DNS resolver looks up the IP address in its local cache.
 - If the DNS resolver does not find the address in the cache, it queries a DNS server.
 - The recursive nature of DNS servers enables them to query one another to find a DNS server that has the correct IP address or to find an authoritative DNS server that stores the canonical mapping of the domain name to its IP address.
 - Once the resolver finds the IP address, it returns it to the requesting program and also caches the address for future use.

It's not DNS

There's no way it's DNS

It was DNS



It was DNS
There's no way it's DNS
It's not DNS

三好





Understanding attacks on DNS

Why perform an attack on the DNS?

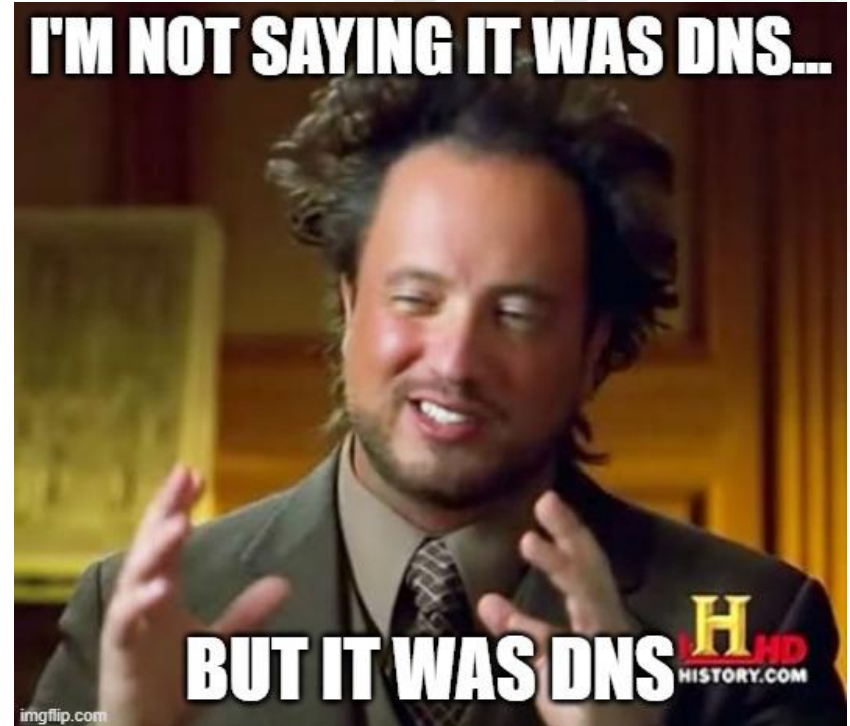
“Because that’s where the money is” – Willie Sutton



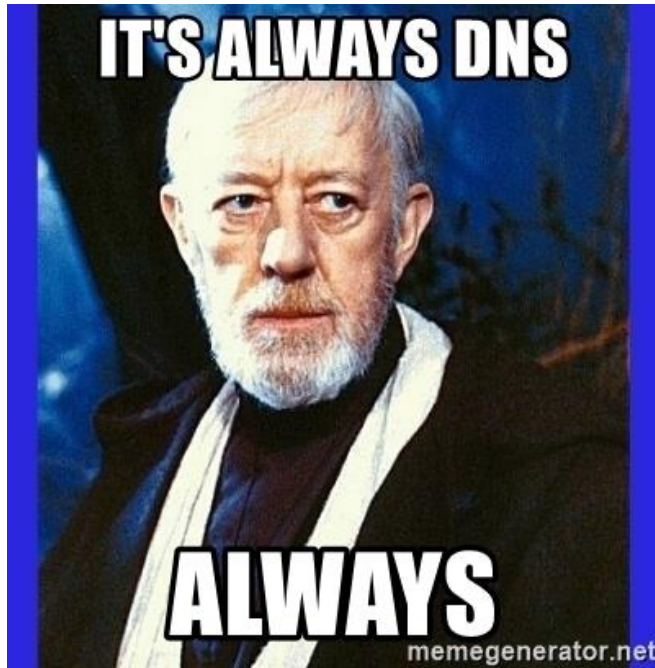
- DNS is a fundamental service of the IP network and the internet.
- If the resolution service becomes unavailable, the majority of applications can no longer function.
- Attackers often try to deny the DNS service by bypassing the protocol standard function, or using bug exploits and flaws.
- DNS is accepted by all security tools with limited verification on the protocol or the usage.
- This can open doors to tunneling, data exfiltration and other exploits employing underground communications.

5 Types of DNS attacks

- DNS Tunnelling
- DNS Amplification
- DNS Flood Attack
- DNS Spoofing
- NXDOMAIN attack



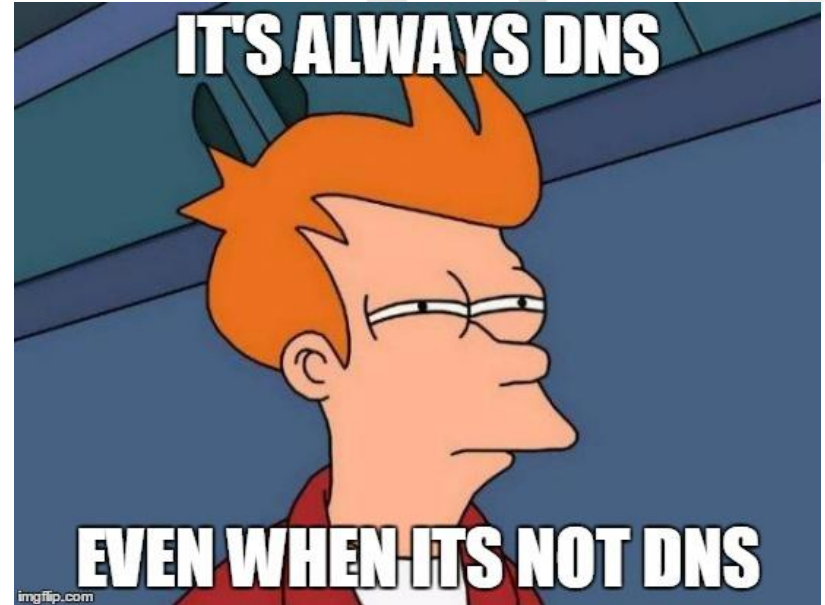
DNS Tunnelling



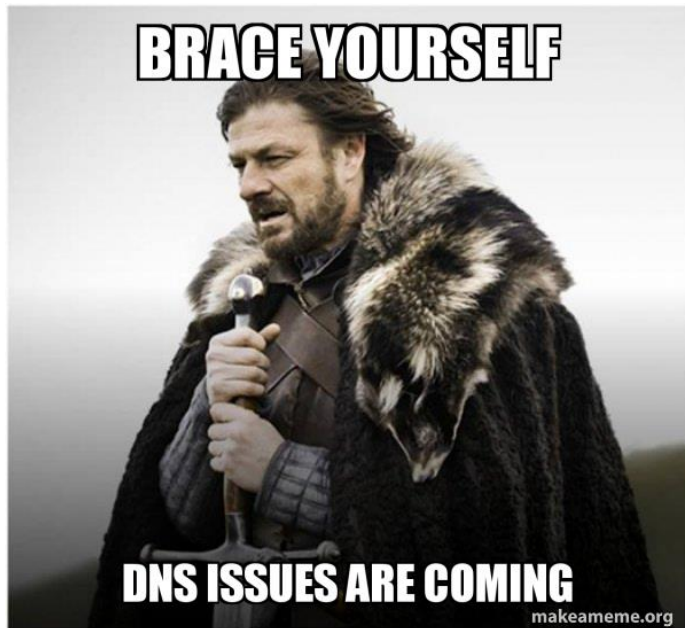
- DNS tunnelling involves encoding the data of other programs or protocols within DNS queries and responses.
- It usually features data payloads that can take over a DNS server and allow attackers to manage the remote server and applications.
- DNS tunnelling often relies on the external network connectivity of a compromised system, which provides a way into an internal DNS server with network access.
- It also requires controlling a server and a domain, which functions as an authoritative server that carries out data payload executable programs as well as server-side tunnelling.

DNS Amplification

- DNS amplification attacks perform Distributed Denial of Service (DDoS) on a targeted server.
- This involves exploiting open DNS servers that are publicly available, in order to overwhelm a target with DNS response traffic.
- Typically, an attack starts with the threat actor sending a DNS lookup request to the open DNS server, spoofing the source address to become the target address.
- Once the DNS server returns the DNS record response, it is passed to the new target, which is controlled by the attacker.



DNS Flood Attack



- DNS flood attacks involve using the DNS protocol to carry out a user datagram protocol (UDP) flood.
- Threat actors deploy valid (but spoofed) DNS request packets at an extremely high packet rate and then create a massive group of source IP addresses.
- Since the requests look valid, the DNS servers of the target start responding to all requests.
- Next, the DNS server can become overwhelmed by the massive amount of requests.
- A DNS attack requires a great amount of network resources, which tire out the targeted DNS infrastructure until it is taken offline.
- As a result, the target's internet access also goes down.

DNS Spoofing

- DNS spoofing, or DNS cache poisoning, involves using altered DNS records to redirect online traffic to a fraudulent site that impersonates the intended destination.
- Once users reach the fraudulent destination, they are prompted to login into their account.
- Once they enter the information, they essentially give the threat actor the opportunity to steal access credentials as well as any sensitive information typed into the fraudulent login form.
- Additionally, these malicious websites are often used to install viruses or worms on end users' computers, providing the threat actor with long-term access to the machine and any data it stores.



NXDOMAIN Attack



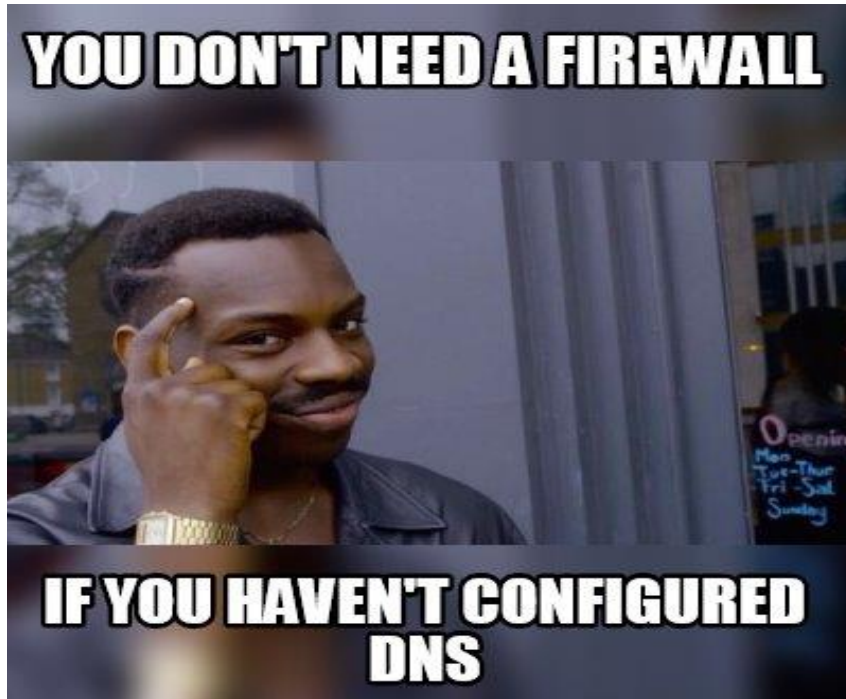
- A DNS NXDOMAIN flood DDoS attack attempts to overwhelm the DNS server using a large volume of requests for invalid or non-existent records.
- These attacks are often handled by a DNS proxy server that uses up most (or all) of its resources to query the DNS authoritative server.
- This causes both the DNS Authoritative server and the DNS proxy server to use up all their time handling bad requests.
- As a result, the response time for legitimate requests slows down until it eventually stops altogether.



Defending against attack

Managing risk of DNS attacks

Keep DNS Resolver Private and Protected



- Restrict DNS resolver usage to only users on the network and never leave it open to external users. This can prevent its cache from being poisoned by external actors.

Configure Your DNS Against Cache Poisoning

- Configure security into your DNS software in order to protect your organization against cache poisoning.
- Add variability to outgoing requests in order to make it difficult for threat actors to slip in a bogus response and get it accepted.
- Try randomizing the query ID, for example, or use a random source port instead of UDP port 53.



Securely Manage Your DNS servers



- Authoritative servers can be hosted in-house, by a service provider, or through the help of a domain registrar.
- DNS requires skills and expertise for in-house hosting, you can have full control.
- Without the required skills and scale, organisations benefit from outsourcing this aspect.

Test Your Web Applications and APIs for DNS Vulnerabilities

- Many vulnerability scanners can automatically probe DNS misconfigurations such as:
 - Direct DNS DoS Attack.
 - DNS Reflection Attack.
 - Zero-Day Vulnerability.
 - Protocol Anomalies.
 - Sloth Domain Attack.
 - DNS Tunneling.
 - DNS Hijacking – Phishing
- DNS must be within scope of any penetration test or other security audit
- Test change control and back-out procedures regularly!





Why DNS Detection and Response is Key to Reducing Cyber Risk

Srikrupa Srivatsan,
Senior Dr. of Product Marketing

BUSINESS CHALLENGES

Network Demands Have Shifted...



Multi-cloud



SaaS



IoT/OT

... Causing Strain on Security Operations

30

Security tools
used; staff and
expertise to
manage 12

\$4M

Average cost
of a data
breach

270

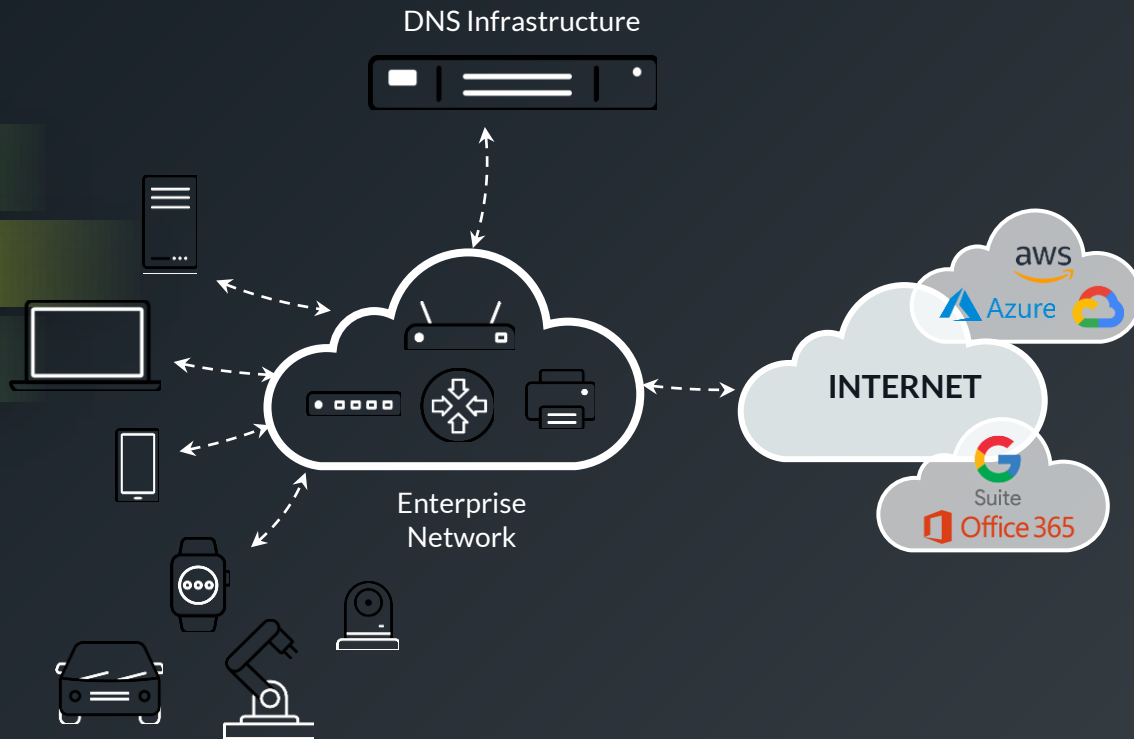
Average time
to identify and
contain

VALUE OF DNS IN SECURITY

DNS spans entire organization

Rich source of telemetry

Closest to Endpoints



EVOLVING YOUR DNS TO PROTECTIVE DNS

Protective DNS



DNS
Server



DNS Threat
Intelligence

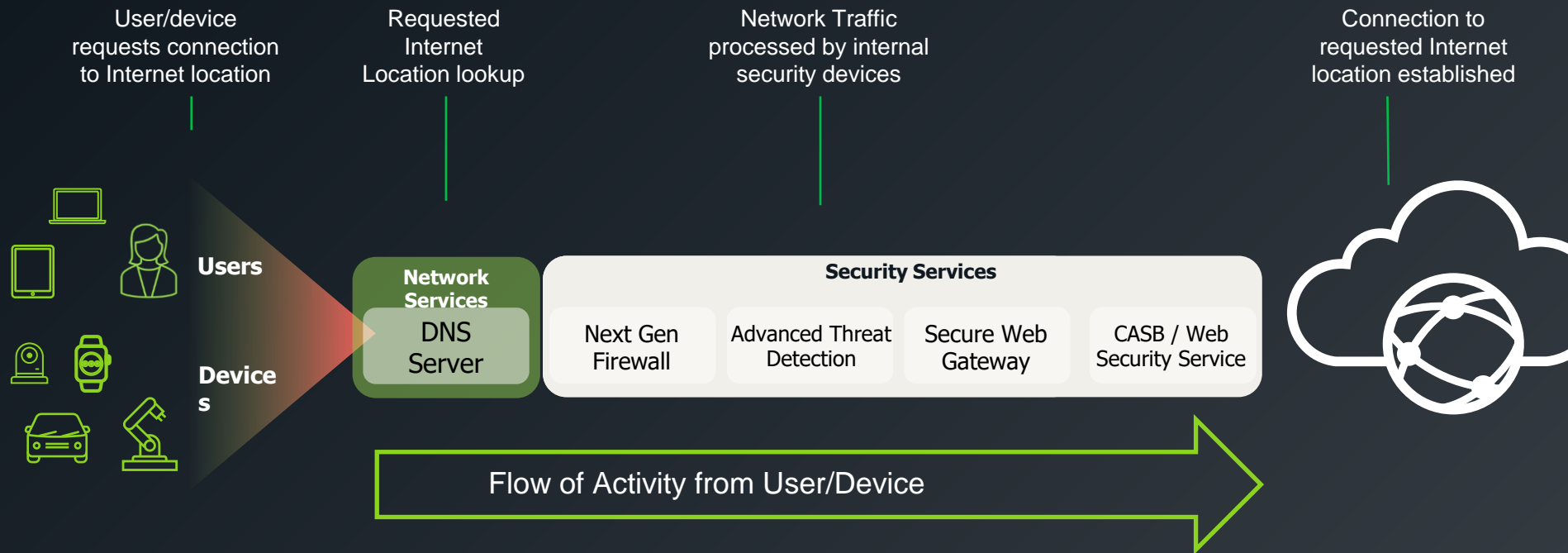


DNS-based AI/ Machine
Learning Engine



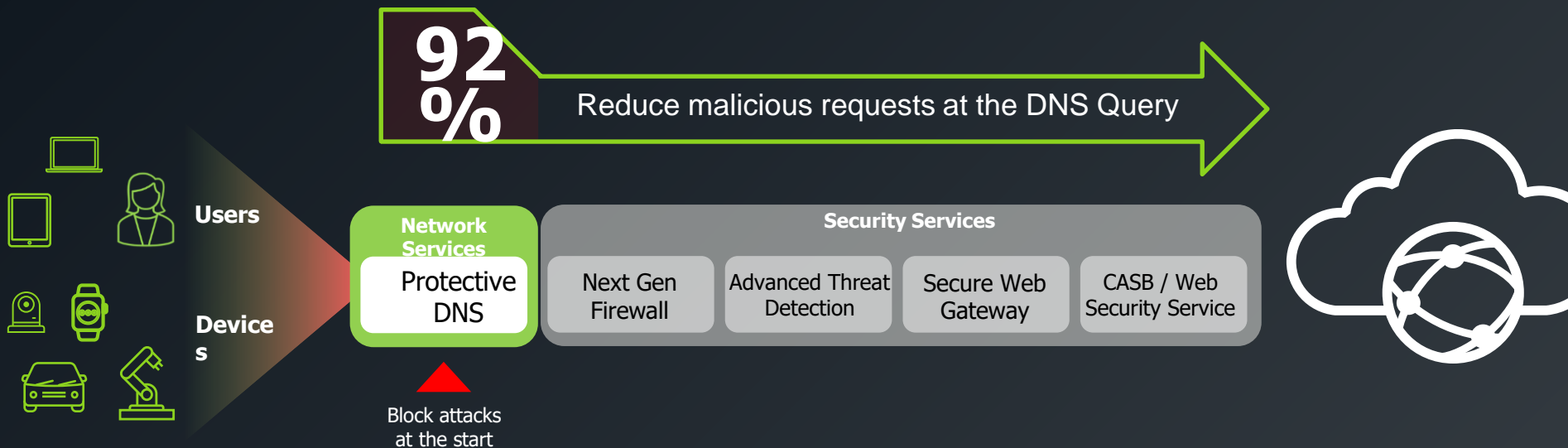
DNS Policy
Engine

STEPS IN AN ATTACK SEQUENCE

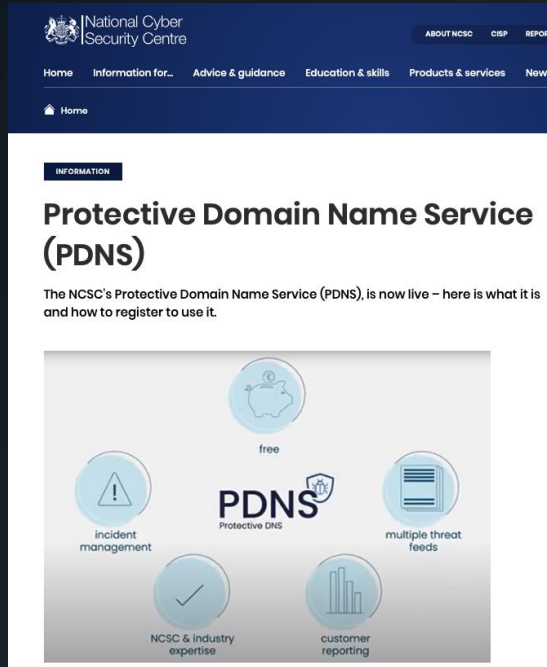


SHIFTING PROTECTION ALL THE WAY TO THE LEFT

At the earliest point with Protective DNS

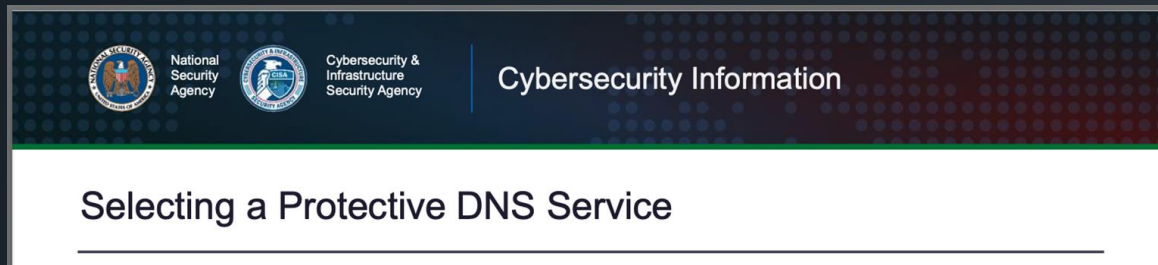


GOVERNMENTS AROUND THE WORLD EMBRACING PROTECTIVE DNS



The screenshot shows the UK National Cyber Security Centre (NCSC) website. The header includes the NCSC logo and navigation links. The main content area is titled "Protective Domain Name Service (PDNS)" and includes a brief description: "The NCSC's Protective Domain Name Service (PDNS), is now live – here is what it is and how to register to use it." Below this is a circular diagram with five icons representing features: "free" (piggy bank), "incident management" (warning triangle), "multiple threat feeds" (document with magnifying glass), "NCSC & industry expertise" (checkmark), and "customer reporting" (bar chart). The central text "PDNS Protective DNS" is prominently displayed.

UK NCSC PDNS



This banner features the logos of the National Security Agency (NSA) and the Cybersecurity & Infrastructure Security Agency (CISA). The text "Cybersecurity Information" is on the right. Below the banner, the title "Selecting a Protective DNS Service" is displayed in a large, bold font.

NSA, CISA

EC starts developing DNS internet infrastructure for 100 million people

NEWS | BROADBAND | EUROPE | 07:15 | BOOKMARK



sovereignty.

The European Commission (EC) plans to onboard 100 million people to a new EU-based DNS internet infrastructure. The DNS4EU will be developed by international consortium led by Czech company Whalebone.

The goal of DNS4EU is to provide EU citizens, companies, and institutions with a secure, privacy compliant, and powerful recursive DNS, an "address book of the internet" enabling browsing web via domain names instead of strings of numbers. The project will become a vital part of European internet

Coming soon... EU Protective DNS Services

THREAT HUNTING IN DNS

Discovering “intent to compromise”

Lookalike Domains




9uZGF5LCA.com
V2VkbmVzZ.com
TW9uZGF5LCAxc.com

DGAs (Domain
Generation Algorithms)

Data Exfiltration,
Malware Infiltration
Using DNS Responses

01100
10110



Suspicious Domains

LOOKALIKE DOMAIN PROTECTION

- **Popular Phishing:** Local users visiting global popular brands lookalikes (E.g: user going to g00gle.com)
Mitigation: Block/Alert/Ignore per policy when domain is visited.
- **Spear Phishing:** User visiting lookalikes of company's own domains/supplier's domains (E.g: user visits Infobloxbenifits[.]com)
Mitigation: Block/Alert/Ignore per policy when domain is visited.
- **Brand Reputation :** Protecting customer's own domain from harm via impersonation (E.g: using infoblocks.com to harm our customers).

Mitigation: Alerts on creation or discovery of domain.

The screenshot displays the Infoblox Lookalike Domains dashboard. The left sidebar contains navigation links: Dashboard, Manage, Policies, Reports, DNS Requests, Activity, Security, Category, Data Exfiltration, Malware, Command and Control, Summary Reports, Lookalike Domains (selected), Research, and Admin. The main content area is titled 'Lookalike Domains' and shows '123 Lookalikes Detected'. A summary card indicates 'Suspicious Lookalike Domains' at '10%' with the note 'Suspicious domains needing review'. Below this is a table of detected domains.

DETECTED	WATCHED DOMAIN	LOOKALIKE	SUSPICIOUS	SOURCE
04/14/22 01:10 am	rolex.com	rolex2sale.com		Custom
04/14/22 01:10 am	rolex.com	rolexdaytonareviews.kyz	Yes	DNS Traffic
04/14/22 01:10 am	rolex.com	188833rolex.com		Custom
04/14/22 01:10 am	rolex.com	rolexautopecas.com		Custom
04/14/22 01:10 am	rolex.com	rolex88.net		DNS Traffic
04/14/22 01:10 am	rolex.com	trolex.com		Custom
04/14/22 01:10 am	rolex.com	rolexinstitute.us	Yes	DNS Traffic



FROM PROTECTIVE DNS TO DNS DETECTION AND RESPONSE



GREATER SECOPS VISIBILITY & CONTEXT

Quick and easy **device and user attribution using** IPAM/DHCP for faster **response**



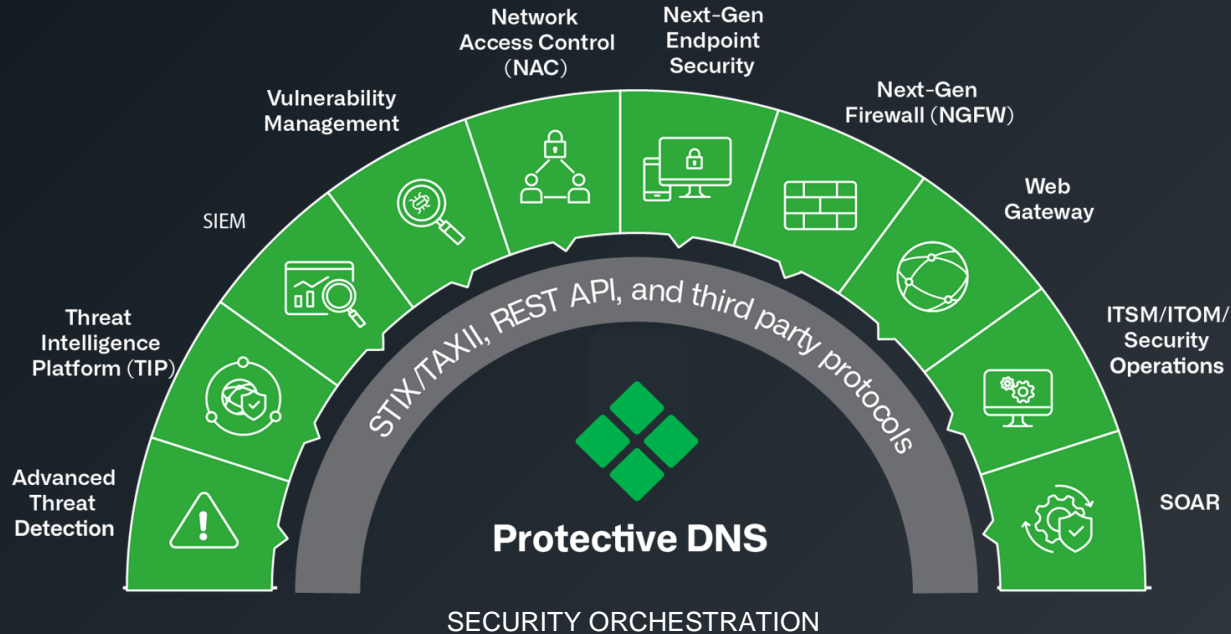
Security event
Source IP address: 198.18.197.61

VS.



Security event: DATA EXFILTRATION
Threat level - Medium
Source IP address: 198.18.197.61
MAC ID: aa.bb.cc.dd.ee.ff
Username: Adam Smith
Fingerprint: Windows 11
Location: Las Vegas Encore
VLAN: 144

RESPONDING QUICKLY WITH ECOSYSTEM



US PUBLIC ENERGY AND WATER UTILITY

Realized significant improvement in MTTR – a critical KPI

Why change from status quo

- SOC spending several hours identifying user associated with IP when there is a security event
- Wanted to break away from “Black box” approach of blocking with no context

DNS Detection and Response Benefits

- Username, device attribution at touch of a button
- Track users as they moved from IP to IP
- Immediately actionable context on threats blocked
- DDI data in Splunk dashboards for easy analysis



SUMMARY - DNS DETECTION AND RESPONSE KEY CAPABILITIES

Identify	Mapping DNS queries to user/device activity using IPAM DNS based Application discovery
Protective DNS	Block phishing, ransomware, malware C&C, DGA, data exfil Content filtering Protect any system anywhere including IoT/OT DNSSEC Customizable policies
Detection	Threat intelligence for detecting communications to known malicious sites DNS threat hunting to detect suspicious domains, emergent domains AI/ML analytics on DNS queries for detecting DGAs, data exfil Lookalike domain detection
Response	Automating remediation actions via ecosystem integrations Automated sharing of DDI data to SOC tools for triage/correlation Easy view of impacted systems in the network Context on IOCs to prioritize threats that pose the most risk



Thank you!

Questions?

Submit questions to the presenters via the on-screen text box



Jonathan Care
Advisor
Lionfish Tech
Advisors



Srikrupa Srivatsan
Director of Product
Marketing
Infoblox



Becky Bracken
Editor
Dark Reading

Thank you for attending

Please visit our sponsor and access any of the resources featured in the resource section of the attendee console.

