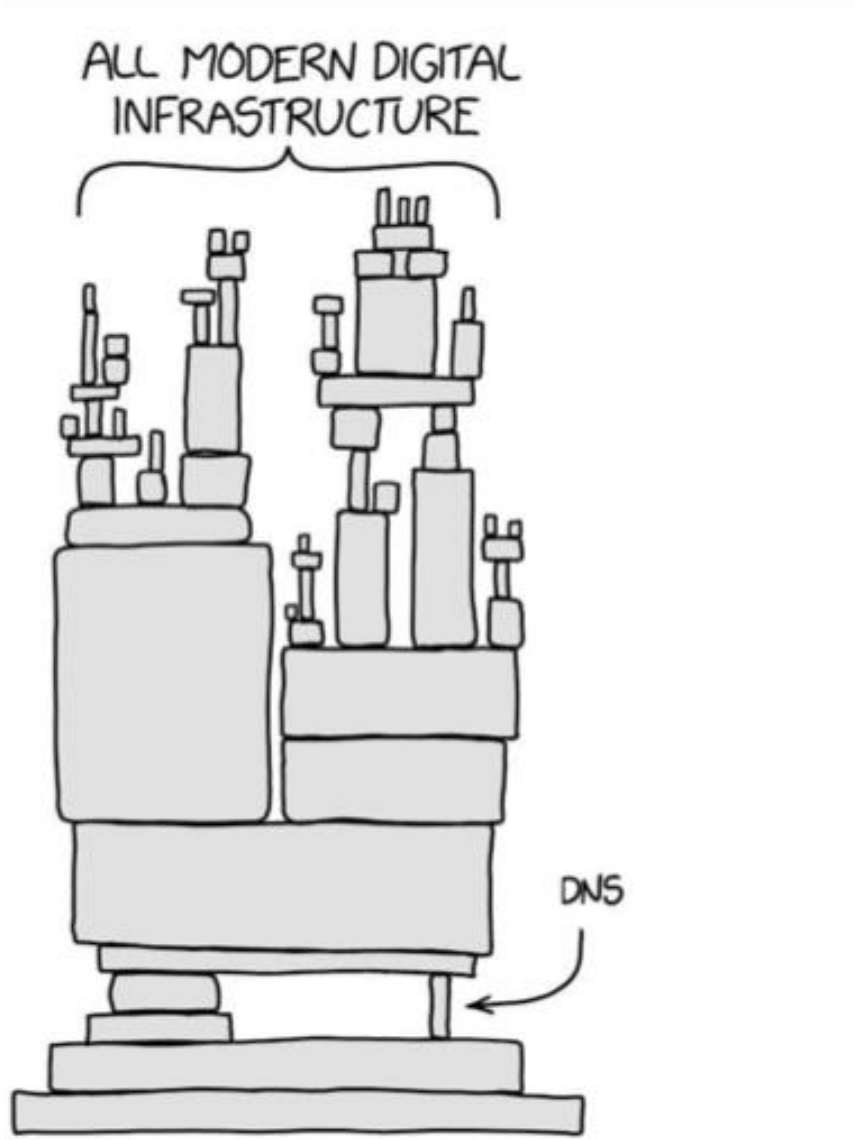
DNS
and Compliance

Prepared by: John Mutama

April 2024

ISACA
Kenya Chapter



ISACA
Kenya Chapter

The DNS Gap – A Multi Dimensional Threat Vector

Making Your Infrastructure Work Against You

78%
DNS: most common application layer attacks[1]

84%
Of reflection/amplification attacks use DNS[1]

>$500
Per min cost of downtime due to DDoS attack[2]

$1.5M
Average cost per year to deal with DNS attacks[2]

The Leading Culprit in Data Exfiltration

$4M
Average consolidated cost of a data breach[3]

46%
% of survey respondents that experienced DNS data exfiltration[4]

45%
% of survey respondents that experienced DNS tunneling[4]

APT/Malware Proliferation Rooted in DNS

91%
Of malware uses DNS to carry out campaigns[5]

431M
New unique pieces of malware in 2015[6]

#1
Malware C&C is #1 responsible vector for crimeware[7]

Ineffective Threat Intelligence

70%
of survey respondents that felt Threat Intel is not timely[8]

46%
% of survey respondents unable to prioritize the threat by category[8]

45%
% of survey respondents lacked context for threat intel to make it actionable[8]

1. Arbor WISR2016 Report
2. Ponemon Institute Study – The Cost of Denial-of-Service Attacks. March 2015\
3. Source: Ponemon Institute, 2016 Cost of Data Breach Study
4. Source: *SC Magazine*, Dec 2014, "DNS attacks putting organizations at risk, survey finds"
5. Source: Cisco 2016 Annual Security Report
6. Symantec 2016 Internet Security Threat Report
7. Verizon 2016 Data Breach Investigations Report
8. Source: Ponemon Institute, 2015 Second Annual Study on Exchange Cyber Threat Intelligence

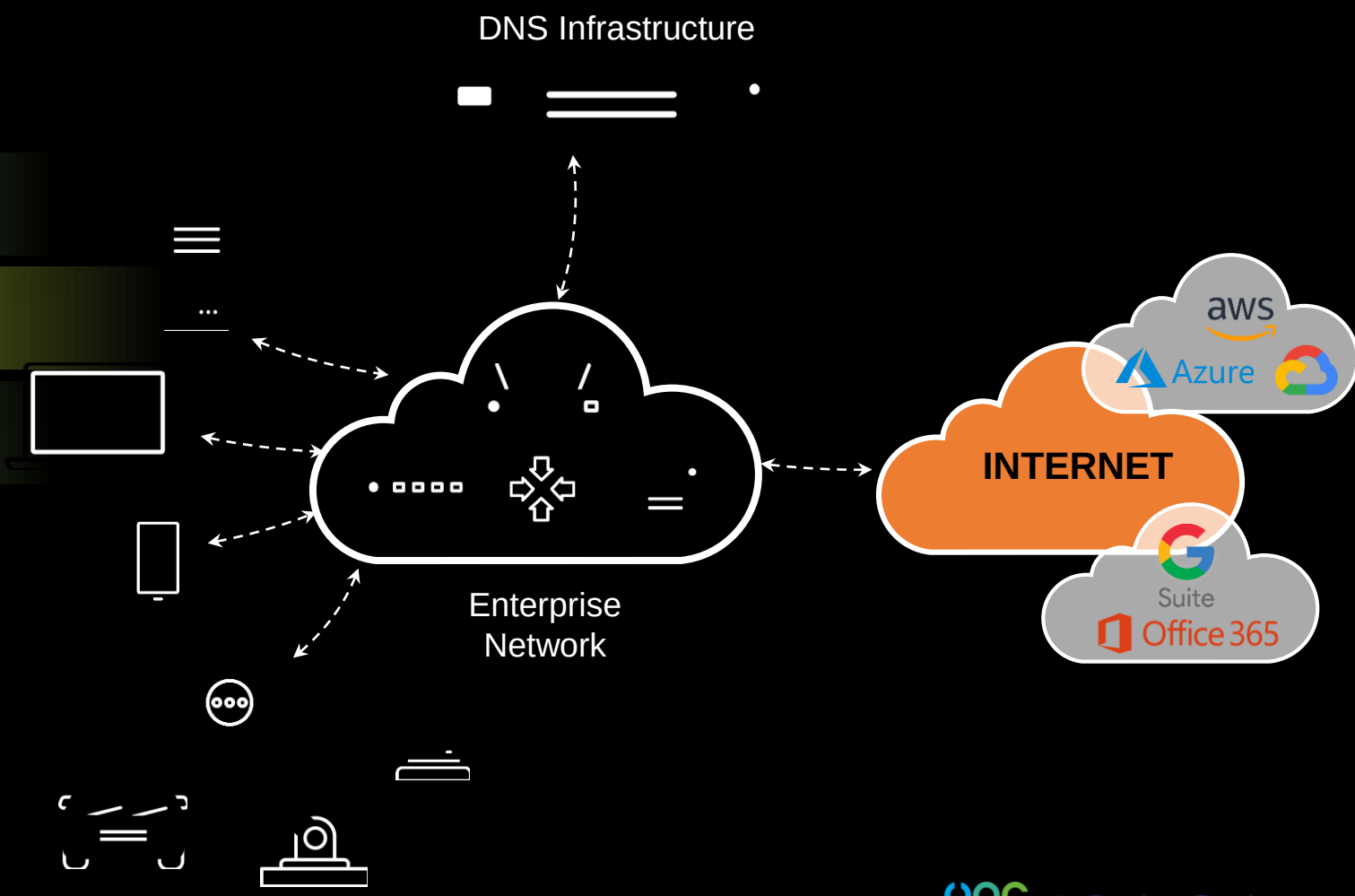
ISACA Kenya Chapter

VALUE OF DNS IN SECURITY

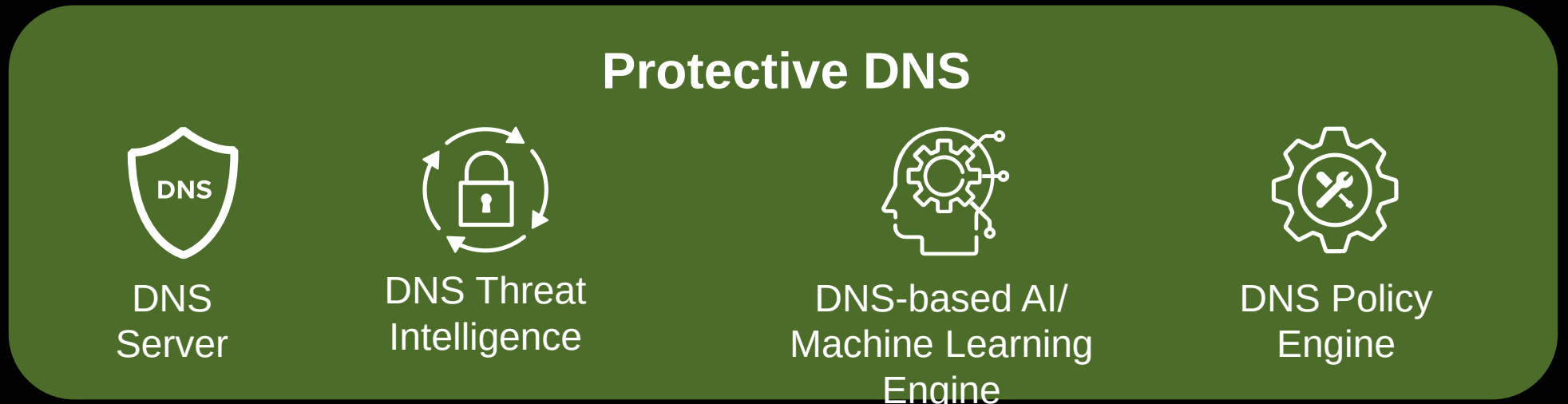
DNS spans entire organization

Rich source of telemetry

Closest to Endpoints



EVOLVING YOUR DNS TO PROTECTIVE DNS



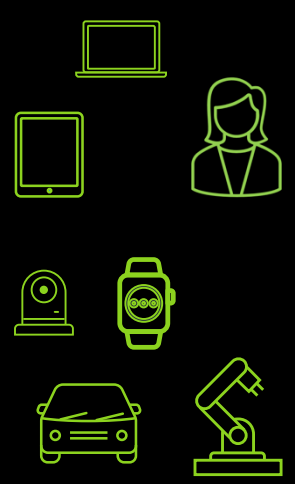
STEPS IN AN ATTACK SEQUENCE

User/device requests connection to Internet location

Requested Internet Location lookup

Network Traffic processed by internal security devices

Connection to requested Internet location established



Users

Devices

Network Services

DNS Server

Security Services

Next Gen Firewall

Advanced Threat Detection

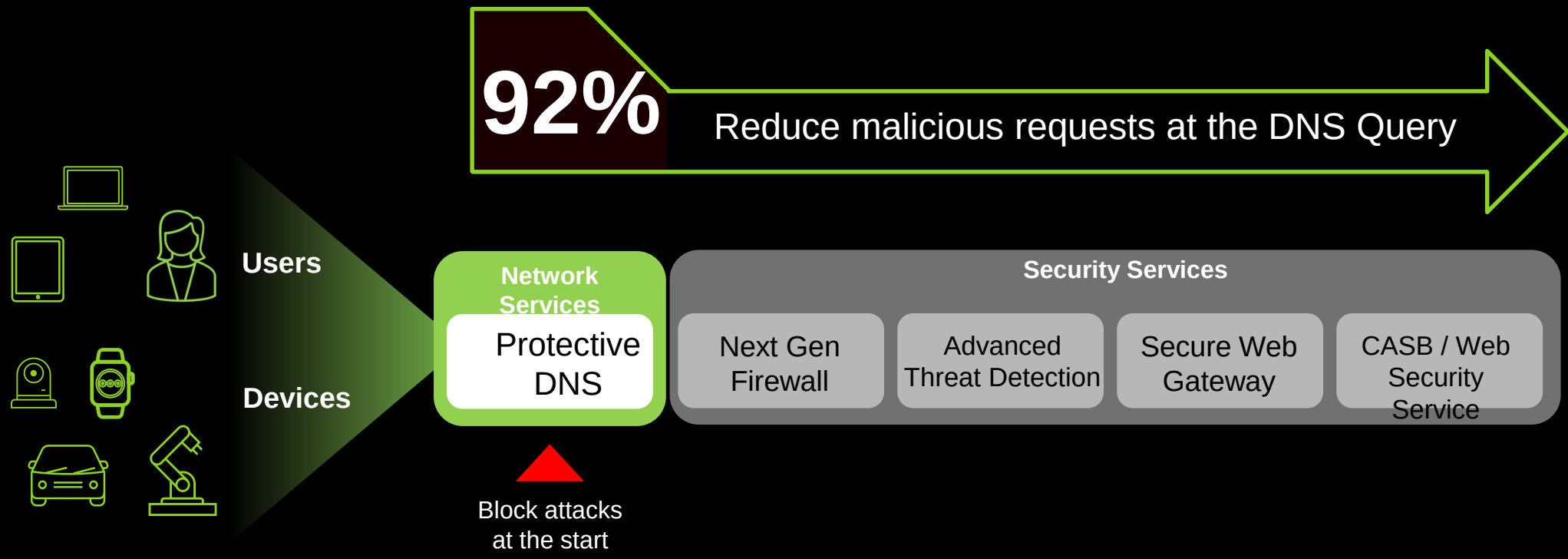
Secure Web Gateway

CASB / Web Security Service

Flow of Activity from User/Device

SHIFTING PROTECTION ALL THE WAY TO THE LEFT

At the earliest point with Protective DNS



ISACA Kenya Chapter

infoblox

National Cyber Security Centre

ABOUT NCSC CISP REPOR

Home Information for... Advice & guidance Education & skills Products & services New

Home

INFORMATION

Protective Domain Name Service (PDNS)

The NCSC's Protective Domain Name Service (PDNS), is now live – here is what it is and how to register to use it.

National Security Agency

Cybersecurity & Infrastructure Security Agency

Cybersecurity Information

Selecting a Protective DNS Service

EC starts developing DNS internet infrastructure for 100 million people

NEWS | BROADBAND | EUROPE | 07:15 | BOOKMARK

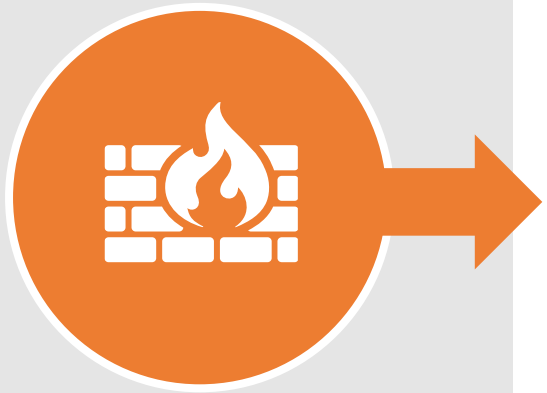
The European Commission (EC) plans to onboard 100 million people to a new EU-based DNS internet infrastructure. The DNS4EU will be developed by international consortium led by Czech company Whalebone.

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 sovereignty.

ISACA Kenya Chapter

Defense-in-Depth and DNS Security Gap

Prevention/detection with standard technologies is hard



Firewalls and IDS/IPS devices DO NOT effectively address DNS security threats

SECURITY GAP

Security gap exists between time malware initiates communication via DNS and first time a traditional firewall inspects client web traffic

A **DNS security layer is needed** in addition to firewalls, IDS/IPS, anti-virus, etc. to fill gap

ISACA Kenya Chapter

Defense-in-Depth and DNS Security Gap

Reputation

Detect & prevent communications to malware, C2, ransomware

Government-grade threat intelligence

Ecosystem

Signature

Infrastructure protection for critical core services

Carrier-grade deep packet inspection

Instant identification of popular tunneling tools

Behavior

Patented streaming analytics technology

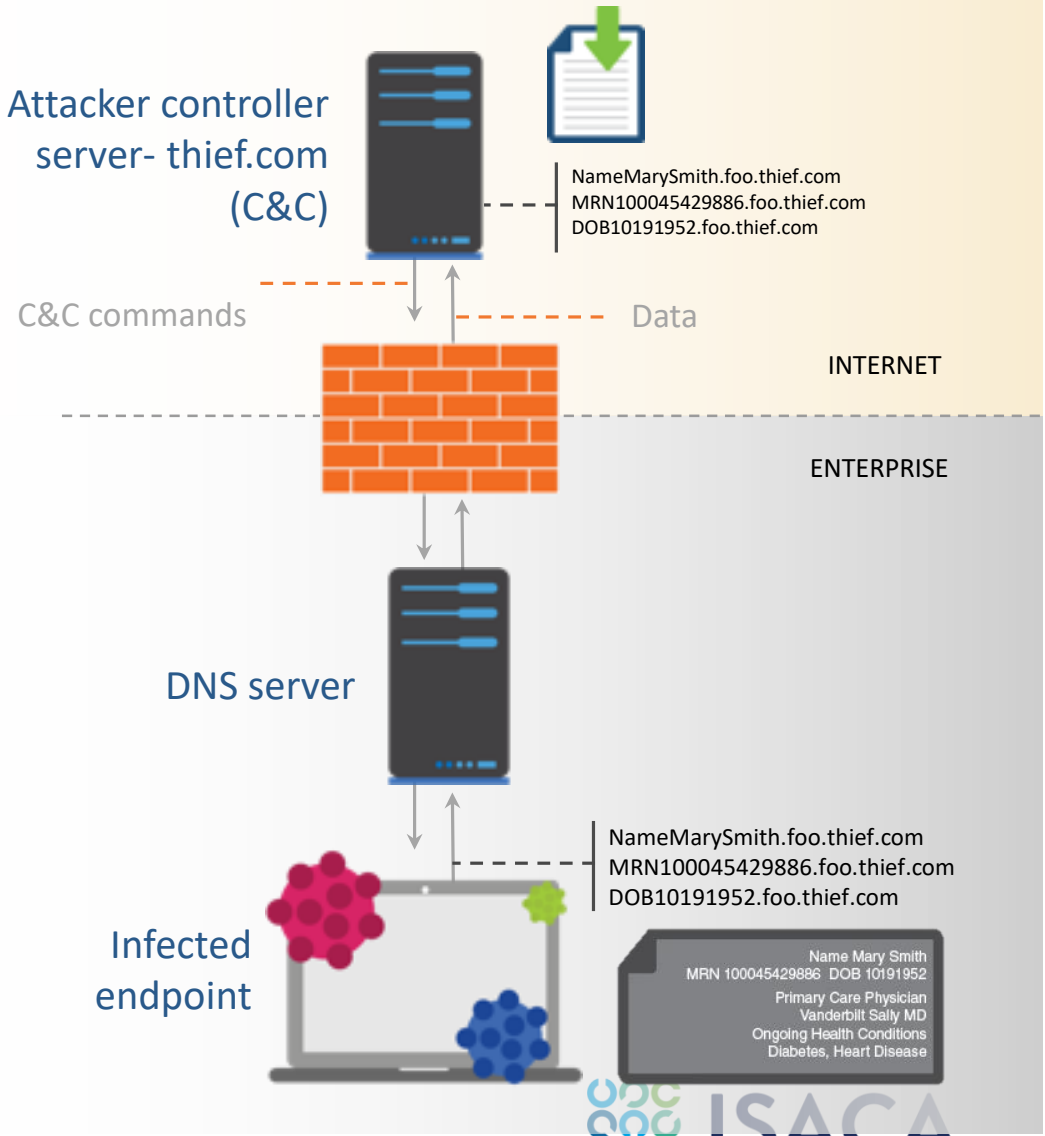
Detect & prevent data exfiltration

”Machine learning”

ISACA Kenya Chapter

Involves at least the following MITRE ATT&CK techniques

- Command and Control
  - Commonly Used Port, Custom Command and Control Protocol, Custom Crypto Protocol, Data Encoding, Data Obfuscation
- Exfiltration
  - Automated Exfiltration, Data Encrypted, Data Transfer Size Limits, Exfiltrate over Command and Control Channel, Scheduled Transfer



Chinese Hackers Using **42,000 Imposter Domains** in Massive Phishing Attack Campaign

The Hacker News, Nov 17, 2022

ISACA Kenya Chapter

infoblox

NIST FRAMEWORK

Guidelines published by Natl. Institute of Standards & Technology used for mitigating Cybersecurity risks

Category	DNS is Foundational & works across entire Cybersecurity Lifecycle
IDENTIFY	• Core DDI – Single source of truth for identification of network assets • DHCP Fingerprinting- Maps IP to MAC/OS to identify BYOD devices in real-time & w/ addl. infrastructure (operationally efficient) • Network Insight – Automated device discovery
PROTECT/ DETECT	• Threat Insight Engine- uses ML to detect & block Day 0 DNS APT's (DNS Data Exfil, DNS-T, DGA's) • Diversified set of Reputational Threat Feeds (Domains, URLs, IPs) • ADP (DDOS Protection) protects DNS Server Infrastructure
RESPOND/ RECOVER	• DDI Context for faster & more accurate IR (Who, What, Where) • DOSSIER- Threat Intel tool for faster Incident Response by investigating known bad or suspicious Domains • Ecosystem Mitigation- forwards DDI Context + Threat Intel across the entire Security Arch (NGFW, NAC, Endpoints, SIEM)

ISACA Kenya Chapter

MITRE ATT&CK FRAMEWORK (v10)

14 Attacker tactics (Goals) & 188 techniques (Methods) based on real-world observations

Initial Access: Spam w/ Phishing links is a common technique used to penetrate networks & launch RW. B1TD blocks MW connection when a user clicks.

C&C: Once infected, MW calls C2 to get instructions. C2 is a Tactic & DNS is a commonly used Protocol & Technique. B1TD block C2 connections.

Exfiltration: B1TD uses ML Models to block DNS Data Exfil attempts based on recognizing anomalous strings of data within the DNS Query. These Day Zero DNS APT's are dynamic & typically evade traditional layers.

Enterprise Matrix

The full ATT&CK Matrix™ below includes techniques spanning Windows, Mac, and Linux platforms and can be used to navigate through the knowledge base.

Last Modified: 2019-07-01 17:29:19.726000

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical

MITRE ATT&CK™

ISACA Kenya Chapter

Lookalike Domain Detection

paypal.com	pąypąl.com	paypal.com	Text
xn--pypl-53dc.com	xn--pypl-btac.com	paypal.com	Punycode

google.com	google.com	google.com	Text
google.com	xn--ggle-0nda.com	xn--ggle-55da.com	Punycode

ISACA Kenya Chapter