Infoblox
NEXT LEVEL NETWORKING

Evolution des pratiques des attaquants du point de vue du DNS

Nicolas Jeanselme – Principal Systems Engineer

Date: March 27th 2019

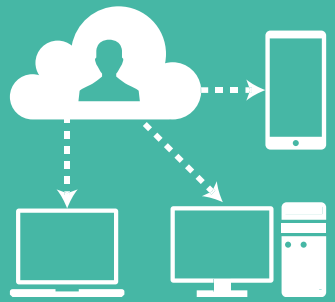
Elevate Your Security

#1
Infrastructure Protection

Next-level Reliability and Availability

#2
Data Protection and Malware Mitigation

Next-level Security for Users and Data



#3
Threat Containment and Operations

Next-level Efficiency & Automation of Security Operations

Rising Flood of Cyberattacks with Multiple Methods of Exploiting DNS

Identifying The Leading Culprit in Data Exfiltration

$3.86M
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]

DNS tunnels used send sensitive information out

Data embedded in DNS queries

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 2018 Annual Security Report
6. https://www.av-test.org/en/statistics/malware/
7. Verizon 2016 Data Breach Investigations Report

APT/Malware Proliferation Rooted in DNS

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

780 million
Malware attacks over the past 10 years, as of May 2018[6]

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

Intruders rely on DNS to infect devices & propagate malware

Malware designed to morph, hide in your infrastructure

Longer it takes to discover, higher the cost of damage

DNS in the Killchain

 |

Examples of malware using DNS for communication

Malware / Group	Discovered	DNS Communication
DNSBot	2019	C2/ exfil / infil
DMSniff POS	2019	C2 DGA – undetected 4 years
GlitchPOS	2019	C2
RogueRobin / DarkHydrus	2018	C2/ exfil / infil
Quadagent / OilRig	2018	C2/ exfil / infil
UDPoS	2018	C2 / exfil
ALMA Communicator / OilRig	2017	C2 / exfil / infil
FIN7	2017	C2 / exfil / infil
DNSMessenger	2017	C2 / infil
Denis / OceanLotus	2017	C2 / infil
Backdoor.Win32.ClIEcker	2017	C2
Trojan.Win32.Ismdoor.gen	2017	C2 / exfil
Wekby	2016	C2
Multigrain POS	2016	Exfil
ProjectSauron / Strider (NSA?)	2016	C2 / exfil
C3PRO-Raccoon	2015	C2
FrameworkPOS	2014	Exfil
PlugX v2	2014	C2
CobaltStrike (pentesting tool)	2013	C2 / infil / exfil
FeederBot	2011	C2

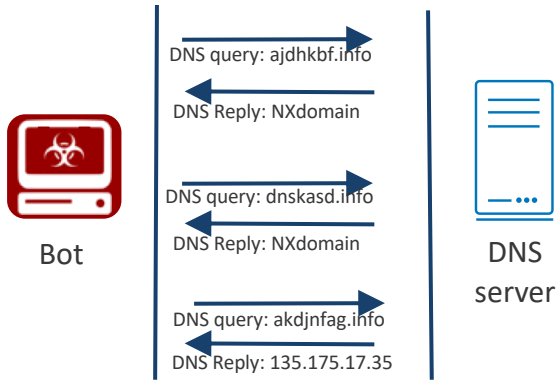
DGA – Domain Generation Algorithm

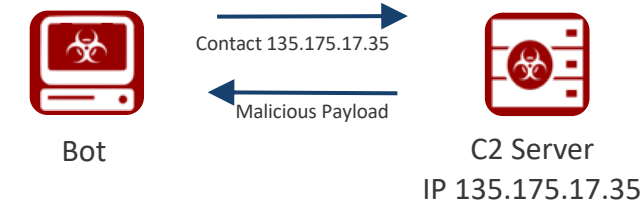
An algorithm producing Command & Control (C2) rendezvous points dynamically

For example: every day malware connects to time-based server FQDN: *<month>-<day>-<year>.com*

ie. on December 24, 2017 malware connects to 2017-12-24.com

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





How many domains are generated by DGAs?

Bamital 197,000	Fobber 2,000	Mewsei 1,984	Pykspa 2 775,342	Simda 11,528
Banjori 421,390	Geodo 90,232	Murofet 1 4,063,680	QakBot 385,000	Suppobox 98,304
Bedep 3,806	Gameover DGA 6,182,000	Murofet 2 262,000	Ramdo 3000	Szribi 2,949
Conficker 125,118,625	Gameover P2P 262,000	Necurs 3,551,232	Ramnit 18,000	Tempedreve 204
CoreBot 18,160	Gozi 16,963	Nymaim 65,040	Ranbyus 64,400	TinyBanker 81,930
Cryptolocker 1,108,000	Hesperbot 178	Pushdo 124,021	Redyms 34	Torpig 17,610
DirCrypt 420	Kraken 300	Pushdo TID 6,000	Rovnix 10,000	UrlZone 10,009
Dyre 592,000	Matsnu 3,346	Pykspa 1 22,764	Shifu 1,554	Virut 15,335,008

- Machine Learning Classifiers that aims at identifying the family of each detected DGA Domain.
- **Malware Family detection makes possible a more appropriate mitigation measure when detected an infected machine within network.**
- Infoblox Classifiers use sophisticated techniques in the field of Machine Learning combined with Natural Language Processing.

Sum of unique domains: 159 712 234 or 34 593 609 without Conficker

until end of 2015

Source: DGArchive, Daniel Plohmann, 2016

Dictionary DGA

Dictionary 1:
face
walk
weak
sell
deep
ball
push
both

+

Dictionary 2:
gone
road
dont
fool
heat
aunt
they
lift
goes

→

Suppobox malware domains:

```
facegone.net.
walkroad.net.
weakdont.net.
sellfool.net.
weakheat.net.
deepaunt.net.
facethey.net.
ballpull.net.
pushaunt.net.
walklift.net.
bothfive.net.
facegoes.net.
```

Dictionary DGA	Example Family	Example Domain
Wordlist	Suppobox	facegone.net
Permutation	VolatileCedar	dotnetexplorer.info

Dictionary DGA Detection

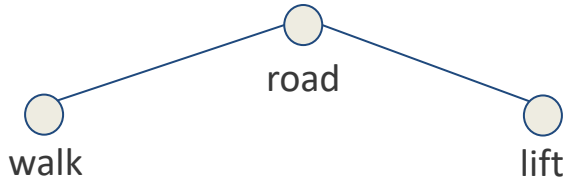
Suppobox malware domains:

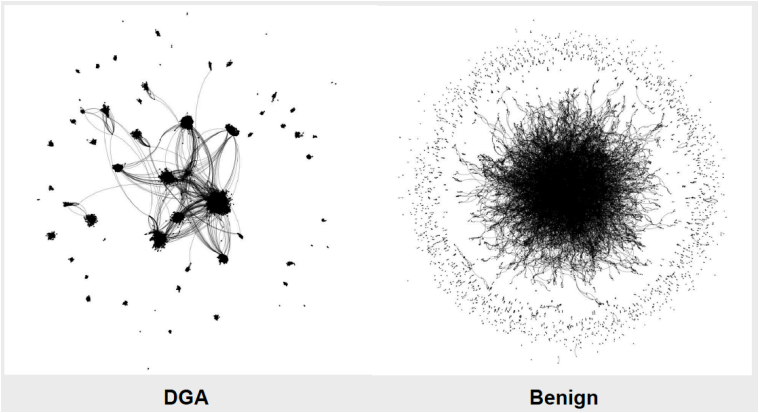
facegone.net.
walkroad.net.
weakdont.net.
sellfool.net.
weakheat.net.
deepaunt.net.
facethey.net.
ballpull.net.
pushaunt.net.
walklift.net.
bothfive.net.
facegoes.net.

Words are used repeatedly!

walkroad.net
walk + road

roadlift.net
road + lift



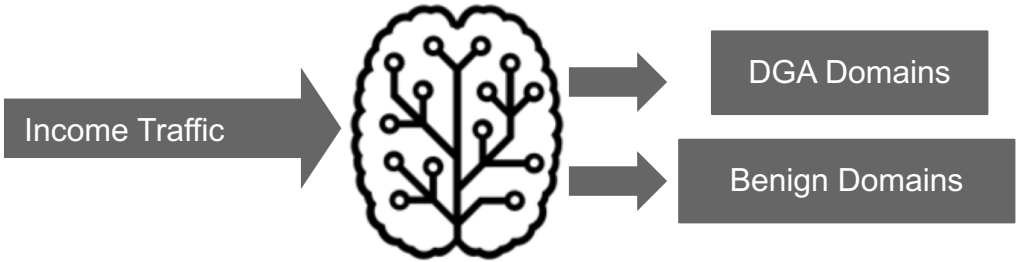


DGA words connect differently!

 |

Inline DGA Detection

- Uses Deep Learning Algorithms to differentiate benign domains from DGA Domains
- Trains Deep Neural Networks using real traffic, which results in models with a better performance to find DGA data in customers networks.
- Online learning: it is constantly retrained to catch the variations and new trends in DNS traffic



Inline DGA Detection

Lookalike Domain Detection

- Detects from Newly Observed Domains (NOD), domain names that try to mimic popular domains (Alexa top-100) or strategic domains for phishing (e.g. banks) and spamming.
- Detects domains that overlaps and/or have homograph n-grams, e.g. letter ‘O’ and number ‘0’ are considered homographs.
  Use distance analysis to detect the likelihood of lookalike attacks
- Detects

  apple.com >>> appIe.com

  – Letter replacement, example g00gle.com, gooogle.com, bankofthevvest.com, rn1cr0soft.corn
  – TLD change, example, walmart.cc
  – other generic highly resembled domains, example: bankofAmericas.com
- SOA record is analyzed and used for catching false positives.

Lookalike Domain Detection

- Doesn’t detect (yet)
  - Alphabet change, used in homograph attacks like Beta Bot Trojan:
    adoḅe[.]com http://xn--adoe-x34a[.]com/

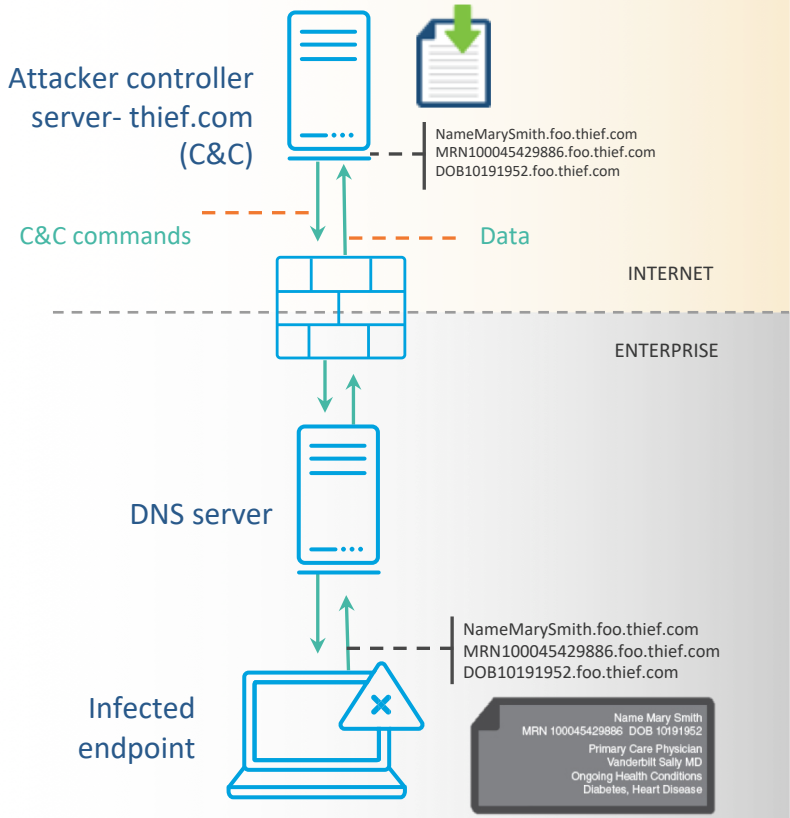
apple.com (Cyrillic)
apple.com (Latin)

Data exfiltration over DNS

1. Infected endpoint gets access to file
2. Encrypts, converts info into encoded format
3. Text broken into chunks and sent via DNS
4. Exfiltrated data reconstructed at other end

Data Exfiltration via host/subdomain
Simplified/unencrypted example:

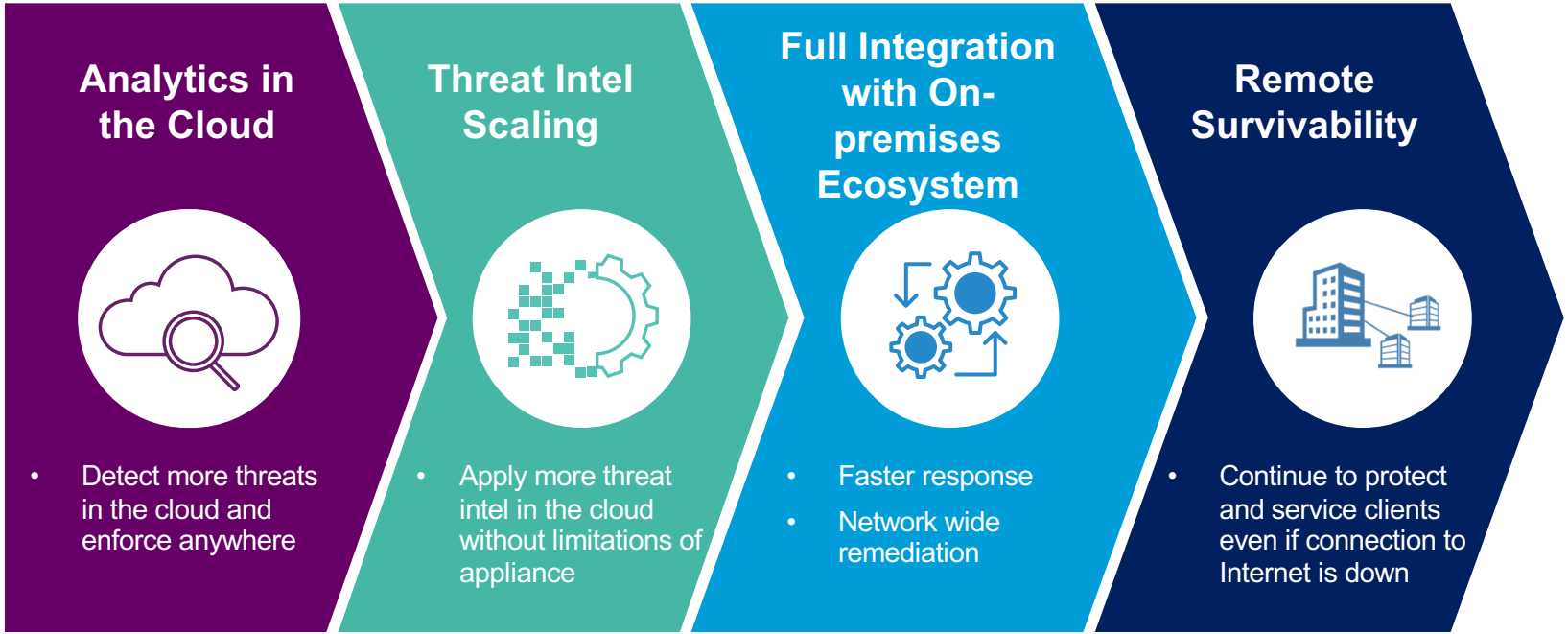
MarySmith.foo.thief.com
SSN-543112197.foo.thief.com
DOB-04-10-1999.foo.thief.com
MRN100045429886.foo.thief.com



Infoblox solution for Data Protection and Malware Mitigation

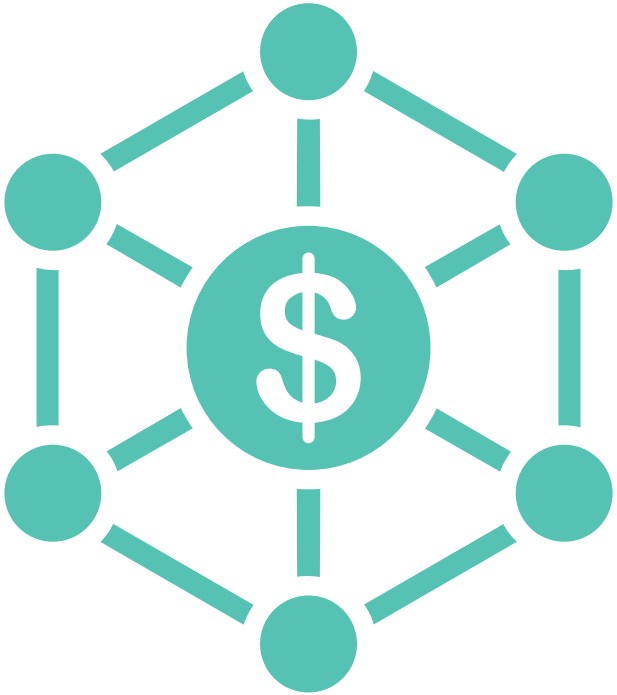
Using a Hybrid Approach

- "**The hybrid cloud will be used more regularly.** Organizations looking to exercise the advantages of the cloud without giving up proximity to data and security will invoke the hybrid cloud."[1] – Comport Technology Solutions



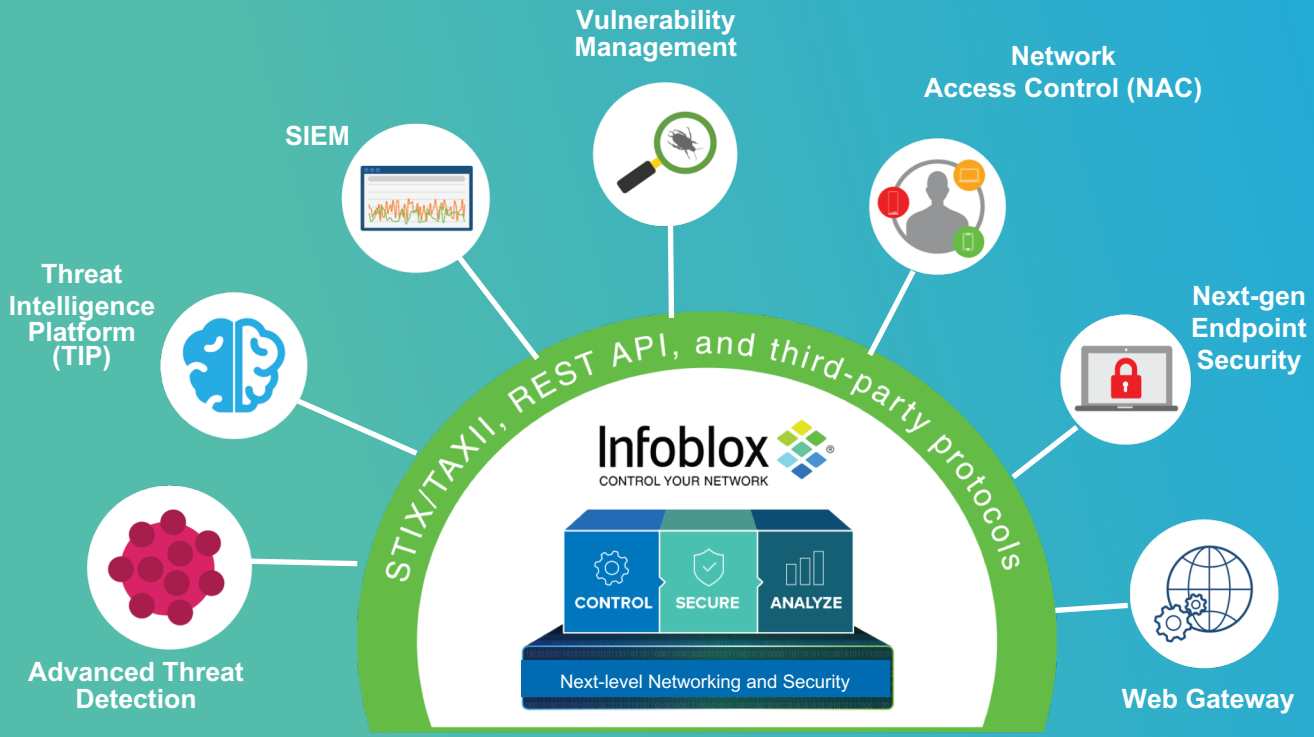
1. Three Top Cloud Computing Trends for 2019, Comport Technology Solutions

Reducing Cost of Existing Tech Stack



- DNS security more cost effective than perimeter defenses
- Immediately blocks known threats/offloads from more expensive perimeter defenses
- Infoblox makes existing security investments more effective

Accelerate Remediation with Ecosystem Integrations



Infoblox
NEXT LEVEL NETWORKING

- **Free Trials/software**
  - ActiveTrust Cloud eval
  - ActiveTrust (on-premises) eval
  - Security(PCAP) assessment

- **Come to our booth to discuss your security architectures**

- **Follow up with sales teams for deep dive on products**


Thank You
Asante
Shukria
Dhanyavadagalu
Vinaka
köszönöm
Kiitos
Maake
Manana
Dankon
Kam Sah Hammida
Matondo
Kasih
Terima
Taiku
Tack
Diolch i Chi
Chokrane
Grazie
Mochchakkeram
Tingki
Paldies
Gratias Tibi
Obrigado
Khun Khap
Kop
Kia Ora
Djiere Dieuf
Eskerrik Asko
Najis Tuke
Go Raibh Maith Agat
Salamat
Merci
Di Ou Mèsi
Hvala
Welalin
Danke
Matur Nuwun
Rahmat
Misaotra
Suksama
Děkuji
Ua Tsaug Rau Koj
Bedankt
Dakujem
Nirringrazzjak
Grazas
cảm ơn bạn
Arigato
Gracias
Juspaxar
Blagodaram
Ngiyabonga
Dziekuje
Dank Je
Danksheen
спасибо
Mauruuru
Biyan
감사합니다
Dankscheen