

# NGSec



## Infoblox DNS Threat Analytics i DNS Firewall

Zacznij panować nad malware i wyciekami danych

Adam Obszyński

CEE SE, Infoblox Inc.

**Infoblox**  
CONTROL YOUR NETWORK



**HOW  
could this HAPPEN?**

**BUSINESS NEWS**

**BIG COMPANY ...  
BIGGER DATA HACK!**

**FIREWALLS**

**PROXIES**

**IDS**



# Agenda

**DNS Basics**

---

**DNS Security Challenges**

---

**Infoblox DNS Firewall Solution**

---

**Infoblox DNS Threat Analytics**

# DNS?



```
;; ANSWER SECTION:  
ngsec.eu.                49460   IN      A       87.98.239.4
```



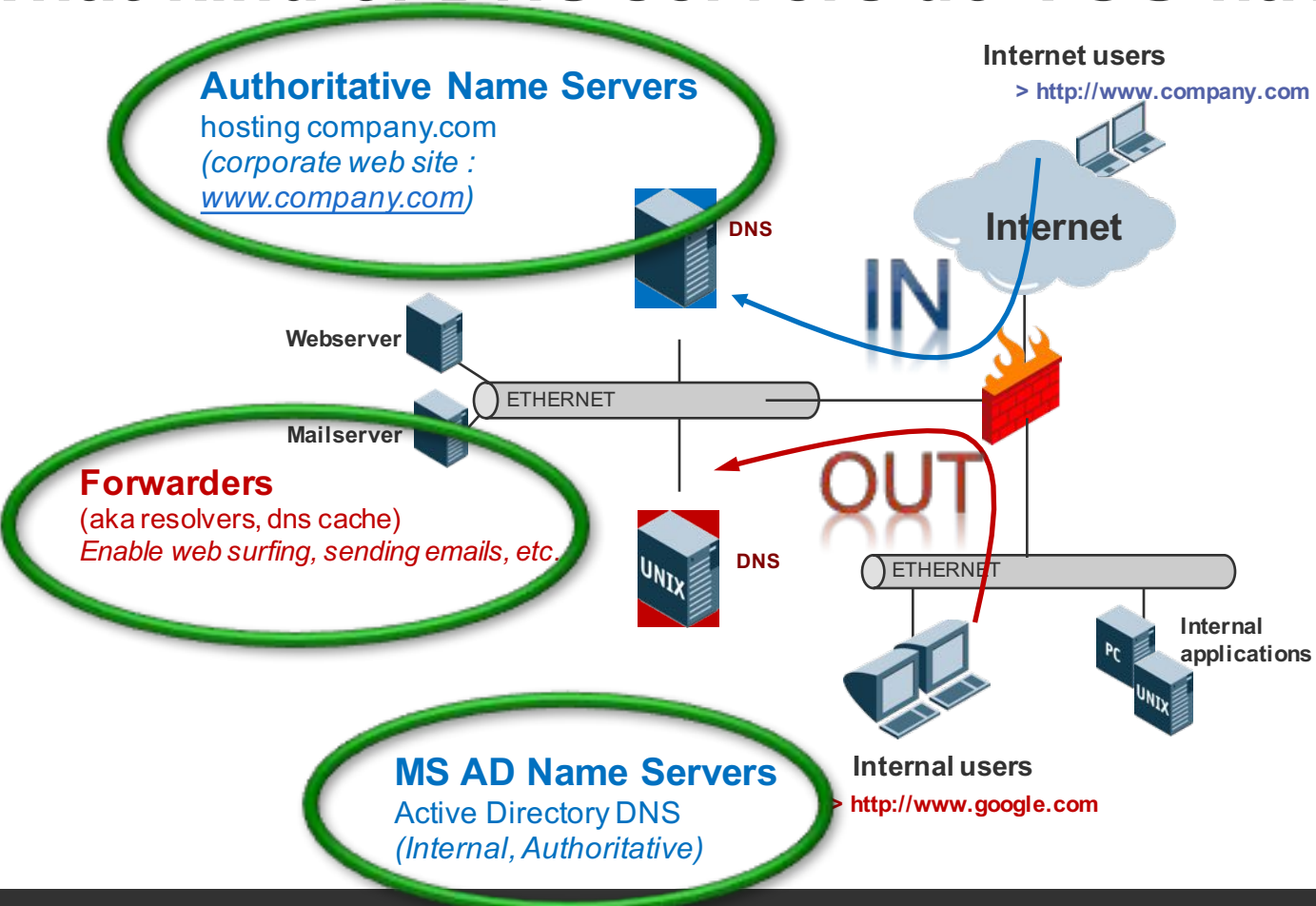
**i** Server not found

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

# What kind of DNS servers do YOU have?



# Why Securing DNS is Critical



DNS is critical  
networking  
infrastructure



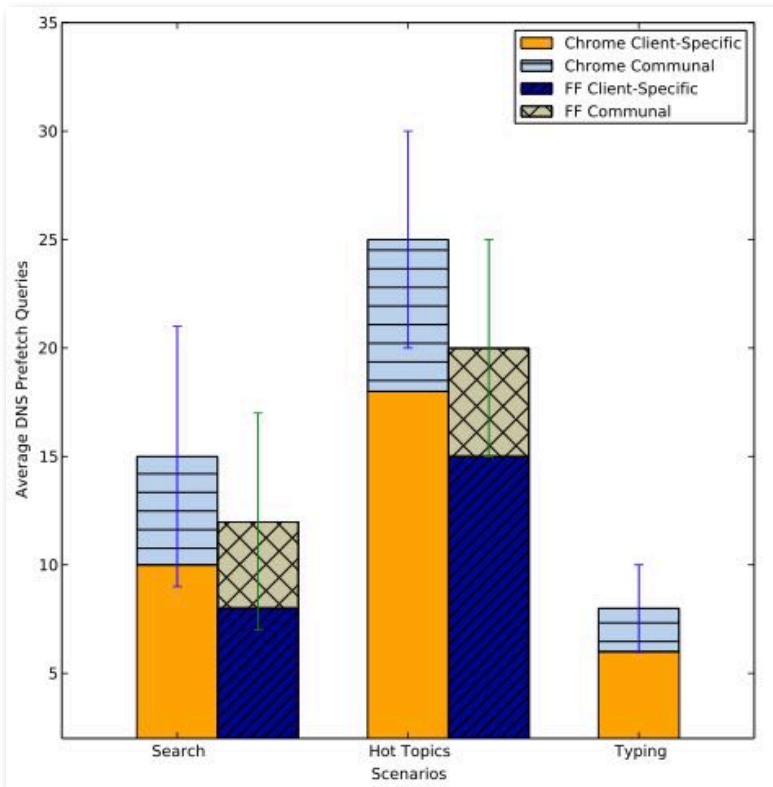
DNS protocol is  
easy to exploit and  
attacks are  
prevalent



Traditional security  
is ineffective against  
evolving threats

Unprotected, DNS increases risk to critical infrastructure and data

# Web Prefetching



```
.domain: 15198+ A? www.tw. (24)
client.: 15198 NXDomain 0/1/0 (80)
.domain: 57176+ A? www.twitter.co. (32)
client.: 57176 NXDomain 0/1/0 (93)
.domain: 40536+ A? www.twitter.com. (33)
client.: 40536 2/4/4 CNAME twitter.com.,
.domain: 17752+ A? twitter.co. (28)
client.: 17752 NXDomain 0/1/0 (89)
.domain: 17497+ A? twitter.com. (29)
.domain: 7252+ A? www.si. (24)
client.: 7252 1/2/1 A 195.246.14.80
.domain: 21334+ A? www.sina.co. (29)
client.: 21334 NXDomain 0/1/0 (90)
.domain: 40279+ A? www.sina.com. (30)
.domain: 12375+ A? www.sina.com. (30)
.domain: 26193+ A? www.sina.com.cn. (33)
client.: 40279 3/3/3 CNAME us.sina.com.cn.,
.domain: 10824+ A? www.my. (24)
client.: 10824 NXDomain 0/1/0 (85)
.domain: 62025+ A? www.myspace.co. (32)
client.: 62025 NXDomain 0/1/0 (93)
.domain: 43338+ A? www.myspace.com. (33)
.domain: 33099+ A? myspace.co. (28)
client.: 33099 NXDomain 0/1/0 (89)
.domain: 37963+ A? myspace.com. (29)
client.: 37963 2/6/6 A 63.135.80.49
.domain: 10881+ A? www.ndtv.co. (29)
client.: 10881 NXDomain 0/1/0 (90)
.domain: 35970+ A? www.ndtv.cn. (29)
client.: 35970 1/2/2 A 124.207.241.165 (118)
.domain: 22146+ A? www.ndtv.com. (30)
client.: 22146 4/9/8 CNAME www.ndtv.com.edgesuite.net.,
CNAME a1807.g.akamai.net., A 128.109.34.37 (421)
```

Invalid Records

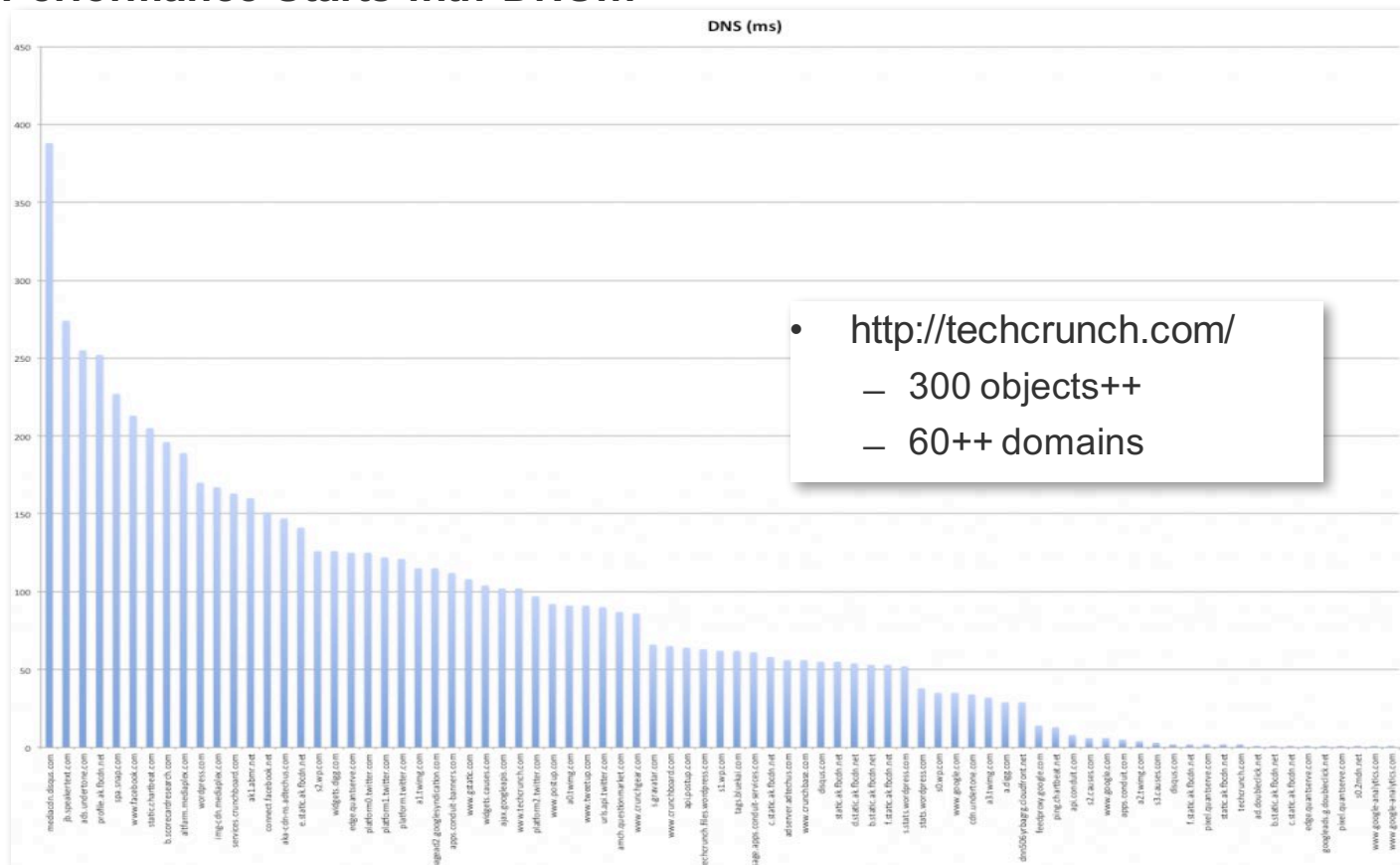
Not the intended website

© 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...

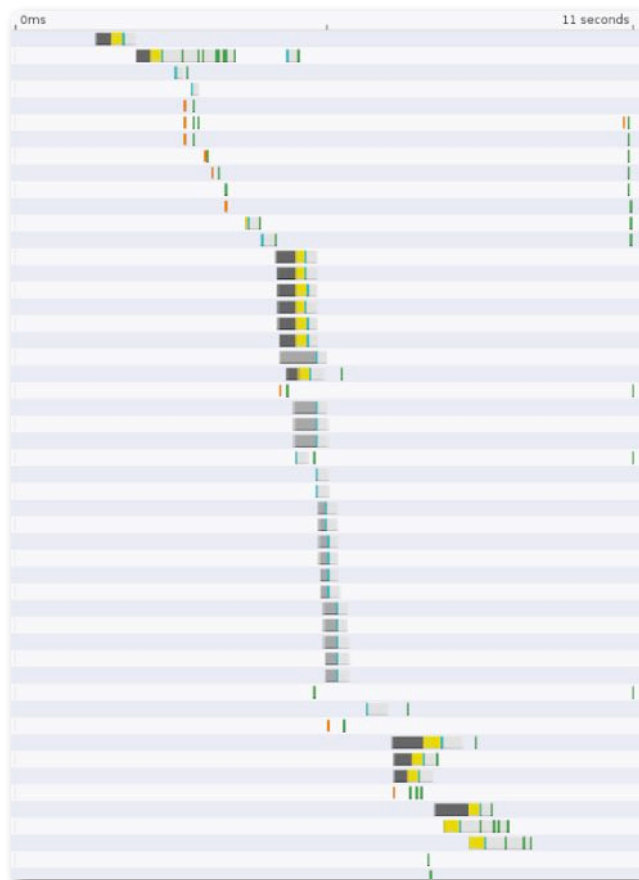


- <http://techcrunch.com/>
  - 300 objects++
  - 60++ domains

© <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

**Figure 13. Monitoring Threats from Recursive DNS**



**DNS**

**91.3%**

of malware uses  
DNS in attacks



**68%**

of organizations  
don't monitor  
recursive DNS

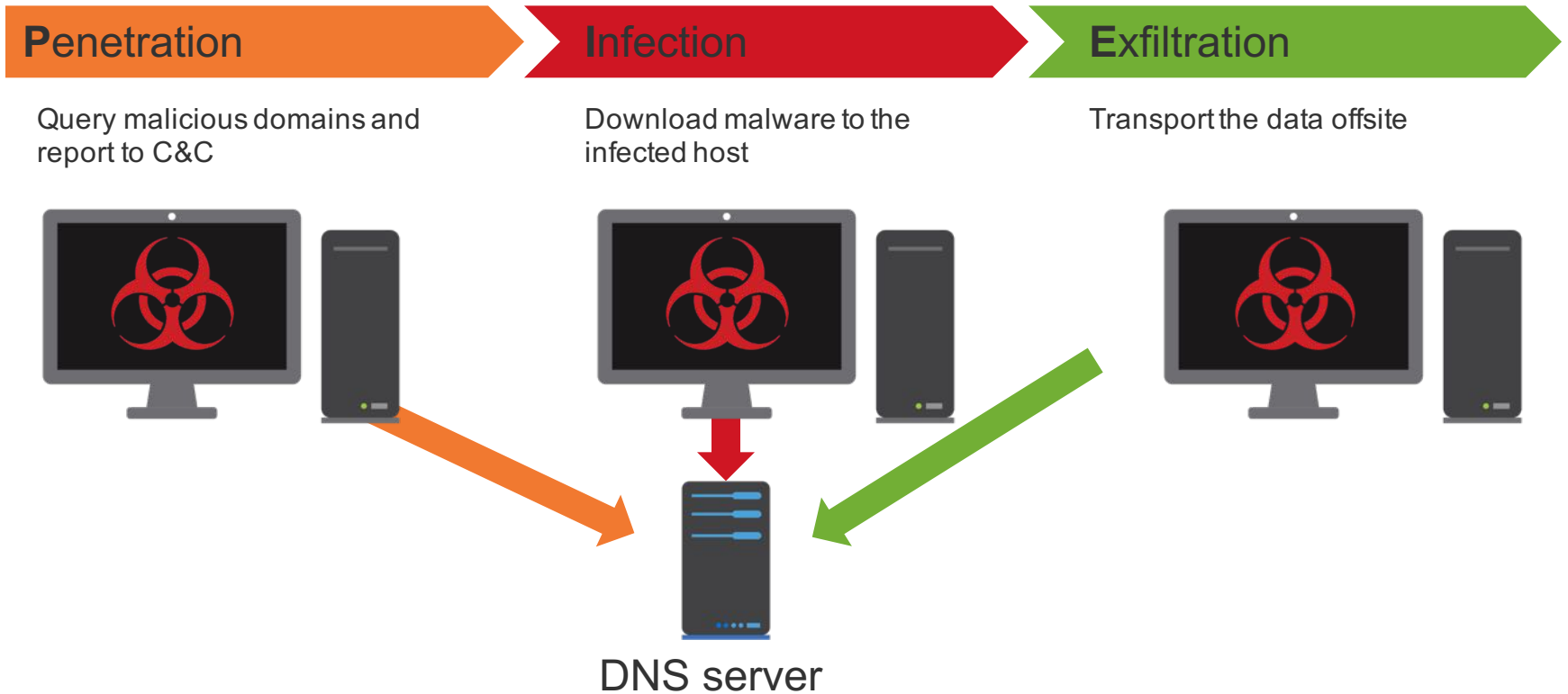
Source: Cisco Security Research



Cisco 2016  
Annual Security Report

# Motion of Malware through Networks: “PIE”

APT/malware uses DNS at every stage



# What the Bad Guys are After and Why

## PII (Personally Identifiable Information)

Information like social security numbers of employees or customers that cybercriminals can use to steal identity, or sell in the underground market for profit

## Regulated Data

Data related to PCI DSS and HIPAA compliance that can be misused

## Intellectual Property

Data that can give an organization a competitive advantage

## Other Sensitive Information

Credit card numbers, company financials, payroll and emails



Hacktivism



Espionage



Financial Profit

# 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 and 100s 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





# DNS Examples - Malware



# Mini DEMO #1

NGSec



# Malware

## **Few queries:**

dig lovemydress.pl

dig brt2014.com

dig all-that-and-more.net

# DEMO Topology

We are safe...



vmware

Bartender

: -)



Mac OS X

Source



Firewall

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	<a href="http://lovemydress.pl/wp-content/themes/sketch/csys.php">http://lovemydress.pl/wp-content/themes/sketch/csys.php</a>	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

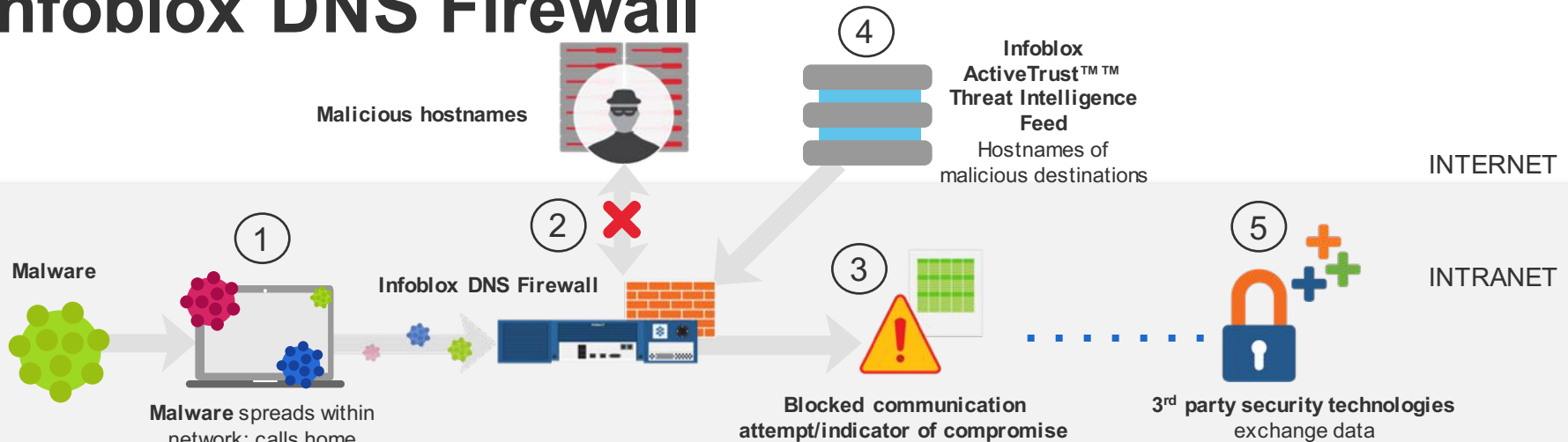
---

<b>Class</b> MalwareC2	<b>Active/Inactive</b> Active
<b>Property</b> MalwareC2_TeslaCrypt	<b>Narrative</b> Ransomware. Mostly infected computer gamers since the target of the encrypted files are game saves, user profiles, recorded replays.
<b>Confidence</b> <span style="background-color: red; color: white; border-radius: 50%; padding: 2px 5px;">High</span>	

# DNS Firewall



# Infoblox DNS Firewall



**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).

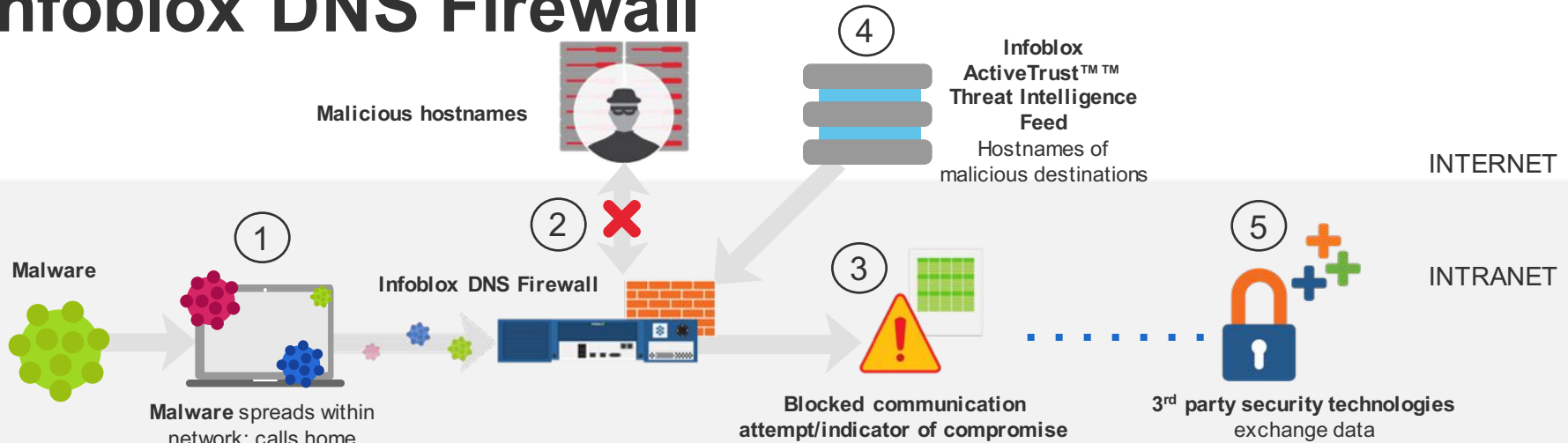
**3 Pinpoint.** Infoblox Reporting lists DNS Firewall action as well as

- User name
- 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 DNS Firewall



**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

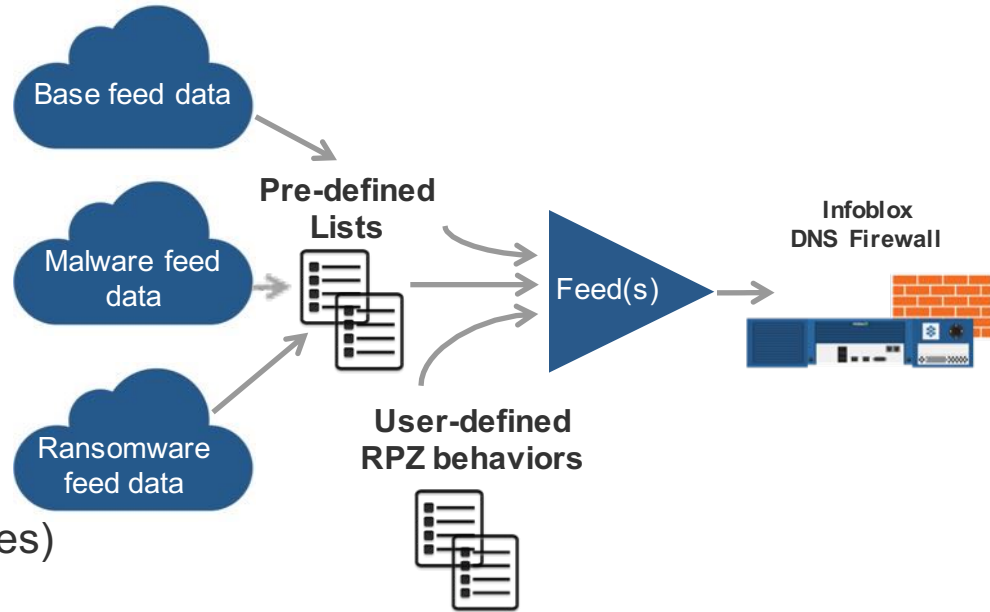
**4** Threat intelligence is regularly updated for up-to-date protection.

**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.

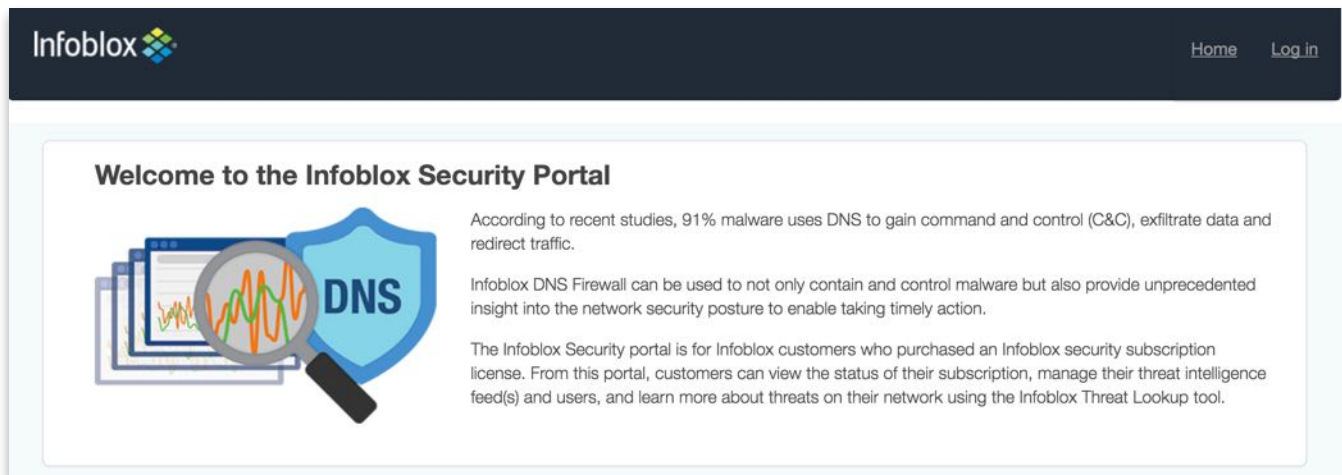


# Infoblox ActiveTrust Threat Intelligence Feed

- Automatic ongoing protection against malware without intervention
- Three data feeds
  - Base
  - Malware
  - Ransomware
- Benefits:
  - High confidence level (low false positives)
  - Flexibility
  - Performance



# 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

# 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/3<sup>rd</sup> party technologies for rapid malware containment



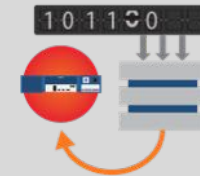
## Insightful

- 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 as part of Cybersecurity Ecosystem

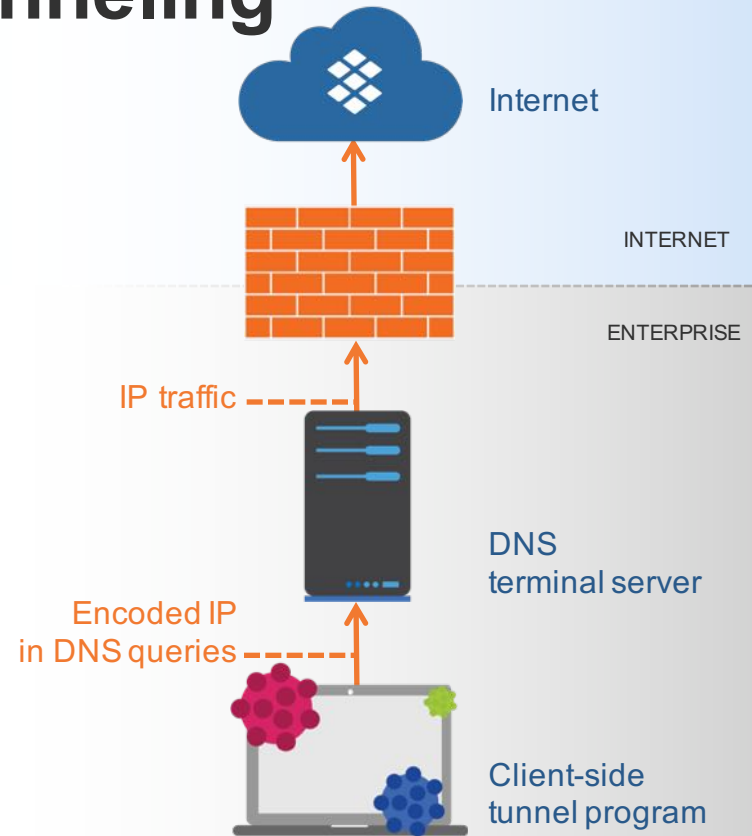


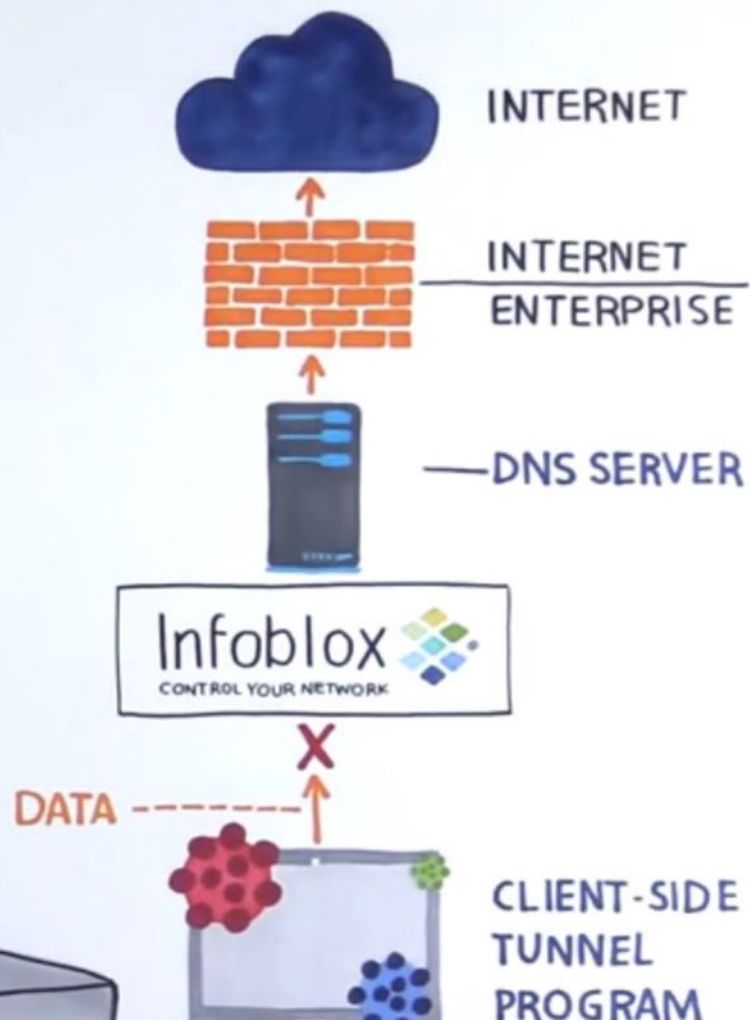
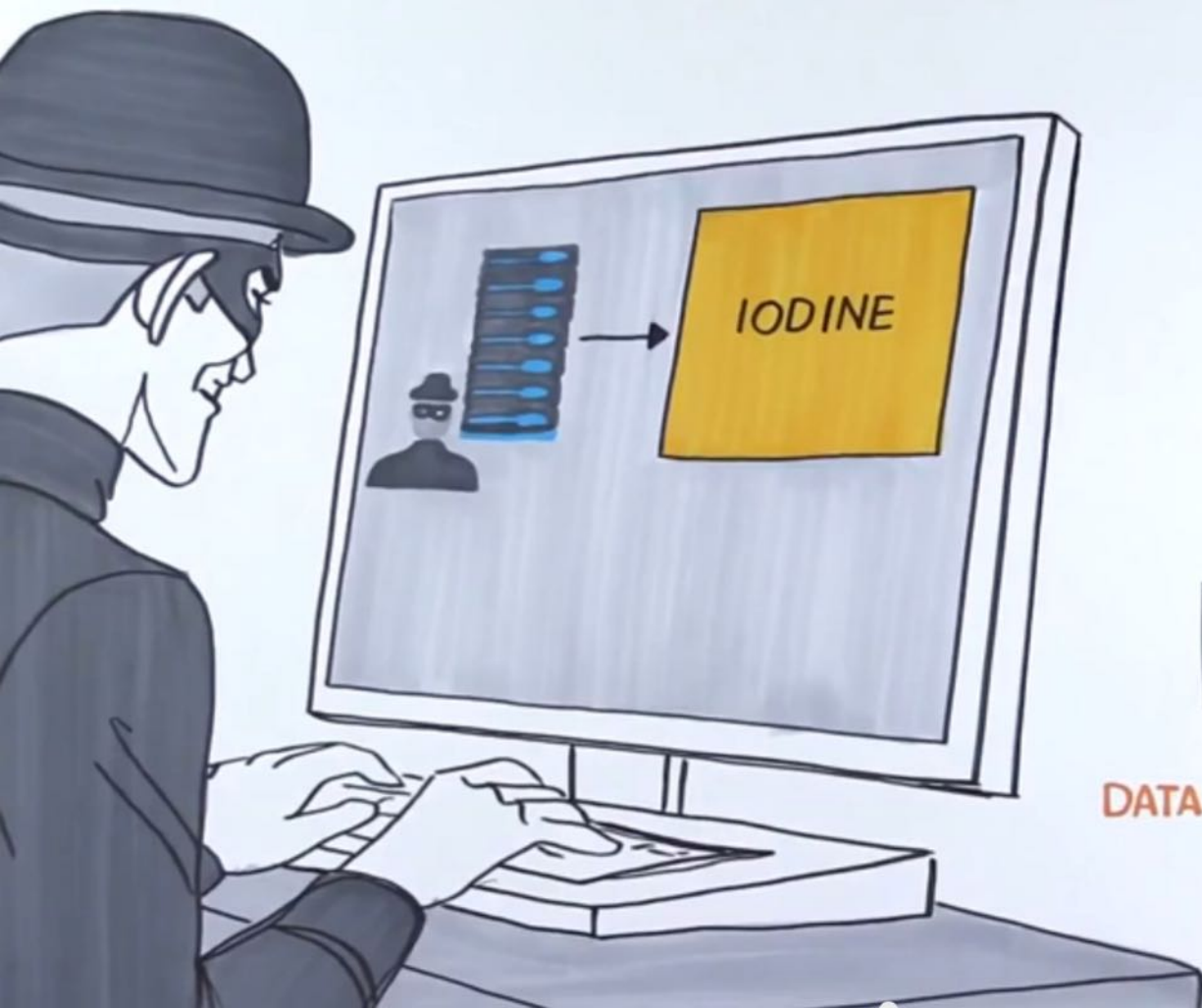
# Exfiltrating Data via DNS Tunneling

- 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

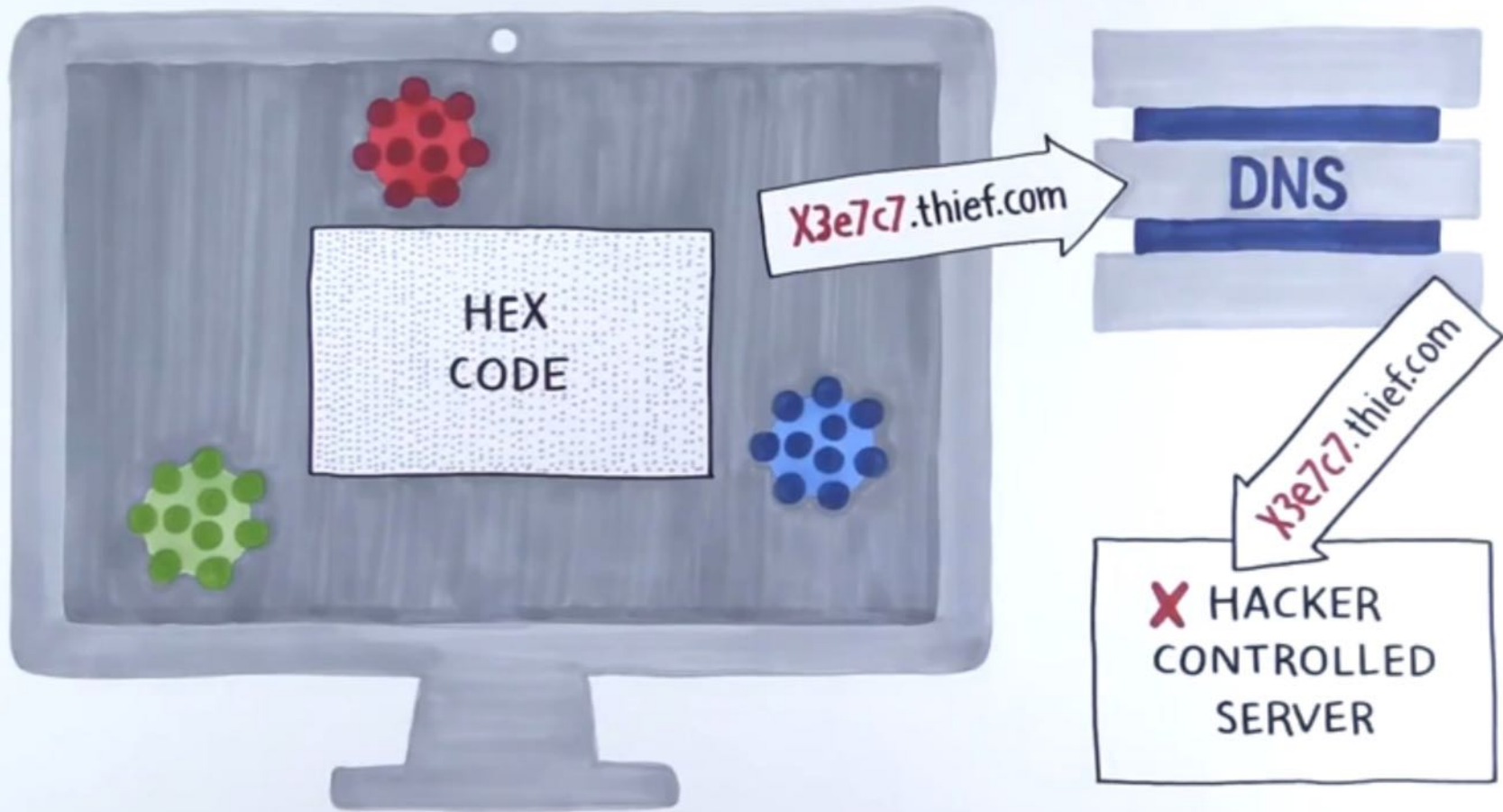
## Examples:

- Iodine
- OzymanDNS
- SplitBrain
- DNS2TCP













# DNS Examples – Data Exfiltration





# DNS Data Exfiltration

## We have DNS blocked.... Really?

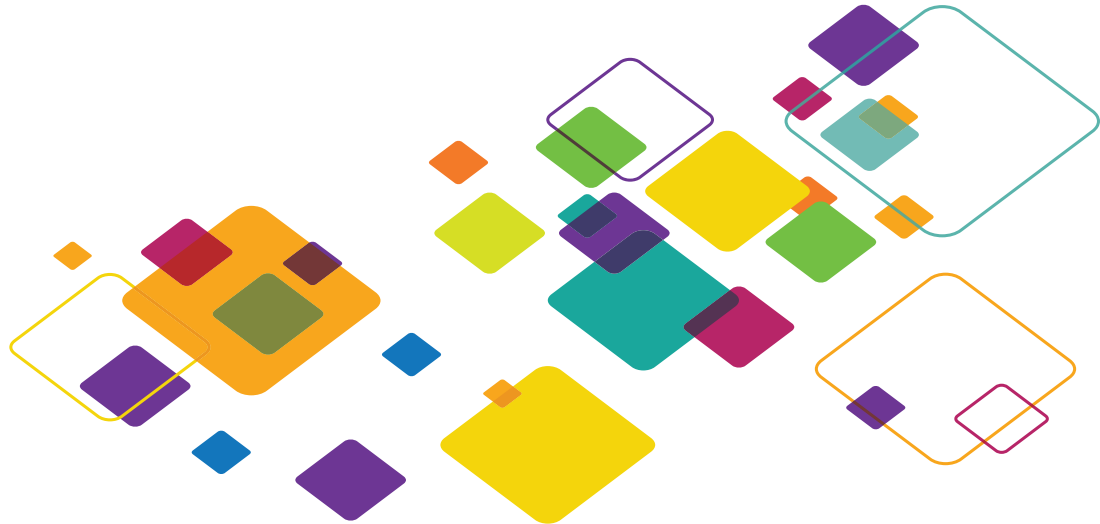
DNS?: [af5ebb91c91494a63c9174f79b9ef3769d0db673d2f735acd5570f73e8ba98.15.2m78ly.dnsevil.com](http://af5ebb91c91494a63c9174f79b9ef3769d0db673d2f735acd5570f73e8ba98.15.2m78ly.dnsevil.com)

DNS?: <mailto:alamakota@af5ebb91c91494a63c9174f79b9ef3769d0db673d2f735acd5570f73e8ba98.15.2m78ly.dnsevil.com>

DNS: <http://af5ebb91c91494a63c9174f79b9ef3769d0db673d2f735acd5570f73e8ba98.15.2m78ly.dnsevil.com>

# DNS Threat Analytics

## *DNS Data Exfiltration*

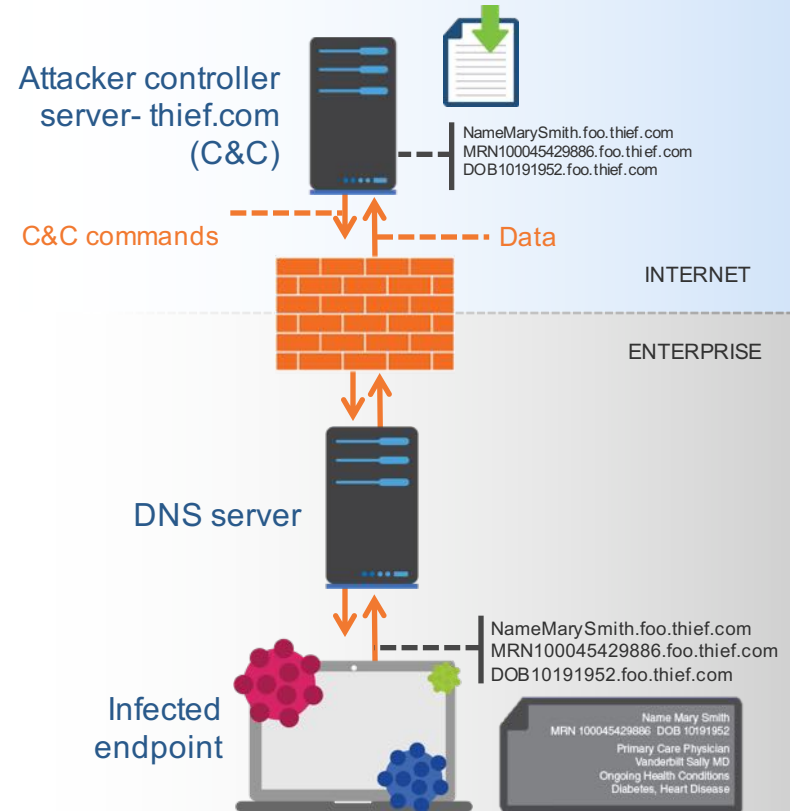


# Data Exfiltration over DNS Queries

- 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





# DEMO Topology

We are safe...



vmware

Bartender

: -)



Mac OS X

Source



Firewall

MacGyver



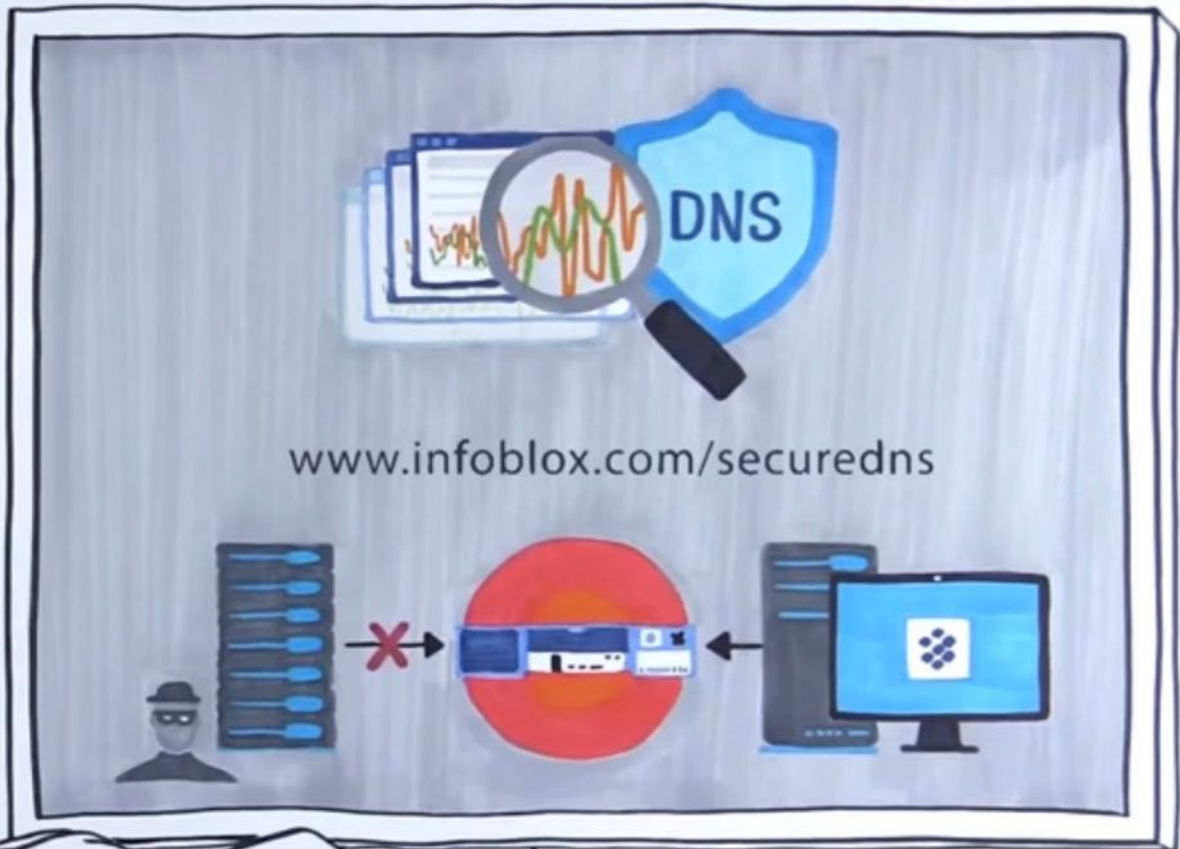
The EVIL one:  
INTERNET

INFOBLOX

**DNS Threat Analytics**

192.168.1.244





# Securing DNS To Block Data Exfiltration

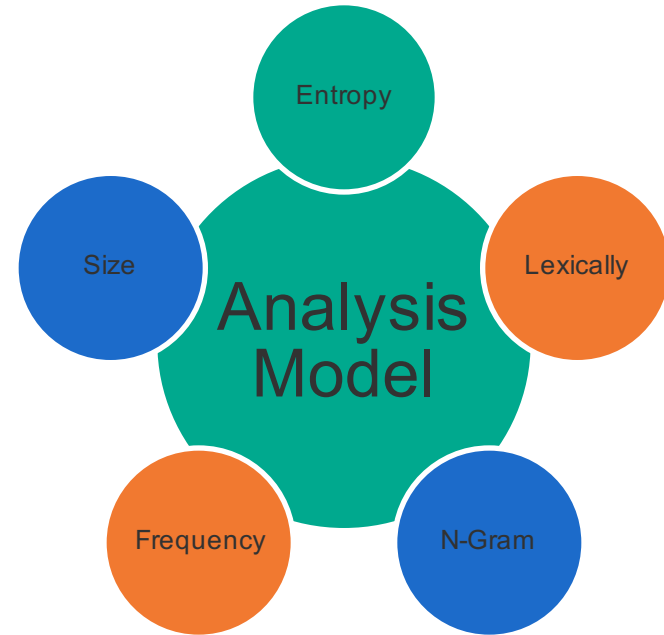
~ Artificial Intelligence



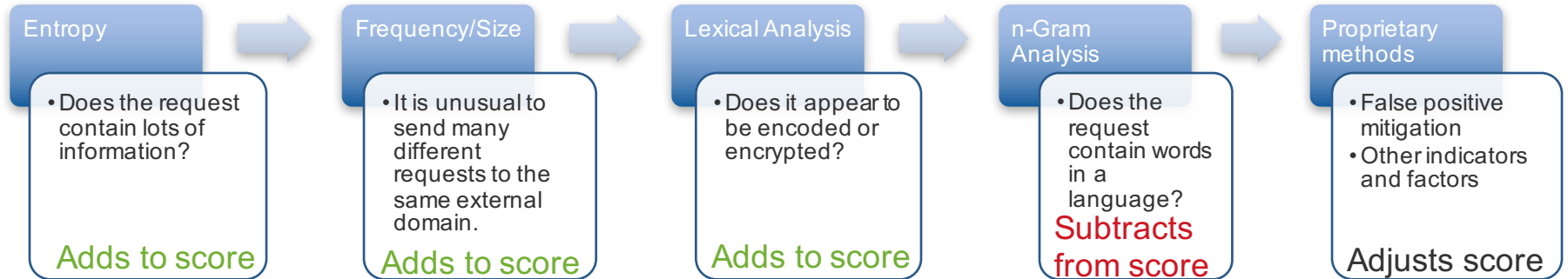
# Using Real-time Streaming Analytics

## 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.



# How the Analytics Model Works



- 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 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

# 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, ransomware, more



## Behavioral Analytics

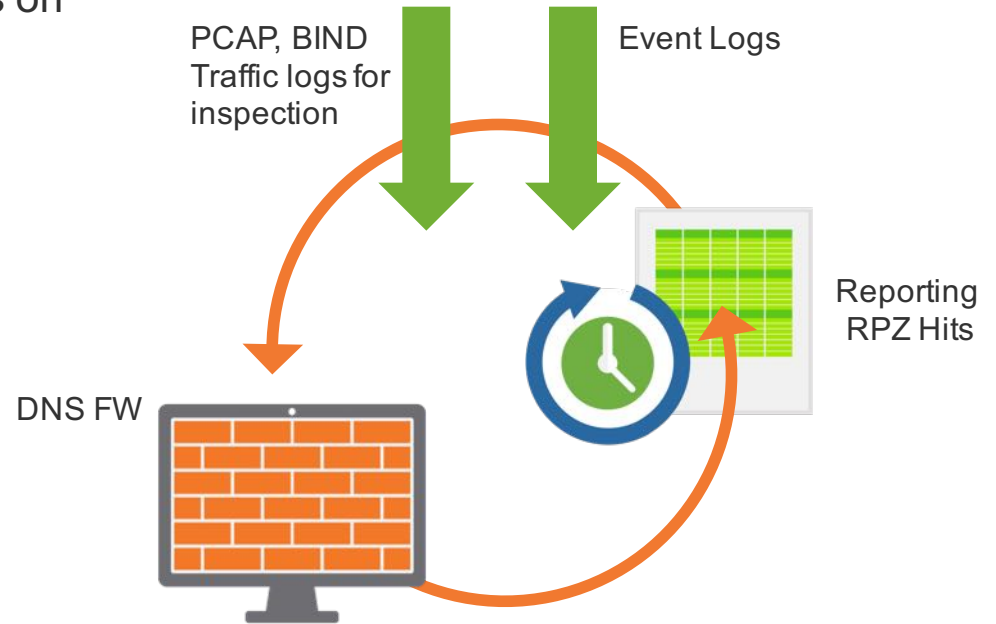
- Detects threats by how the endpoint is acting
- Surfaces unknown threats
- Can take threat data and refine it
- Threat feeds can be adjusted based on findings

Threat Intelligence + Behavioral Analytics = Most Complete Protection

# 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





NGSec

Infoblox 

