Infoblox DNS Threat Insight & DNS Firewall
Time to control DNS – for You, for Your subscribers and Your users!

Adam Obszyński

CEE SE, Infoblox Inc.

Agenda

DNS Basics
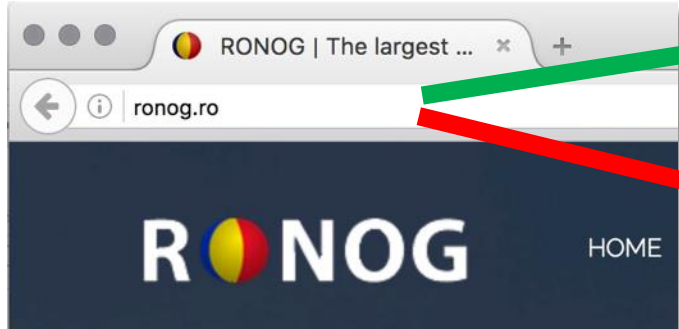
DNS Security Challenges

Infoblox DNS Firewall Solution

Infoblox DNS Threat Analytics

DNS?


```
;; ANSWER SECTION:
ronog.ro.                 21599    IN      A      195.95.178.25
```

RONOG | The largest ...

ronog.ro
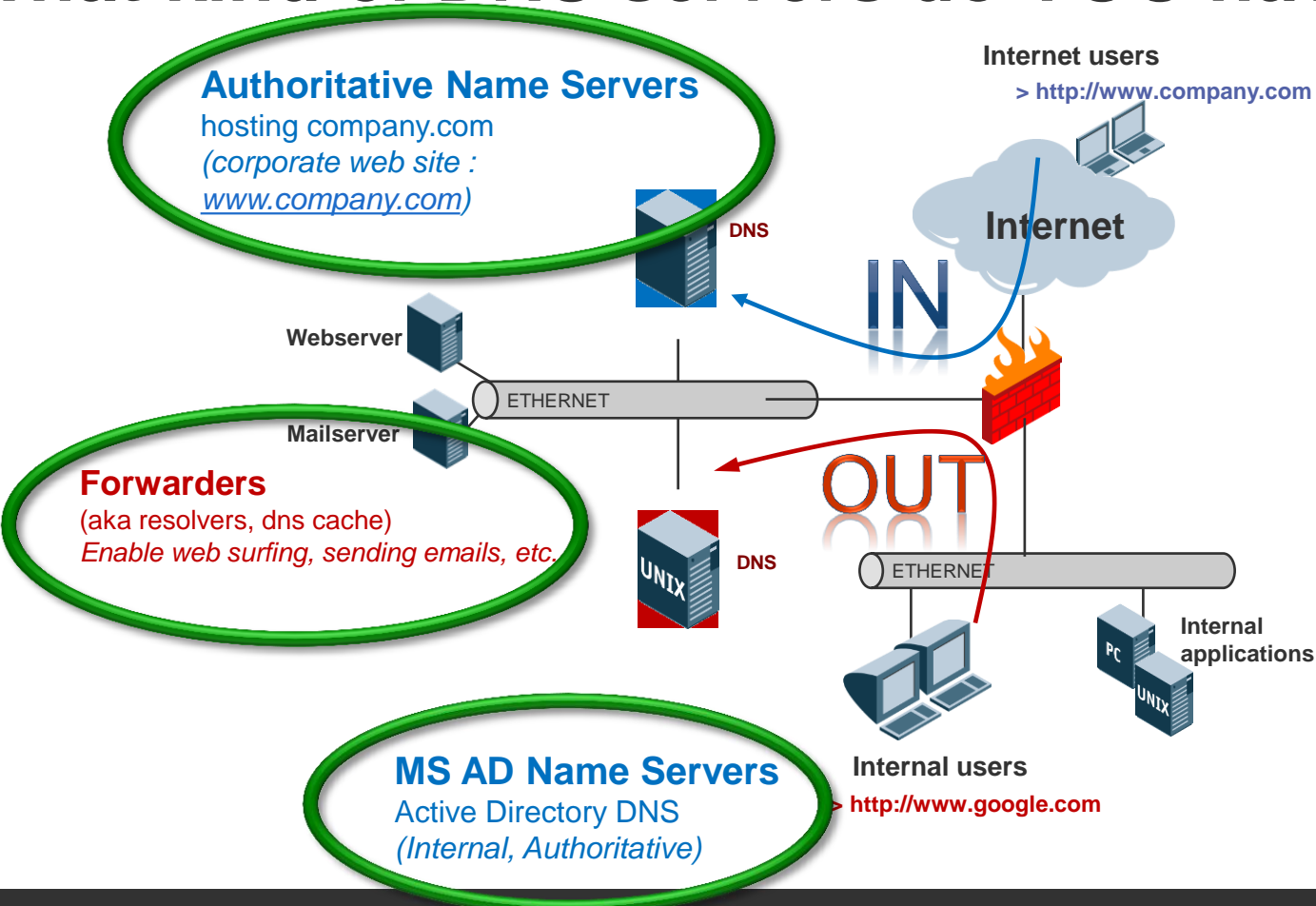
R **NOG**   HOME

ⓘ Server not found

Firefox can't find the server at www.ngsec.eu.

- Check the address for typing errors such as **ww**.example.com instead of **www**.example.com
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

Try Again

Infoblox

What kind of DNS servers do YOU have?

Authoritative Name Servers
hosting company.com
(corporate web site :
www.company.com)

Internet users
> http://www.company.com

Internet

DNS

IN

Webserver

ETHERNET

Mailserver

Forwarders
(aka resolvers, dns cache)
Enable web surfing, sending emails, etc.

OUT

UNIX DNS

ETHERNET

Internal applications

PC UNIX

MS AD Name Servers
Active Directory DNS
(Internal, Authoritative)

Internal users
> http://www.google.com

Infoblox

Why Securing DNS is Critical

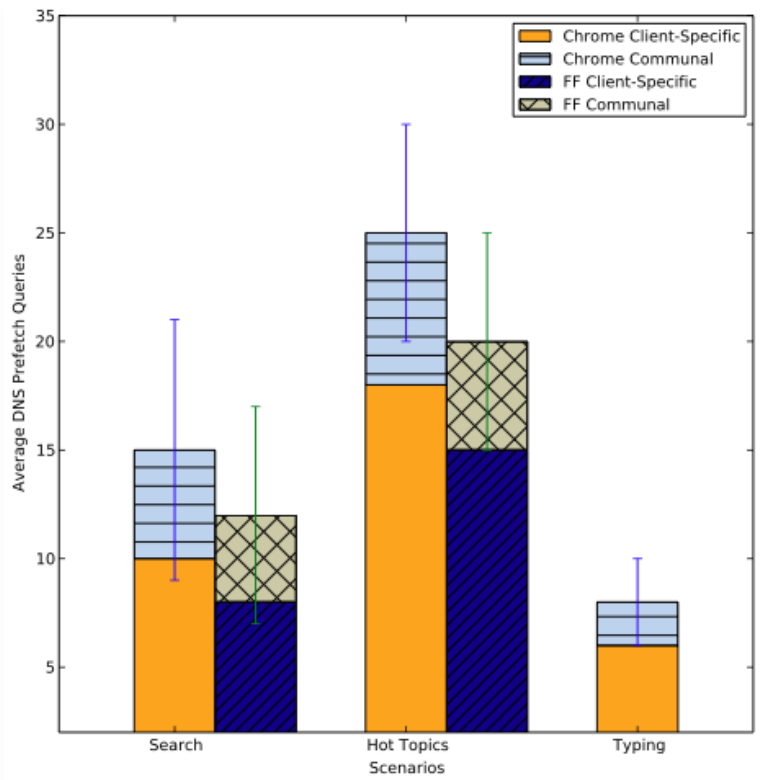DNS is critical networking infrastructure

DNS protocol is easy to exploit and attacks are prevalent

Traditional security is ineffective against evolving threats

Unprotected, DNS increases risk to critical infrastructure and data

Infoblox

Web Prefetching

© Srinivas Krishnan and Fabian Monrose
Department of Computer Science University of North Carolina at Chapel Hill

Web 9.0 and DNS – Sample
Fast Web Performance Starts with DNS…

DNS (ms)

- http://techcrunch.com/
  - 300 objects++
  - 60++ domains

© http://blog.catchpoint.com/
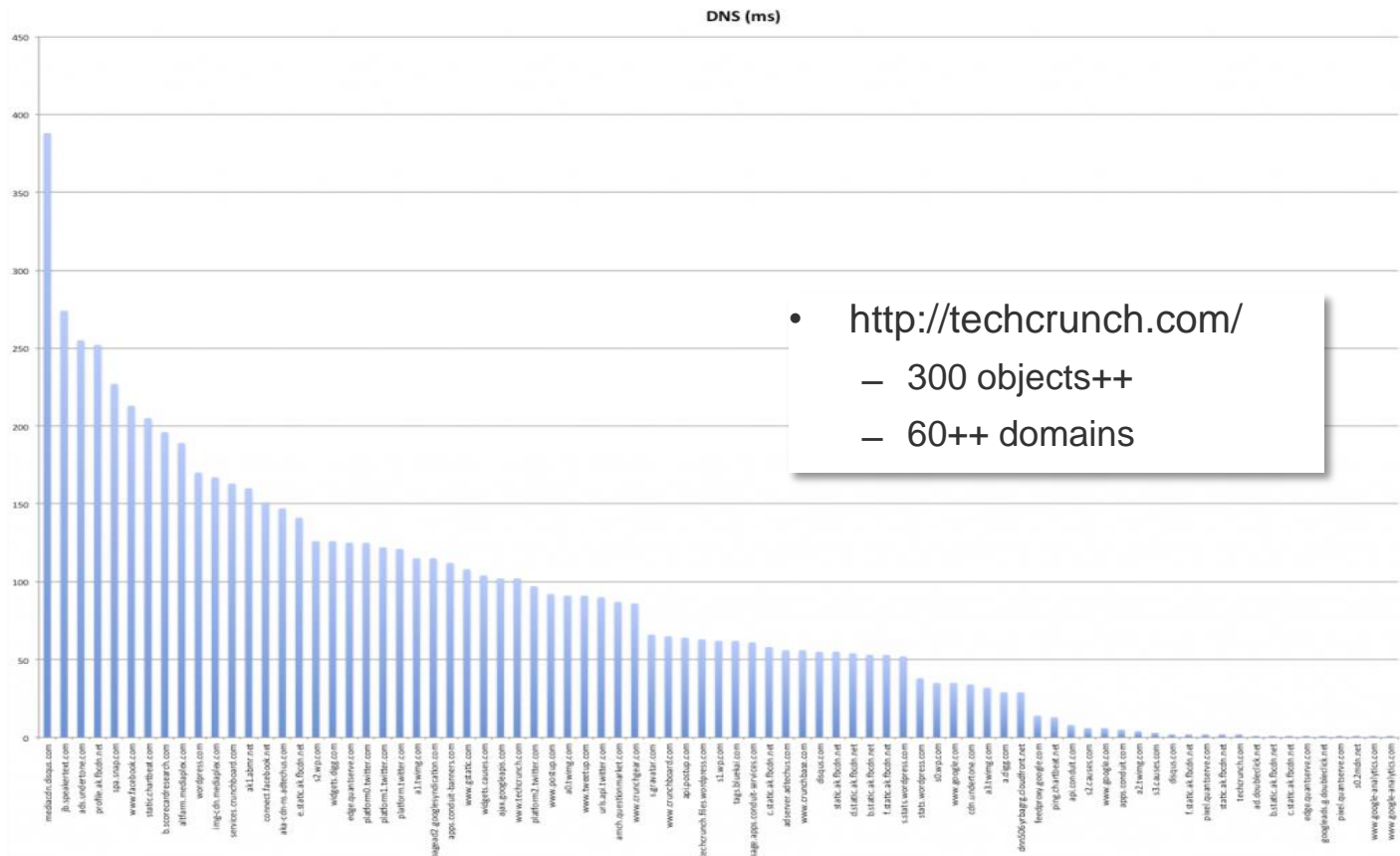
Web 9.0– Sample 2
Web Starts with DNS…
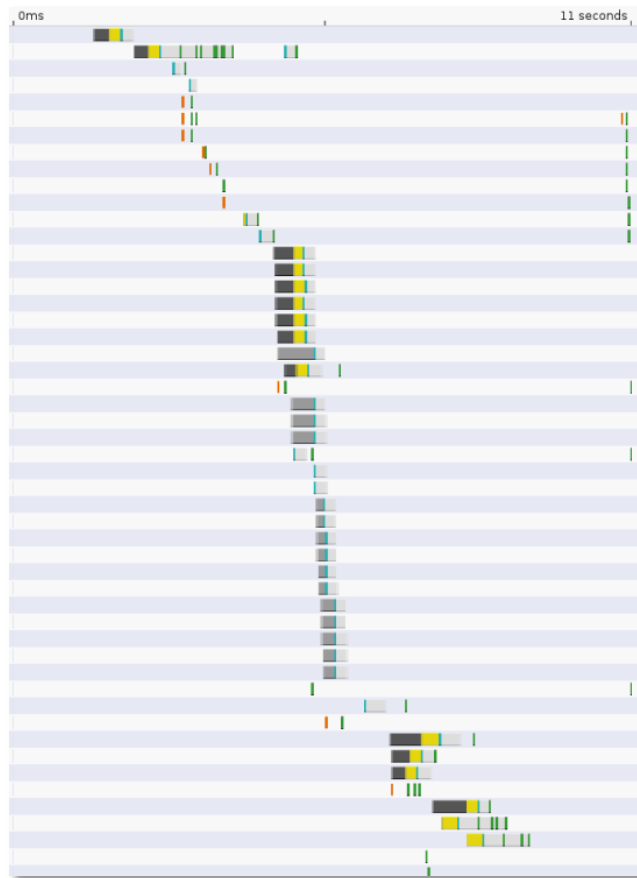
- Two components to DNS latency:
  - Latency Client <-> Server
  - Caches <-> name servers
    - Cache misses
    - Under provisioning
    - Malicious traffic

© https://developers.google.com/

Malware Exploiting DNS

- Over 91% percent malware uses DNS
  - To gain command and control
  - To exfiltrate data
  - To redirect traffic
- Despite adversaries' reliance on DNS, few organizations are monitoring DNS
- Crimeware attacks rely primarily on Malware C&C communications via DNS
- Average total cost of data breach ~$3.8M USD
- The question isn't if, but when you will be attacked, and how effectively you can respond

Source: Cisco 2016 Annual Security Report

Infoblox

Figure 13. Monitoring Threats from Recursive DNS

DNS

91.3%
of malware uses
DNS in attacks

68%
of organizations
don't monitor
recursive DNS

Source: Cisco Security Research

Cisco 2016
Annual Security Report

Motion of Malware through Networks: "PIE"

APT/malware uses DNS at every stage

P Penetration Query malicious domains and report to C&C	**I** Infection Download malware to the infected host	**E** Exfiltration Transport the data offsite

DNS server

Infoblox
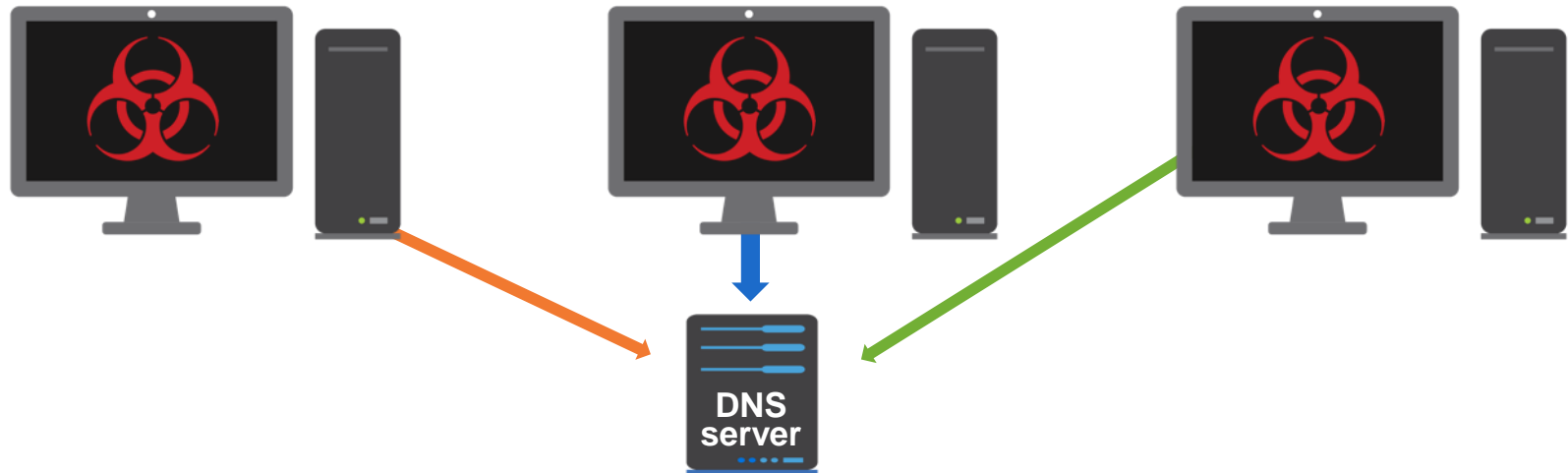
Malware Exploiting DNS - Examples

Ransomware - CryptoLocker

- Targets Windows-based computers in form of email attachment
- Upon infection, uses DNS for callback to C&C server and attain encryption software
- Encrypts files on local hard drive and mapped network drives
- If ransom isn't paid, encryption key deleted and data irretrievable

Financial and Banking Malware/Trojans also use DNS

- **GameOver Zeus (GOZ)**
  - 500,000 – 1M infections globally and100s of millions of dollars stolen
  - Takes control of private online transactions and diverts funds to criminal accounts
- **Dyre**
  - As of Q1-2015, 125% increase of DYRE-related infections worldwide vs. a year ago
  - Dyre exploits top 3 Windows-based web browsers to steal credentials using MITB techniques
- **Poseidon**
  - In early 2015, Cisco publicized this, new form of point-of-sale (POS) malware
  - Builds upon previous Trojans like Zeus and BlackPOS that affected retail stores like Target and Home Depot.

Malware Exploiting DNS - Examples

Wiper malware
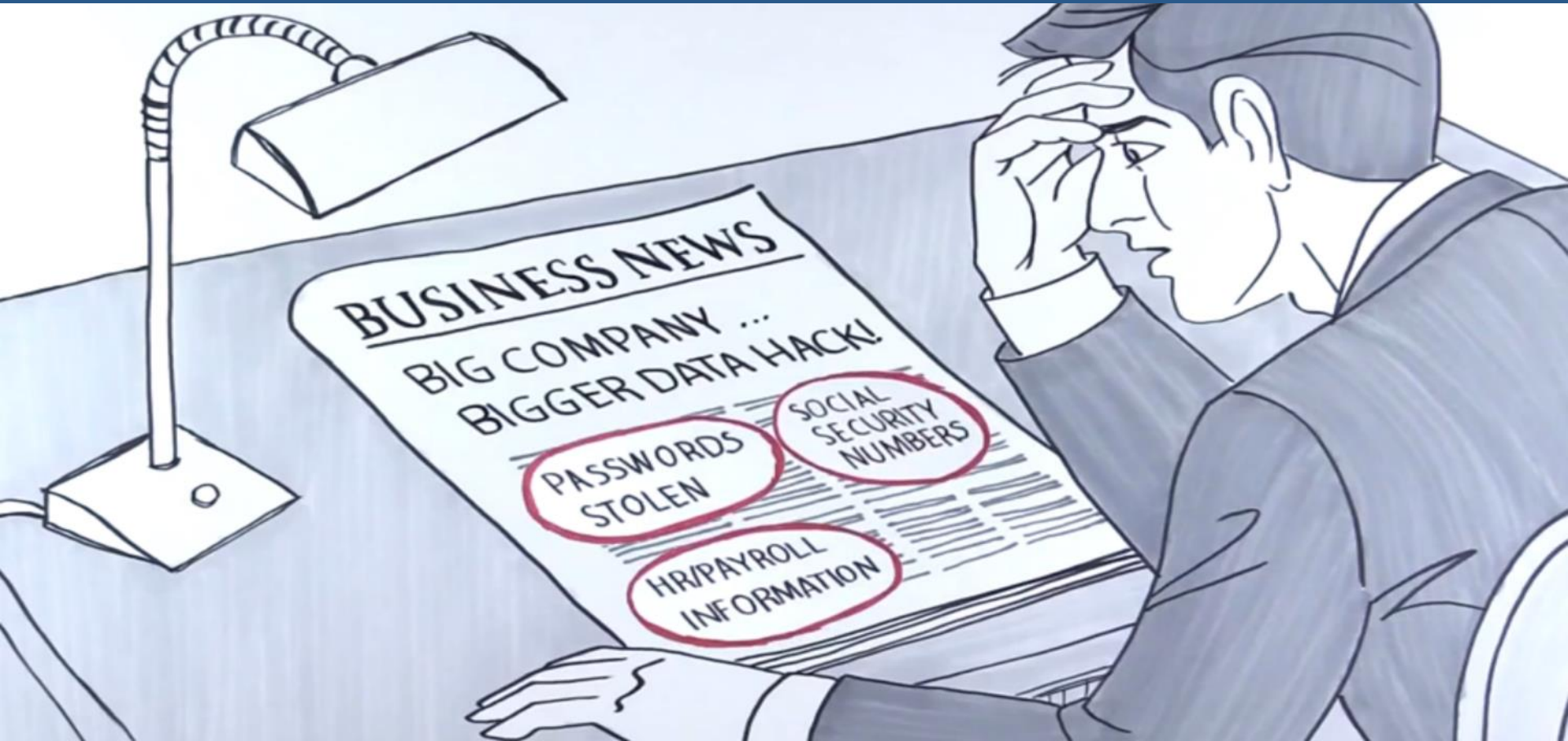
- Targets Windows-based servers by exploiting network file shares
- "Dropper" installs itself as a Windows service when executed
- Attempts to connect to C&C network – requires DNS callbacks
- Accesses the hard drive, exfiltrates data, and wipes all content

Infoblox

DNS Examples - Malware

Infoblox

Malware

Few queries:
dig lovemydress.pl
dig brt2014.com
dig all-that-and-more.net

DEMO Topology
We are safe…

Bartender
:-)

Source

MacGyver

INFOBLOX
DNS Firewall

192.168.1.244

The EVIL one:
INTERNET

Malware

Few queries:
dig lovemydress.pl
dig brt2014.com
dig all-that-and-more.net

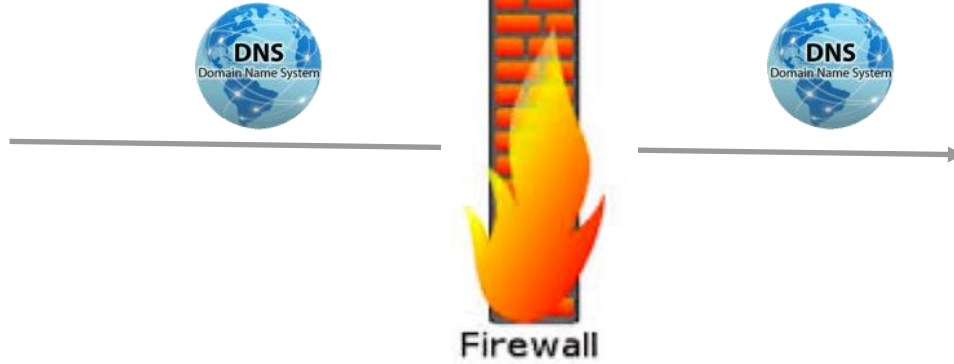| Host	Domain	URL	Detected	Received	Up	Class	Property	Type	Profile
lovemydress.pl	lovemydress.pl	http://lovemydress.pl/wp-content/themes/sketch/csys.php	2016-03-15T15:25:...	2016-03-15T15:25:...	true	MalwareC2	MalwareC2_Teslacrypt	HOST	IID
lovemydress.pl	lovemydress.pl		2016-04-15T19:06:...	2016-04-15T19:06:...	true	MalwareC2	MalwareC2_TeslaCrypt	HOST	IID

lovemydress.pl	Feed: AntiMalware	Severity: High	Discovered on: 2016-04-15

Class
MalwareC2

Active/Inactive
Active

Property
MalwareC2_TeslaCrypt

Narrative
Ransomware. Mostly infected computer gamers since the target of the encrypted files are game saves, user profiles, recoded replays.

Confidence
High

Infoblox

DNS Firewall

Infoblox DNS Firewall

Malicious hostnames

Infoblox ActiveTrust™™ Threat Intelligence Feed
Hostnames of malicious destinations

INTERNET

INTRANET

Malware

④

① **Malware** spreads within network; calls home

Infoblox DNS Firewall

② ✖

③ **Blocked communication attempt/indicator of compromise**

⑤ **3rd party security technologies** exchange data
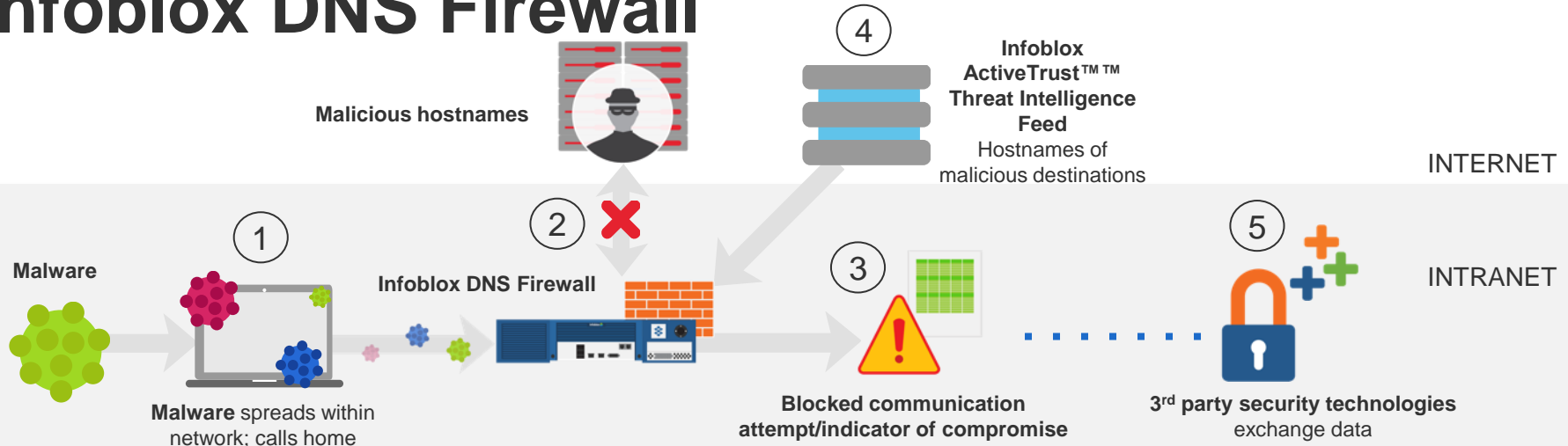
1 An infected device brought into the office. Malware spreads to other devices on network.

2 Malware makes a DNS query to find "home" (botnet / C&C). DNS Firewall looks at the DNS response and takes admin-defined action (disallows communication to malware site or redirects traffic to a landing page or "walled garden" site).

3 **Pinpoint.** Infoblox Reporting lists DNS Firewall action as well as

- User name (from MS AD)
- Device IP address
- Device MAC address
- Device type (DHCP fingerprint)
- Device host name
- Device lease history

4 Threat intelligence is regularly updated for up-to-date protection.
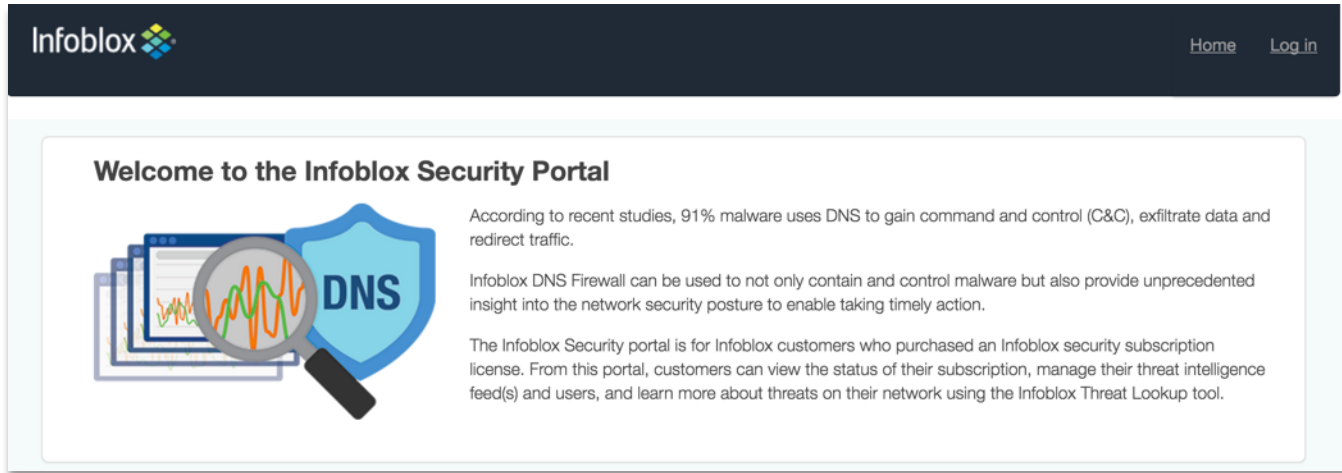
5 Additional threat intelligence from sources outside Infoblox can also be used by DNS Firewall and DNS Firewall can likewise share indicators of compromise with other security technologies for enhancing protection and easing incident response efforts.

Infoblox

Infoblox ActiveTrust Threat Intelligence Feed

- Automatic ongoing protection against malware without intervention

- Three data feeds
  - Base
  - Malware
  - Ransomware

- Benefits:
  - High confidence level (low false positives)
  - Flexibility
  - Performance

Base feed data

Malware feed data

Ransomware feed data

Pre-defined Lists

Feed(s)

Infoblox DNS Firewall

User-defined RPZ behaviors
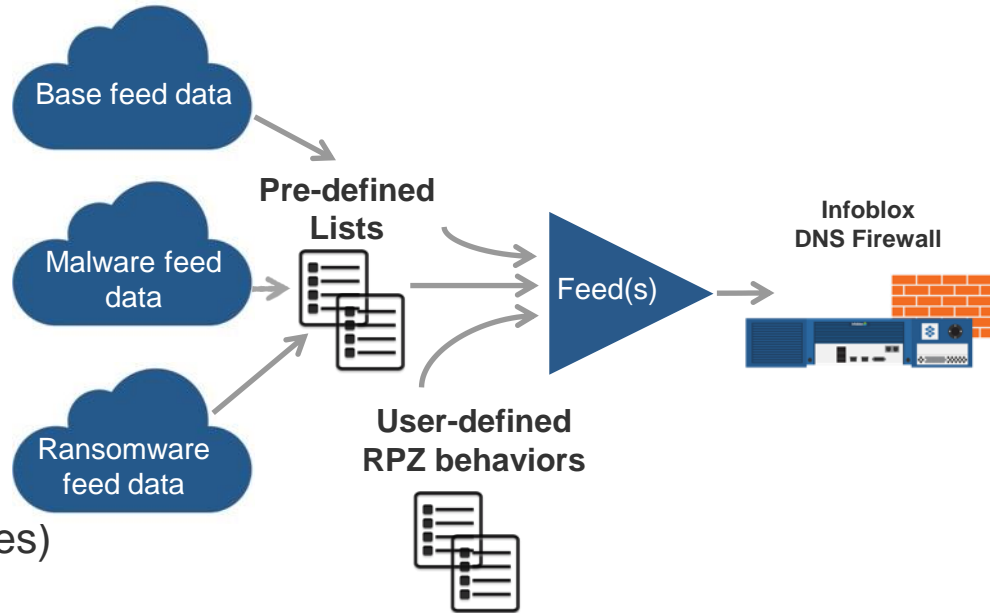
Security Portal for Context and Management

Welcome to the Infoblox Security Portal

According to recent studies, 91% malware uses DNS to gain command and control (C&C), exfiltrate data and redirect traffic.

Infoblox DNS Firewall can be used to not only contain and control malware but also provide unprecedented insight into the network security posture to enable taking timely action.

The Infoblox Security portal is for Infoblox customers who purchased an Infoblox security subscription license. From this portal, customers can view the status of their subscription, manage their threat intelligence feed(s) and users, and learn more about threats on their network using the Infoblox Threat Lookup tool.

- **Threat Lookup Portal**
  - Threat description
  - Severity level and classification
  - Active/inactive

- **Manage feed, subscription and users**
  - Verify feed(s) enabled on DNS Firewall
  - Manage feed subscription
  - Add/remove users

Infoblox

Key Benefits of Infoblox DNS Firewall

Proactive

- Existing network infrastructure for disrupting malicious communication
- DNS-based data exfiltration prevention using analytics
- Real-time data sharing w/3rd party technologies for rapid malware containment

Insightful

- Critical threat insight for easing prioritization and taking action
- Pinpointing infected devices for easing remediation efforts
- Contextual reporting, alerts, and incident notification

Adaptable

- Cloud-based, automated, and up-to-date threat intelligence feed
- Scalable protection
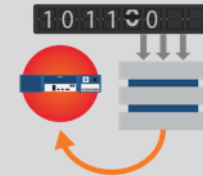
Source: (1) Infoblox estimate. (2) Open Resolver Project http://openresolverproject.org. (3) Arbor Networks Worldwide Infrastructure Security Report Vol. X

Infoblox

Infoblox as part of Cybersecurity Ecosystem

STIX/TAXII

splunk>

IBM.

RAPID7

SIEM

Vulnerability Management

Cisco ISE

Cisco ACI / APIC

ANOMALI

Threat Intelligence Platform

hp

LogRhythm
The Security Intelligence Company

aruba
a Hewlett Packard Enterprise company

CISCO

Network Access Control

THREATCONNECT

FireEye

Advanced Threat Detection

STIX/TAXII, REST API, and third-party protocols

Infoblox
CONTROL YOUR NETWORK

DNS

Infoblox DDI Appliance with Built-in Security

CARBON BLACK
ARM YOUR ENDPOINTS
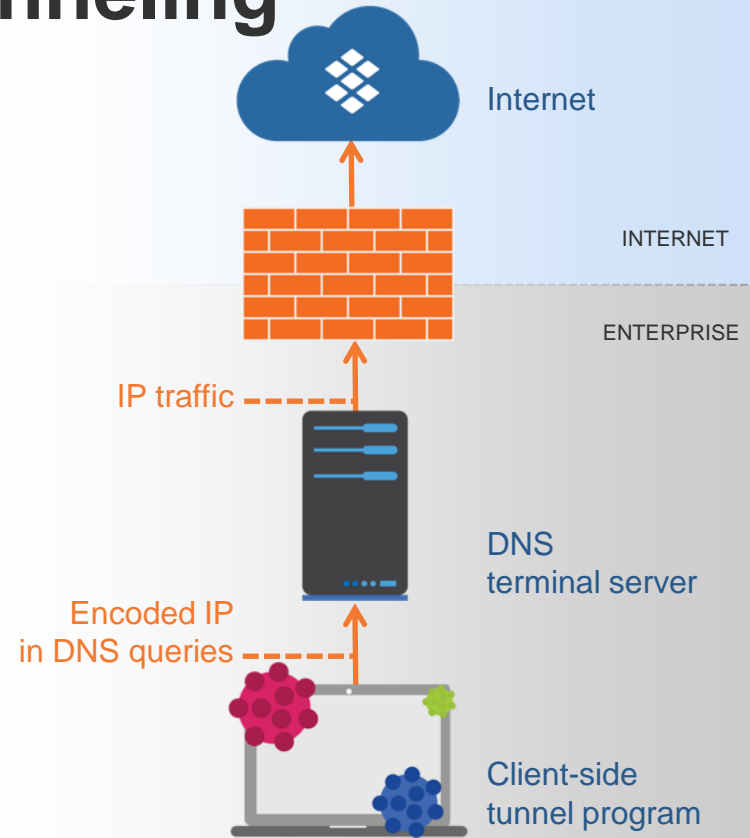
Next-gen Endpoint Security

Infoblox

Exfiltrating Data via DNS Tunneling

- Uses DNS as a covert communication channel to bypass firewalls

- Attacker tunnels other protocols like SSH, or web within DNS

- Enables attackers to easily insert malware, pass stolen data or tunnel IP traffic without detection

- A DNS tunnel can be used as a full remote-control channel for a compromised internal host

Examples:

- Iodine
- OzymanDNS
- SplitBrain
- DNS2TCP
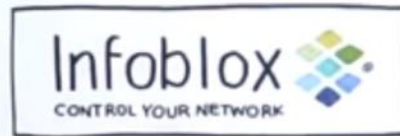
Internet

INTERNET

ENTERPRISE

IP traffic

DNS terminal server

Encoded IP in DNS queries

Client-side tunnel program

Infoblox

IODINE

INTERNET

INTERNET
ENTERPRISE

DNS SERVER

Infoblox
CONTROL YOUR NETWORK

DATA

CLIENT-SIDE
TUNNEL
PROGRAM

X3e7c7.thief.com

DNS

X3e7c7.thief.com

HEX
CODE

✗ HACKER
CONTROLLED
SERVER

infoblox
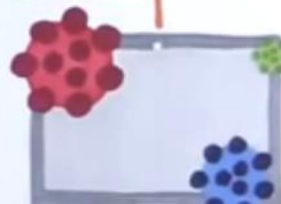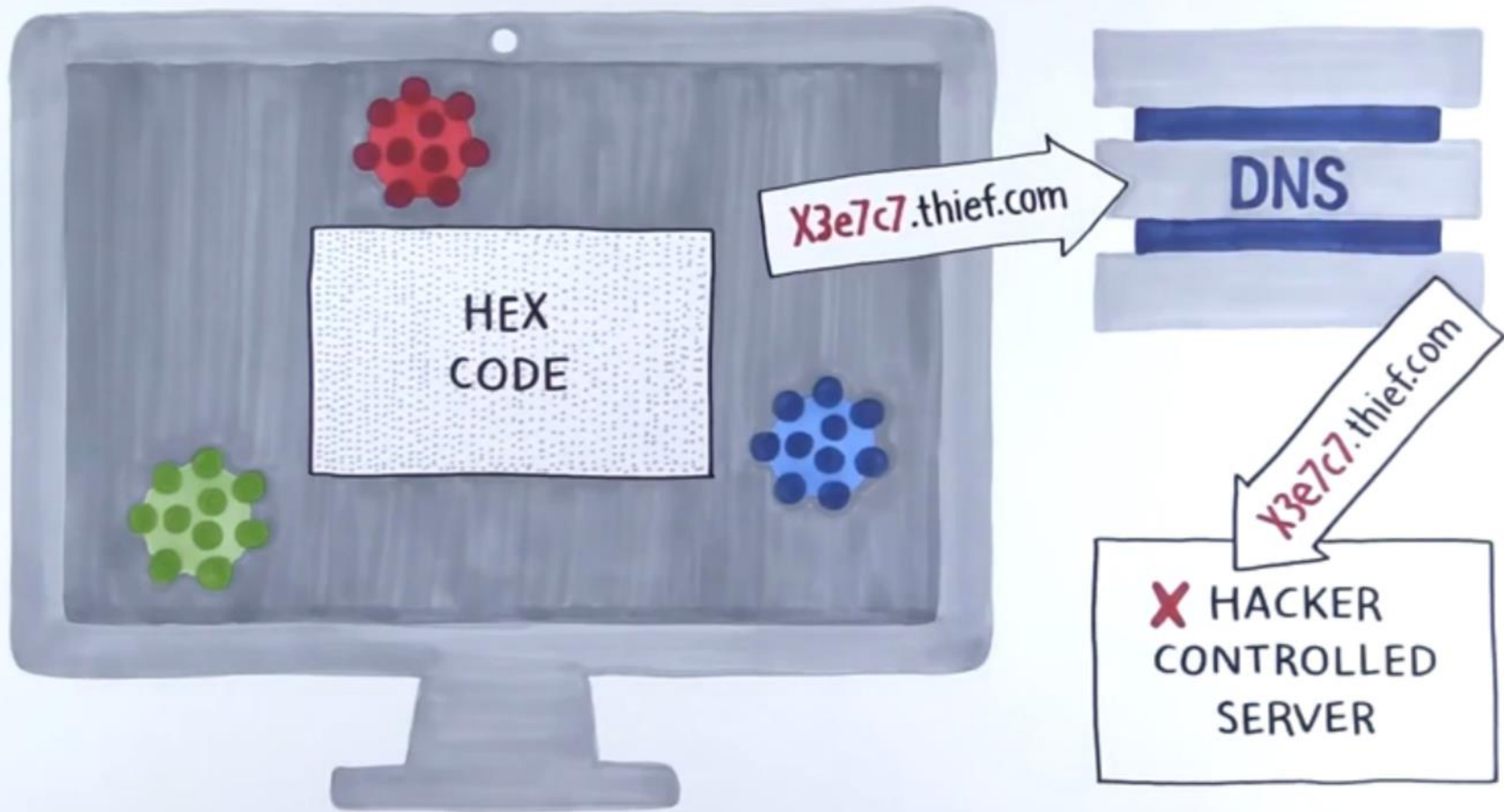
DNS Examples – Data Exfiltration

Data Exfiltration

Let's do data leak :

http://www.ignoremydata.com/

DNS Data Exfiltration

We have DNS blocked…. Really?

DNS?: ==af5ebb91c91494a63c9174f79b9ef3769d0db673d2f735acd5570f73e8ba98.15.2m78ly.==ignoremydata.com

DNS?: mailto:alamakota@==af5ebb91c91494a63c9174f79b9ef3769d0db673d2f735acd5570f73e8ba98.15.2m78ly.ignoremydata.com==

DNS: http://==af5ebb91c91494a63c9174f79b9ef3769d0db673d2f735acd5570f73e8ba98.15.2m78ly.==ignoremydata.com

DNS Threat Analytics
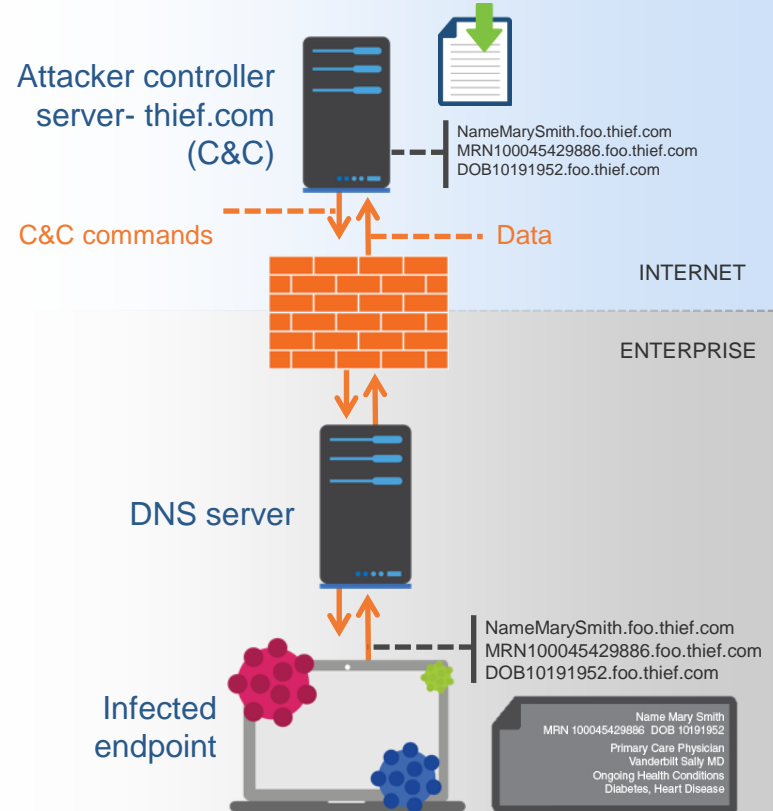## *DNS Data Exfiltration*

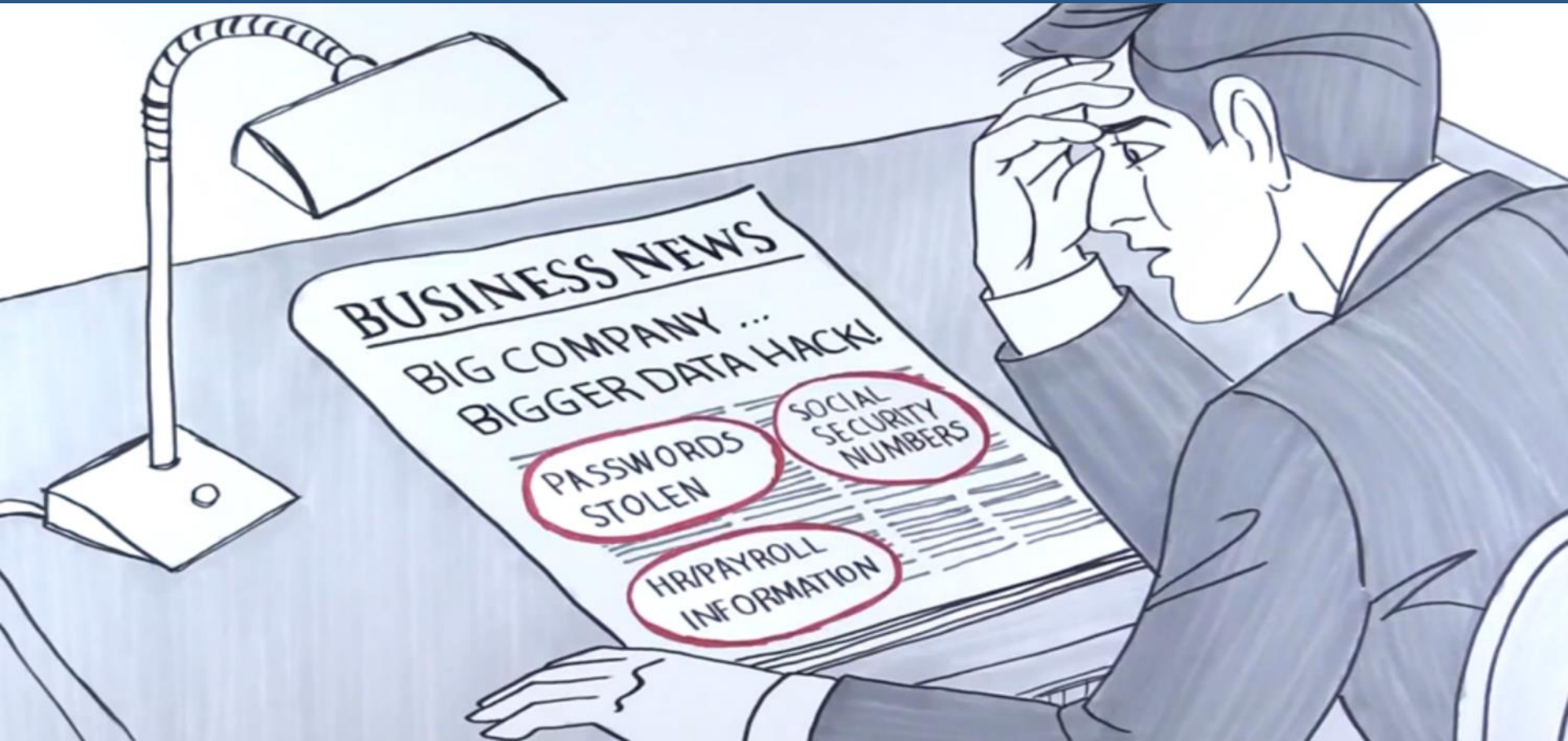Infoblox

Data Exfiltration over DNS Queries

- Infected endpoint gets access to file containing sensitive data
- It encrypts and converts info into encoded format
- Text broken into chunks and sent via DNS using hostname.subdomain or TXT records
- Exfiltrated data reconstructed at the other end
- Can use spoofed addresses to avoid detection

Data Exfiltration via host/subdomain Simplified/unencrypted example:

MarySmith.foo.thief.com
SSN-543112197.foo.thief.com
DOB-04-10-1999.foo.thief.com
MRN100045429886.foo.thief.com

Attacker controller server- thief.com (C&C)

NameMarySmith.foo.thief.com
MRN100045429886.foo.thief.com
DOB10191952.foo.thief.com

C&C commands   Data

INTERNET

ENTERPRISE

DNS server

NameMarySmith.foo.thief.com
MRN100045429886.foo.thief.com
DOB10191952.foo.thief.com

Infected endpoint

Name Mary Smith
MRN 100045429886   DOB 10191952
Primary Care Physician
Vanderbilt Sally MD
Ongoing Health Conditions
Diabetes, Heart Disease

Infoblox

DEMO Topology
We are safe…

Bartender
:-)

Source

The EVIL one:
INTERNET

Firewall

MacGyver

INFOBLOX
DNS Threat Analytics

192.168.1.244

Infoblox

Data Exfiltration

Let's do data leak :

http://www.ignoremydata.com/

www.infoblox.com/securedns
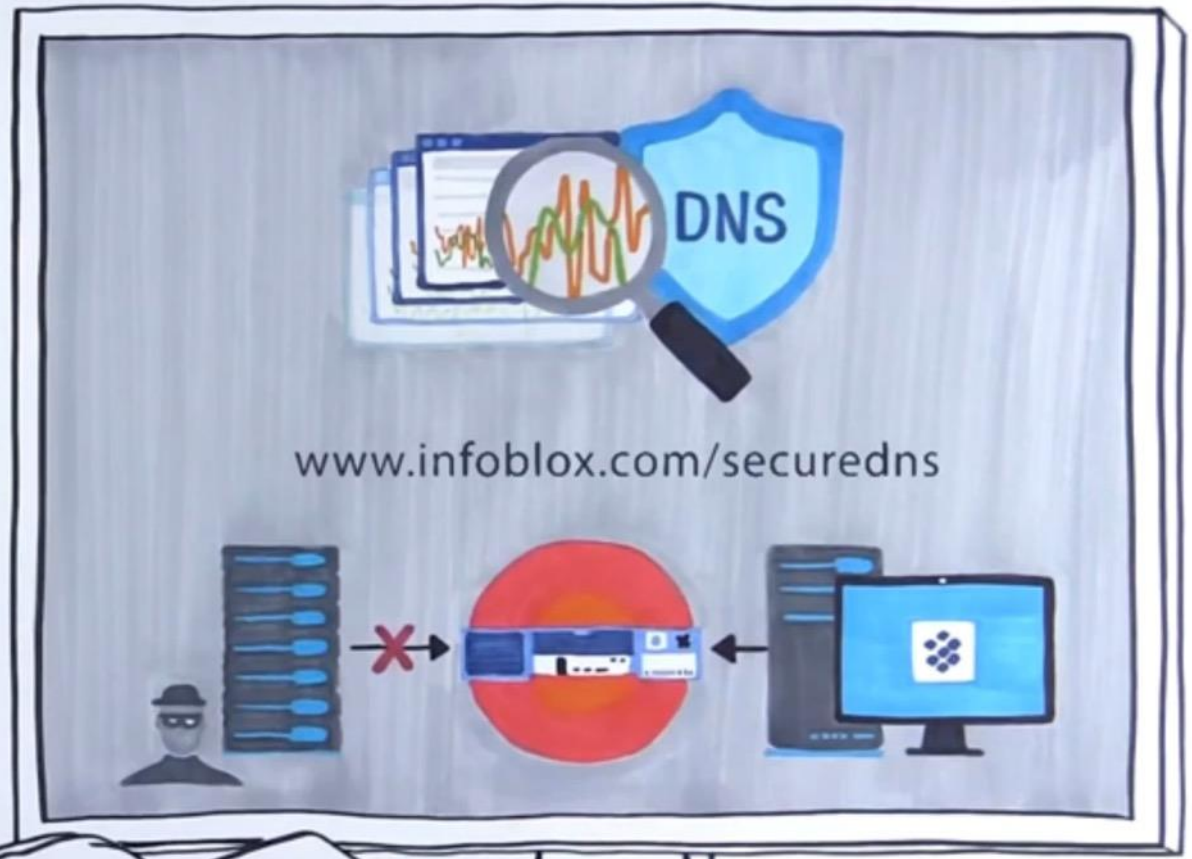
infoblox

Securing DNS To Block Data Exfiltration

~ Artificial Intelligence

Infoblox

Using Real-time Streaming Analytics
Infoblox DNS Threat Analytics

- Detects sophisticated data exfiltration techniques which don't have well known signatures (zero day)
  - Models the behavior of DNS queries
  - Looks at TXT records, A, AAAA records
  - Detects presence of data using lexical and temporal analysis
  - Automatic adds destinations to internal RPZ feed
  - Scales protection to all parts of the network
- Not a substitute for DLP products.

Entropy

Lexically

Size

Analysis Model

Frequency

N-Gram

Infoblox
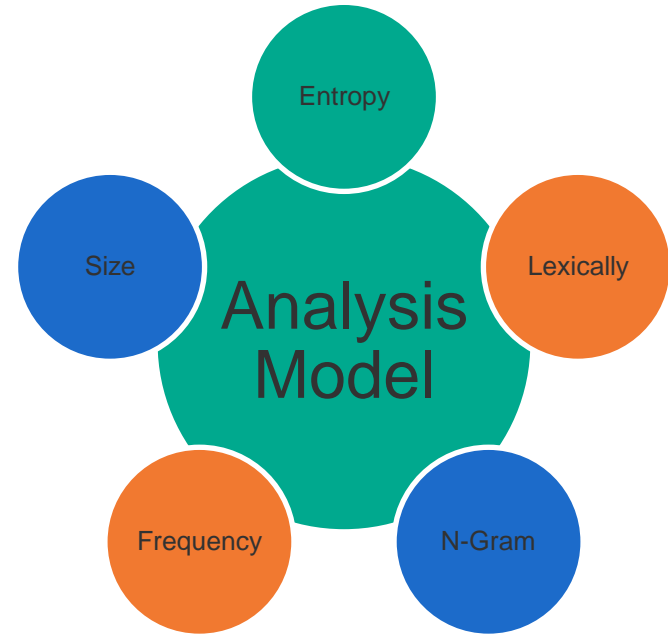
How the Analytics Model Works

Entropy	Frequency/Size	Lexical Analysis	n-Gram Analysis	Proprietary methods
• Does the request contain lots of information?	• It is unusual to send many different requests to the same external domain.	• Does it appear to be encoded or encrypted?	• Does the request contain words in a language?	• False positive mitigation • Other indicators and factors
Adds to score	Adds to score	Adds to score	Subtracts from score	Adjusts score

- Analytics algorithms are sophisticated and complex
- Simplifying greatly, certain attributes add to a threat score, others subtract from it
- All attributes are evaluated and weighted
- After all attributes are evaluated, a final score will classify a request as exfiltration or not
- If the finding is exfiltration, the destination DNS server is added to a special RPZ zone that contains the block, log, redirect policy

Infoblox

Infoblox DNS Threat Analytics

Active Blocking of Data Exfiltration Attempts
Automatically adds destinations to RPZ feed and scales enforcement to all parts of network through Grid wide update

Integrated into DNS
Data exfiltration protection built directly into DNS, providing real-time protection without need for additional network infrastructure or end point agents

Unique Patented Technology
Uses machine learning and performs real-time streaming analytics on live queries; uses advanced math (entropy, lexical analysis and time series) to determine presence of data

Visibility
Pinpoints infected devices or potential rogue employees that try to steal data

Infoblox

Summary

Protection against Known and Unknown Threats

Threat Feeds

- Regular threat feeds are about known threats
- Constantly updated
- Tailored for high detection, low false positives
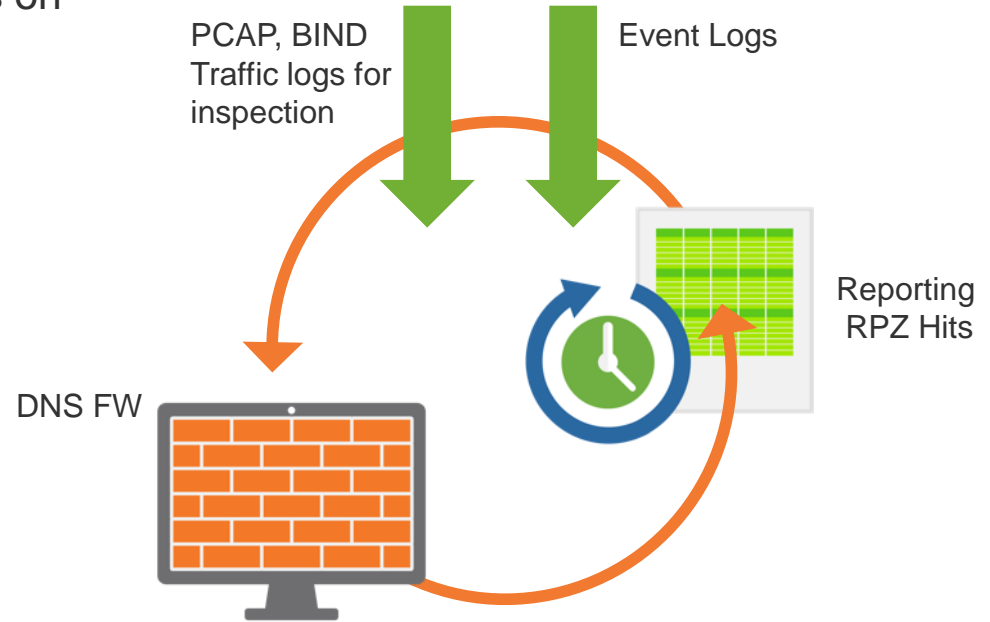- Cover malware, phishing, ransom ware, more

Behavioral Analytics

- Detects threats by how the endpoint is acting
- Surfaces unknown threats
- Can take threat data and refine it
- Threat feeds can be adjusted based on findings

Threat Intel

Behavioral Analytics

Threat Intelligence + Behavioral Analytics = Most Complete Protection

Infoblox

Try DNS Firewall
Send us your PCAP Files

- Infoblox analyzes and provides insights on malicious activity in seconds
- Report on findings to take back to management

PCAP, BIND Traffic logs for inspection

Event Logs

Reporting RPZ Hits

DNS FW

Infoblox