infoblox | DARKREADING

Why successful security professionals need to leverage DNS

40 years after DNS was first established, attacks are on the rise.

88% Organizations were victimized by attacks that leverage DNS from 2021-2022

70% Experienced application downtime as a result

92% Attacks that can be prevented with DNS[1]

Defending the DNS attack surface is not simple.

Because DNS relies on implicit trust,

Attackers can deny the use of DNS to legitimate users or services, causing general application or network outage

Attackers can manipulate and falsify the DNS lookup response to misdirect clients to malicious destinations

> **"Once the attacker is controlling the communication, you see the criminal and malicious opportunities are almost boundless"**
>
> Steve Benton, VP of Threat Research, Anomali

Malware increasingly exploits DNS.

$942,000
The average cost of a successful attack that leverages DNS[2]

The tactic

Because DNS is a trusted protocol used to publish critical information, today's attackers increasingly use it to:

Bypass most defenses due to little to no DNS visibility

Exfiltrate valuable data or infiltrate malicious code

Avoid detection of C2 or other communications

The defenses

Resolution blocking: Use DNS Response Policy Zones (RPZs) to prevent the malicious domain from resolving to an IP address

Response substitution: RPZs can also be used to replace the malicious IP address in the DNS response with a different IP address

The Case of WannaCry Ransomware

Impact

Hundreds of thousands of computers in 150+ countries in 2017

Strategy

Exploited weakness in Microsoft's Server Message Block (SMB) to infect the victim, encrypt files, and spread to other devices in the network

Role of DNS

WannaCry used DNS to avoid detection by trying to resolve a nonexistent domain name to identify sandboxes from real networks

Defense

The DNS Kill Switch: By registering the malware domain and providing valid DNS lookup results, the spread was stopped

Lookalike domains are on the rise.[3]

300,000
The number of lookalike domains Infoblox identified from January of 2022 to March of 2023[4]

70+ Billion
The number of DNS events Infoblox analyzes daily to identify new threats

The tactic

- Lookalike domains are domain names that appear similar or nearly identical to a legitimate domain
- Phishing, SMSishing, and other attacks use lookalike domains to fool defenses, gain end user trust, and trick investigators
- Victims no longer face fake brand name domains, but are increasingly targeted by domains impersonating the supply chain or other trusted partners

The defense

Response Policy Zone (RPZ)

- Using RPZs allows DNS queries to flow unimpeded to legitimate domains while blocking access to malicious ones
- RPZ is an open standard that defines a specific DNS zone type that contains security policy actions mapped to domain names

> **"There have always been and probably always will be some bigger targets, such as banks, pharmaceuticals and anything related to industrial systems, but the bottom line is: everyone is a target."**
>
> Gary Cox, Technical Director for Western Europe, Infoblox[5]

Common Lookalike Attacks

Phishing

Because many users will not pay close attention to subtle differences in domain names, today's attackers use similar looking lookalike domains to trick people

Example: gmail.com

gmial.com
transpose letters "a" and "i"

gmai1.com
substitute letter "l" with number "1"

With the emergence of Internationalized Domain Names (IDNs), the non-ASCII character sets available have made it possible to create nearly indistinguishable lookalike domains

Example: google.com

google.com (Cyrillic O)
google.com (Green Omicron)

Business Email Compromise (BEC)

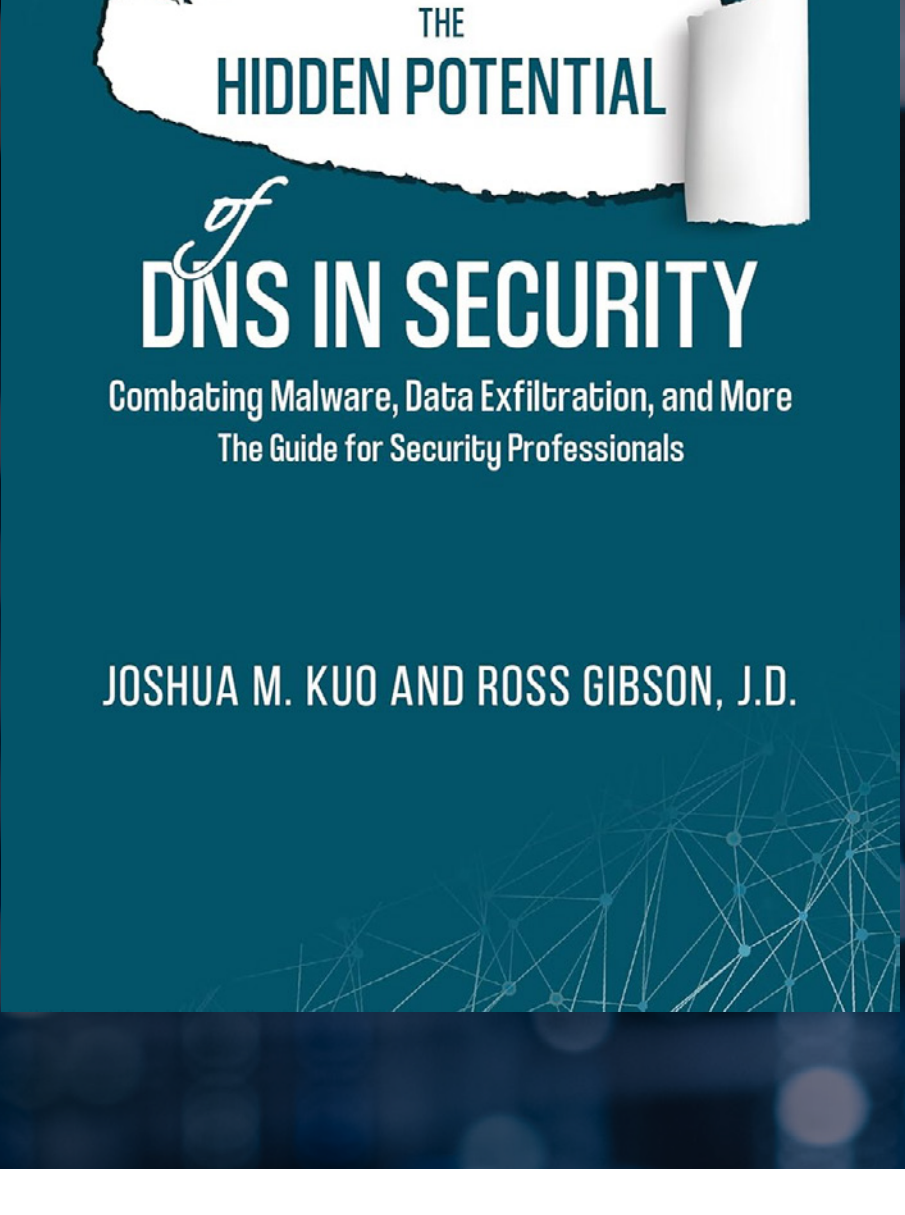
Attackers register lookalike domains imitating real businesses

They then send victims email communications impersonating legitimate businesses to trick their victims into making costly mistakes

$1.8 billion
The financial loss to businesses due to BECs in 2020

Find out how to protect your organization ›

The Hidden Potential of DNS in Security



infoblox | DARKREADING

1. ExecutiveGov, "Anne Neuberger on NSA's Secure DNS Pilot Program", 2020
2. Dark Reading, "Everything You Need to Know about DNS Attacks", 2023
3. Infoblox, "Lookalike domain attacks are on the rise. Be on the lookout for these four types.", 2023
4. A Deep3r Look at Lookal1ke Attacks, Infoblox, 2023
5. #InfosecurityEurope: New Study Takes a Deep Dive Into Lookalike Attacks, Infosecurity Magazine, 2023