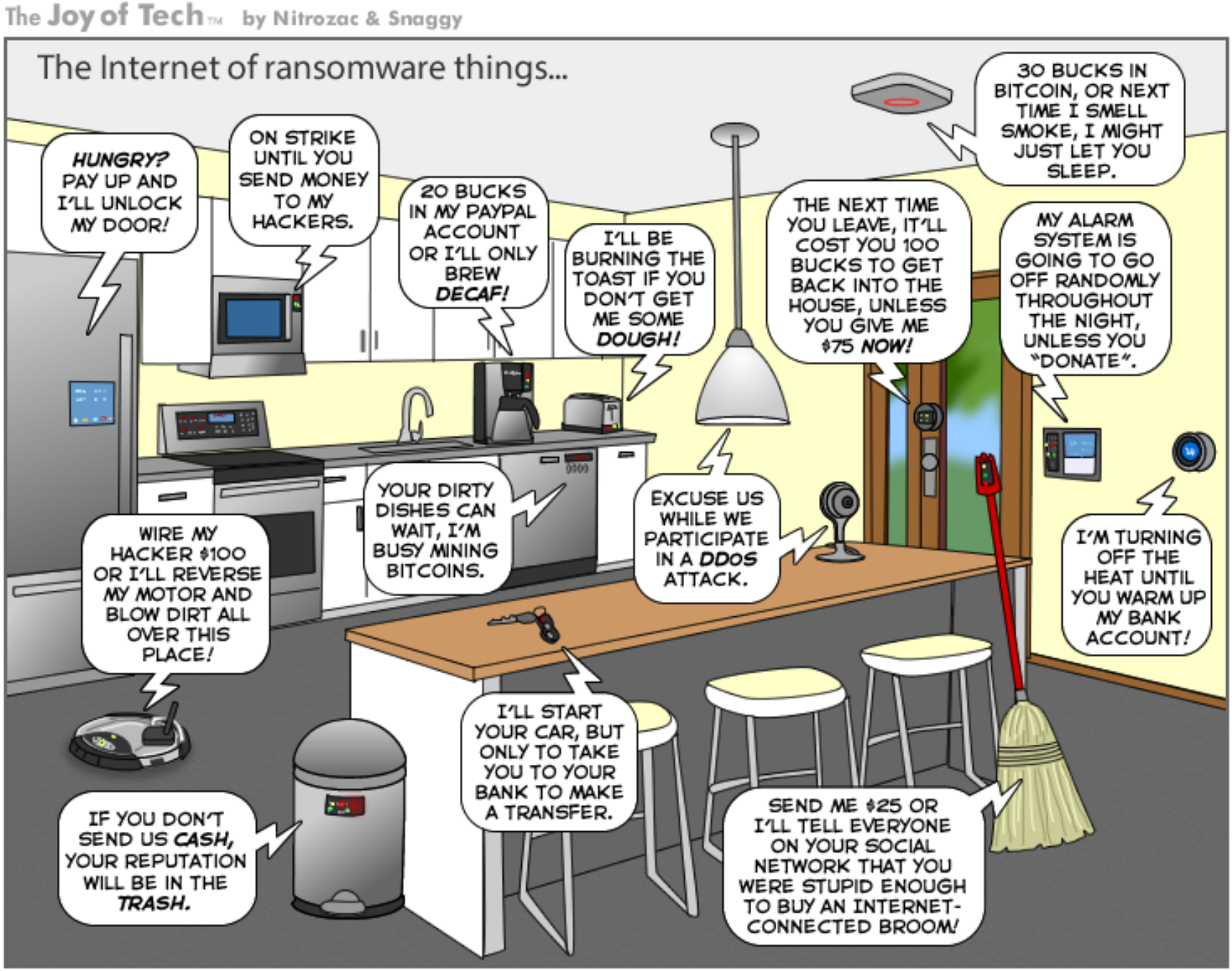
O que os Dados DNS Revelam sobre os Ataques Cibernéticos Mundiais

Ricardo Rodrigues
System Engineer, Latin America

O Sonho da Vida Conectada

nominum

IoT: Internet of Things? ou… Internet of Threats?



nominum

Ataques Cibernéticos

- BYOD, IoT e botnets trazem novos desafios
  - O que fazer se o ataque vem de dentro da sua rede?
    - Bloquear milhares de assinantes infectados?

Ataques Cibernéticos

- BYOD, IoT e botnets trazem novos desafios
  - O que fazer se o ataque vem de dentro da sua rede?
    - Bloquear milhares de assinantes infectados?
  - Como mitigar o ataque sem prejudicar o assinante?
    - É preciso bloquear o tráfego malicioso e permitir o legítimo

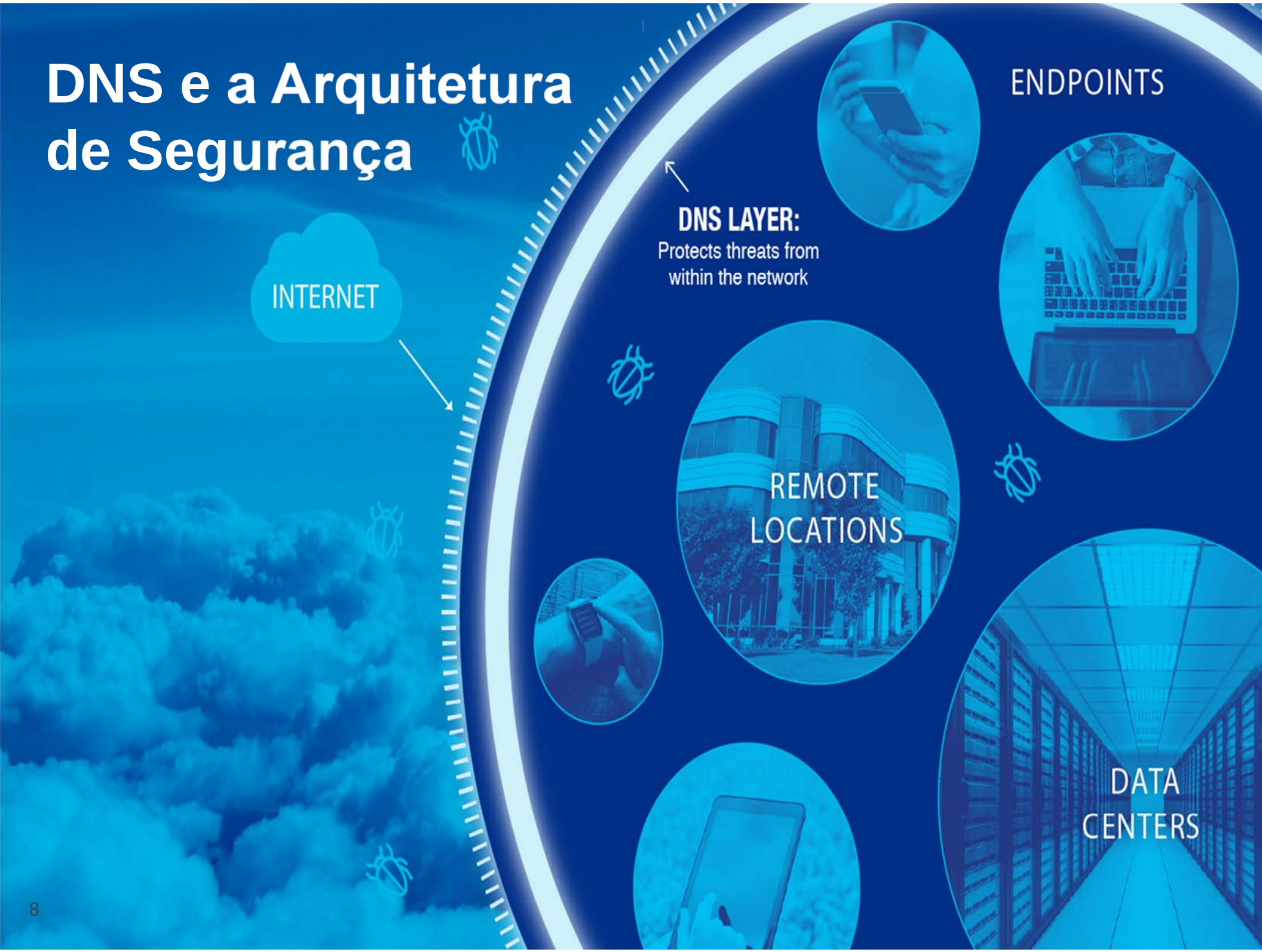
Ataques Cibernéticos

- BYOD, IoT e botnets trazem novos desafios
  - O que fazer se o ataque vem de dentro da sua rede?
    - Bloquear milhares de assinantes infectados?
  - Como mitigar o ataque sem prejudicar o assinante?
    - É preciso bloquear o tráfego malicioso e permitir o legítimo
- É possível ser pró-ativo?
  - Como identificar os assinantes infectados?
  - É possível impedir que assinantes infectados gerem ataques?

Ataques Cibernéticos

- BYOD, IoT e botnets trazem novos desafios
  - O que fazer se o ataque vem de dentro da sua rede?
    - Bloquear milhares de assinantes infectados?
  - Como mitigar o ataque sem prejudicar o assinante?
    - É preciso bloquear o tráfego malicioso e permitir o legítimo
- É possível ser pró-ativo?
  - Como identificar os assinantes infectados?
  - É possível impedir que assinantes infectados gerem ataques?
- É preciso adicionar novos elementos na rede?
  - Ou posso fazer melhor uso dos existentes?

DNS e a Arquitetura de Segurança



Nominum Data Science Security Analysis

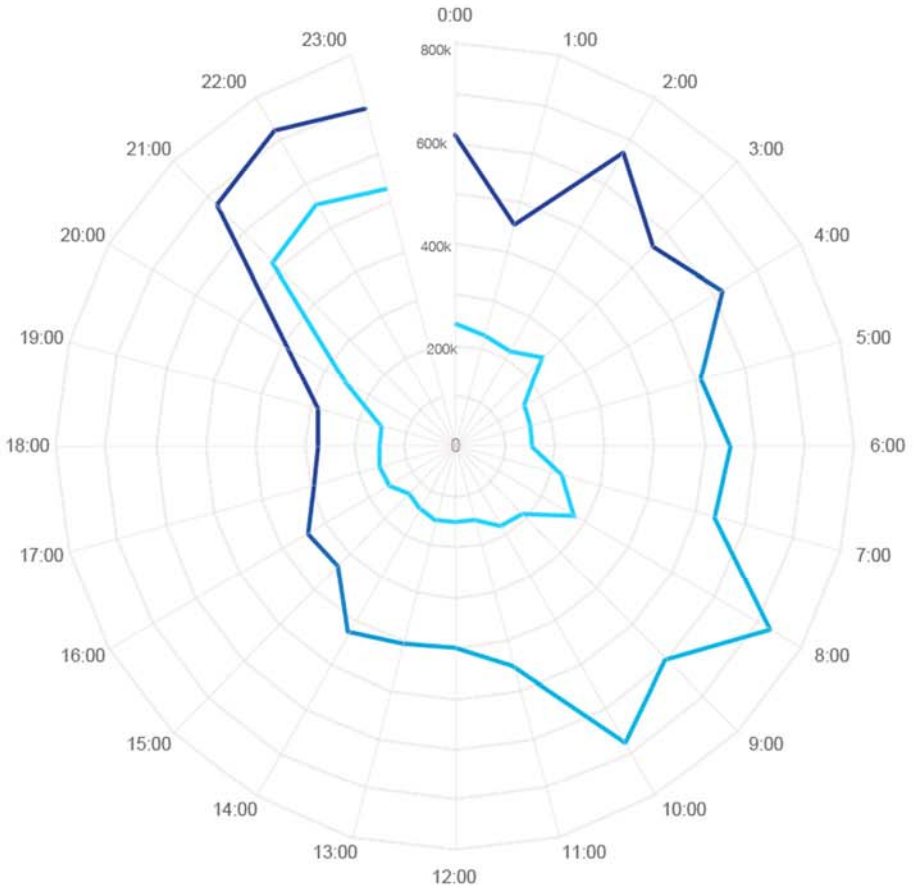
Dados DNS	
Métrica	**Valor**
Período Analisado	01/mar/2016 – 31/ago/2016
Total de Consultas DNS	14.700.000.000.000
Número Médio de Nomes DNS Únicos por dia	422.900.000

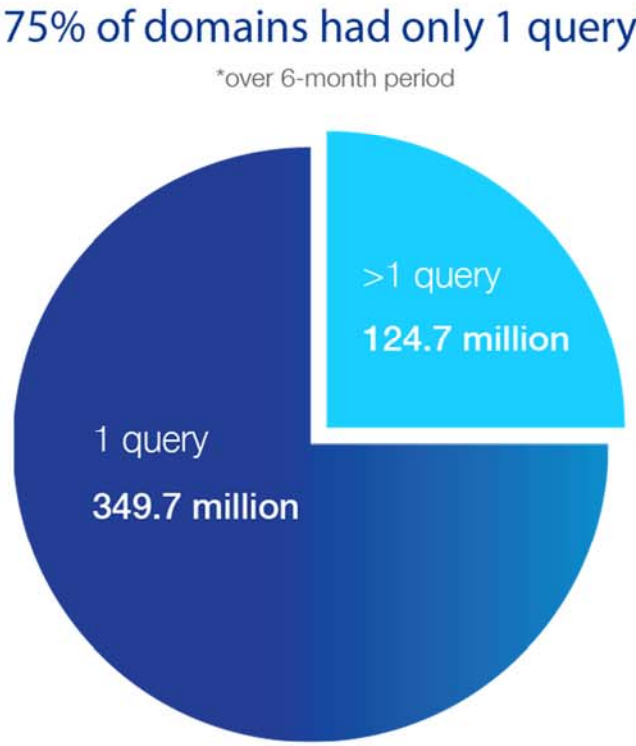
Aprox 3% do tráfego global total

nominum

Panorama das Ameaças

Novos Nomes DNS – Período de 24 horas





NEW DOMAINS PER DAY

5 million

NEW DOMAINS PER MONTH

150 million

NEW DOMAINS MARCH – AUG 2016

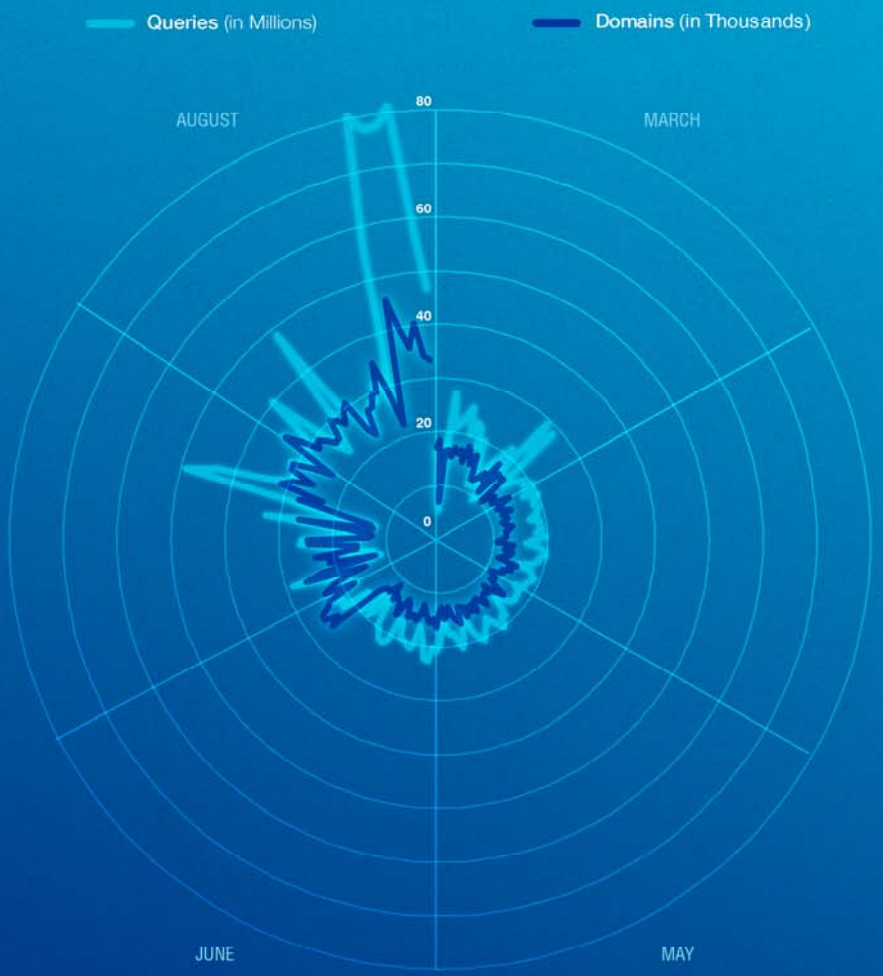
1 billion

nominum

Threat Tracker 2016

3X growth
in queries
and domains

82 million
malicious
queries daily
(by end of Aug)

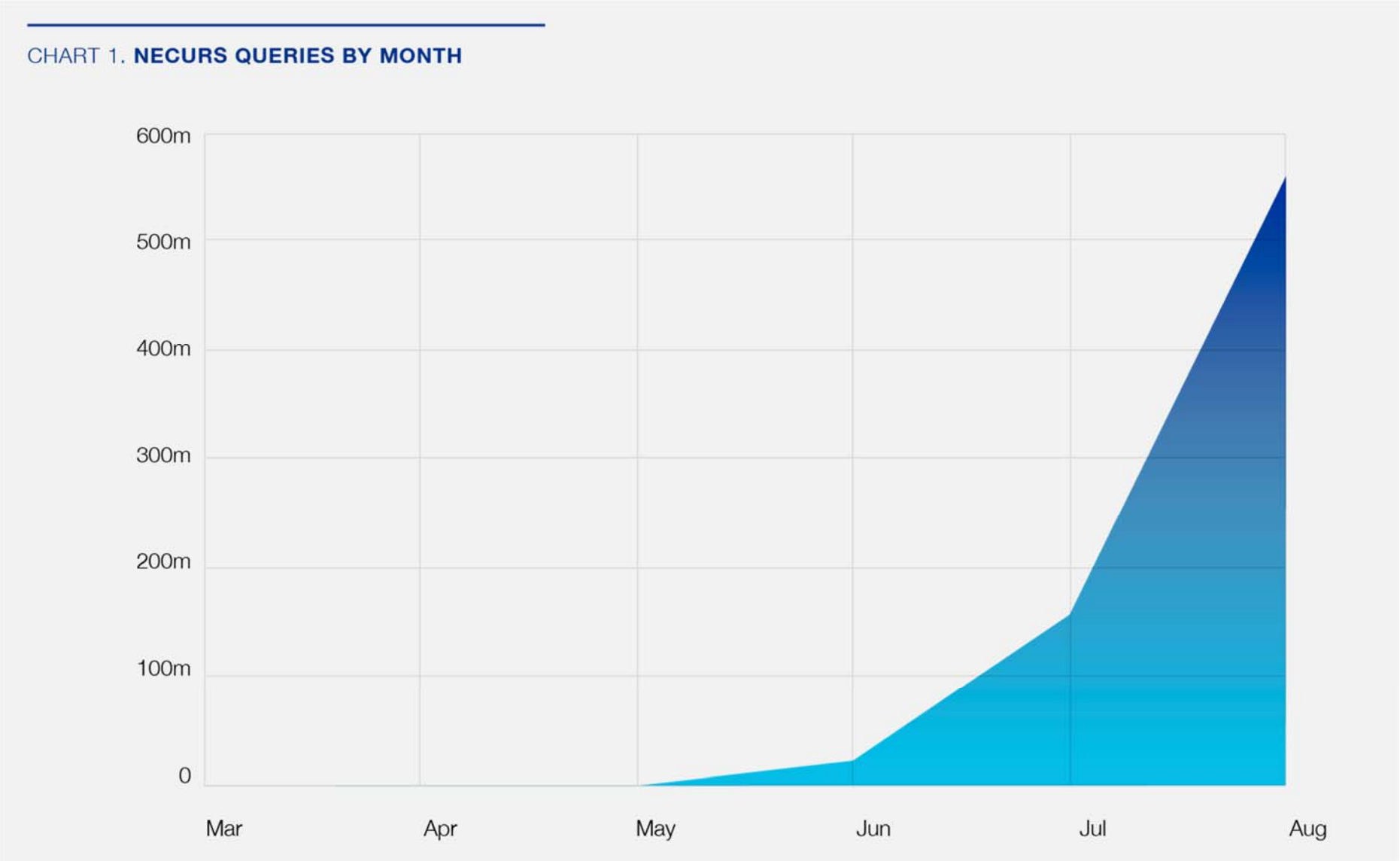


94,000
domains added
daily to block list

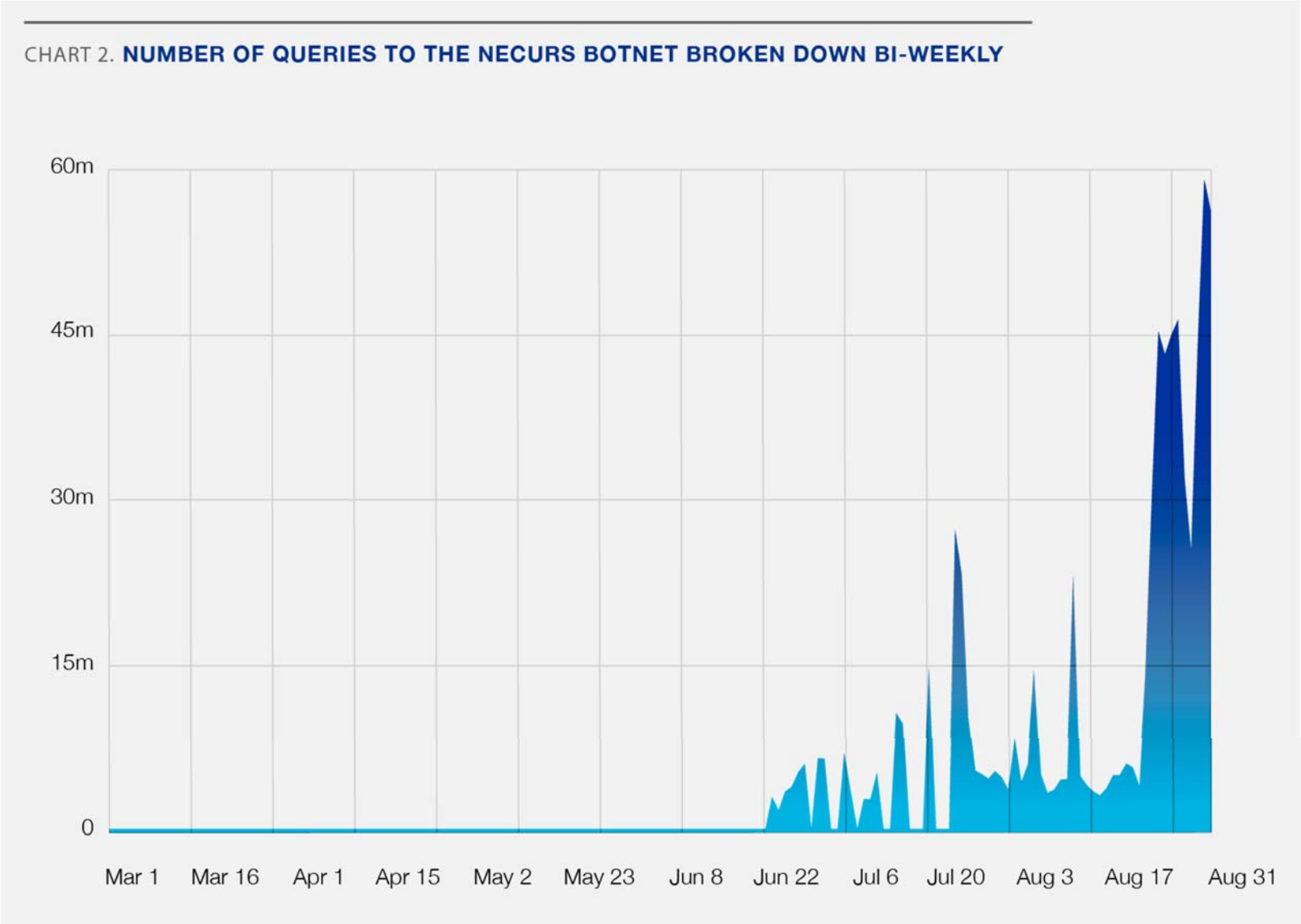
nominum

Principais Ameaças Identificadas

Necurs: Número de Consultas / Mês

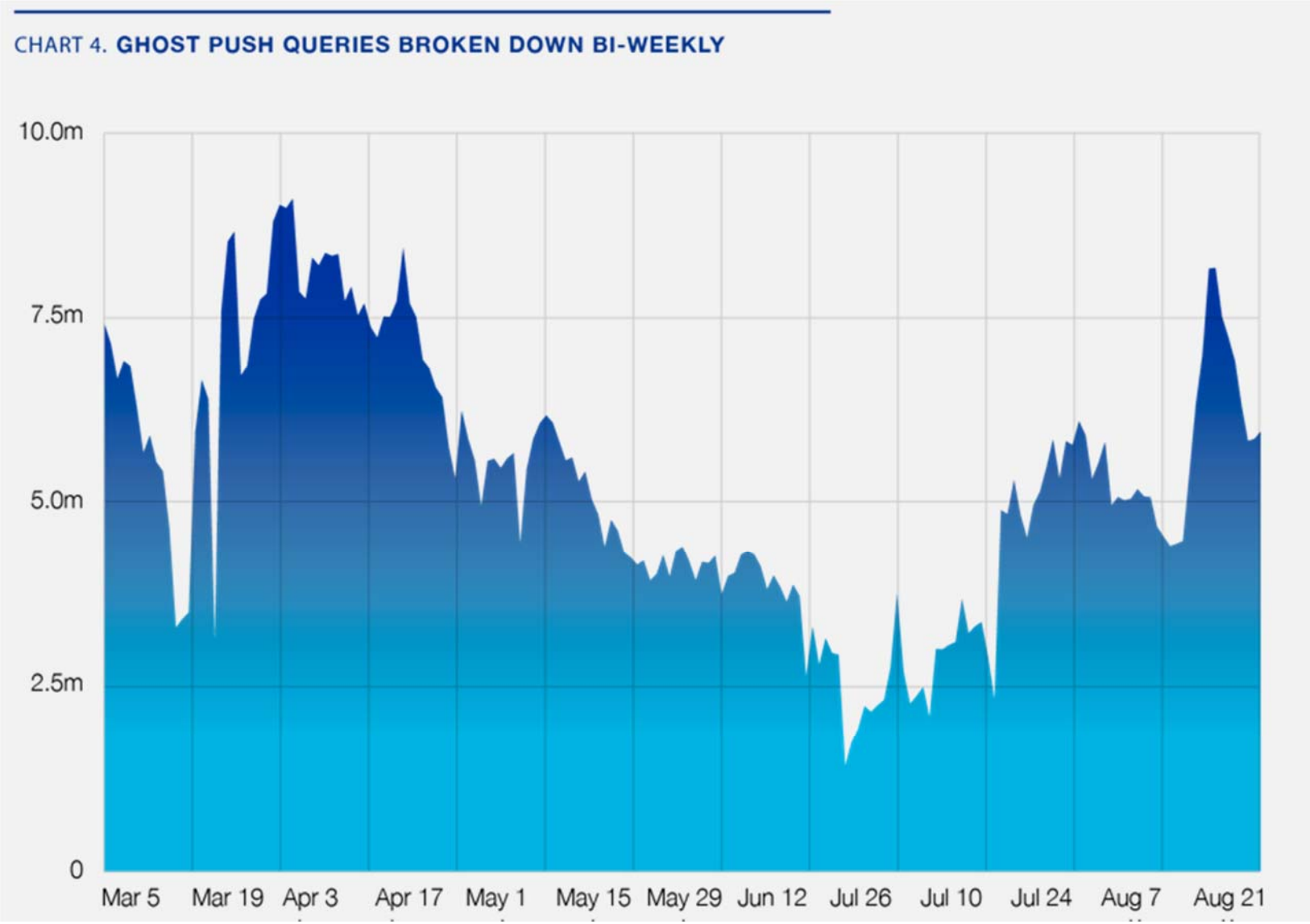


Necurs: Número de Consultas / Quinzena



nominum

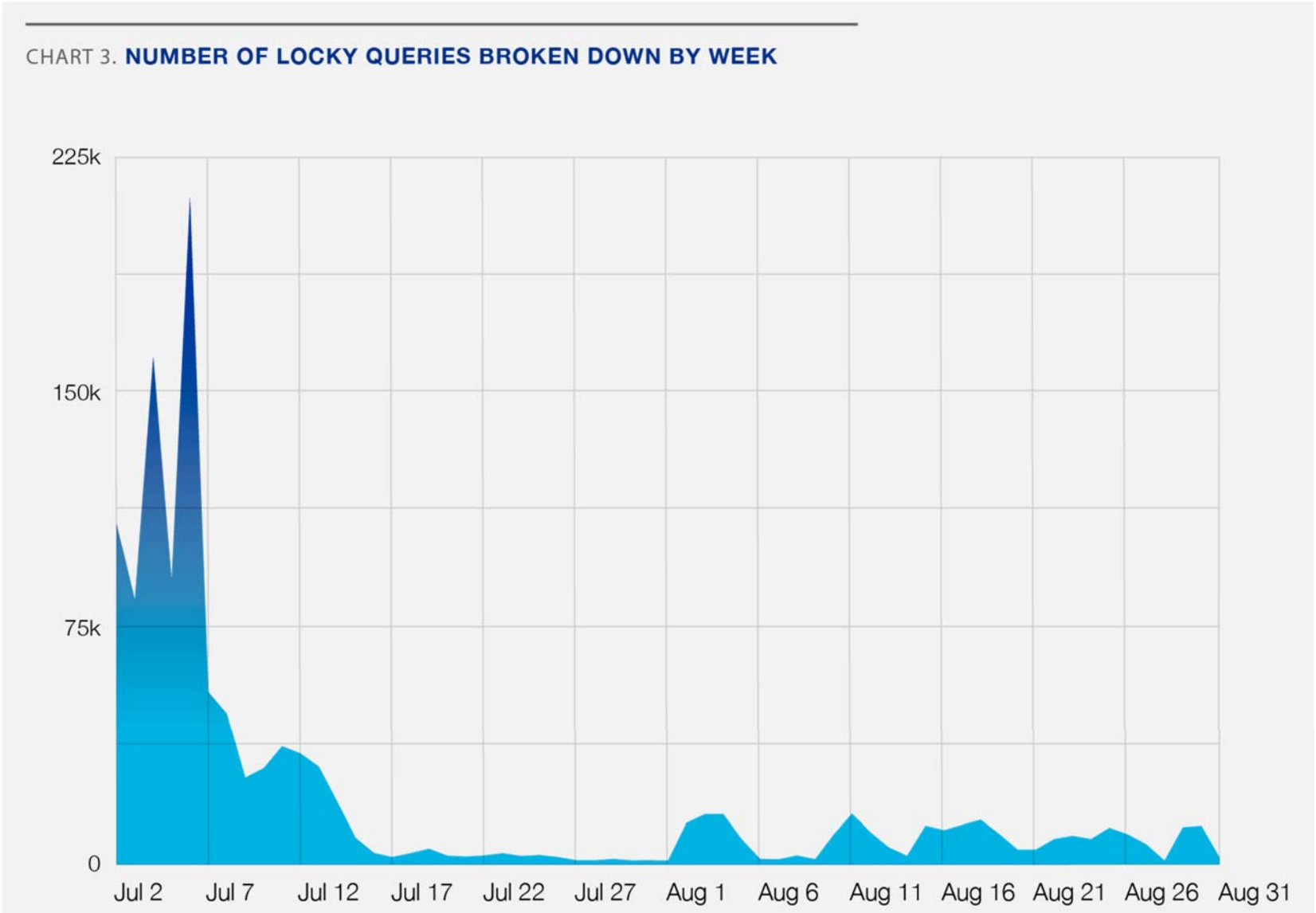
Ghost Push: Malware para Android



nominum

Locky: Ransomware

CHART 3. **NUMBER OF LOCKY QUERIES BROKEN DOWN BY WEEK**



nominum

Locky by the numbers

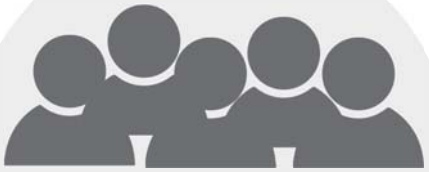
7 in 10	160	90,000
Malicious email attachments delivered by Locky in Q2 2016[1]	File types that can be encrypted by Locky (e.g., .docx, .jpeg, .xlsx)[2]	Devices infected daily around the world[3]
$ 459	**$ 17,000**	**$1.6M per day**
Average ransom demand (BTC 0.5 to 1.00)[3]	Largest Locky payout to date[3]	Average daily payout by Locky at the current bitcoin exchange rate[3]

[1] https://blog.barkly.com/ransomware-statistics-2016
[2] https://blog.avast.com/a-closer-look-at-the-locky-ransomware
[3] http://www.smartdatacollective.com/david-balaban/412688/locky-ransomware-statistics-geos-targeted-amounts-paid-spread-volumes-and-much

Mirai

50,000 bots
PRSD
3 Alvos

Código
disponibilizado
30/Setembro

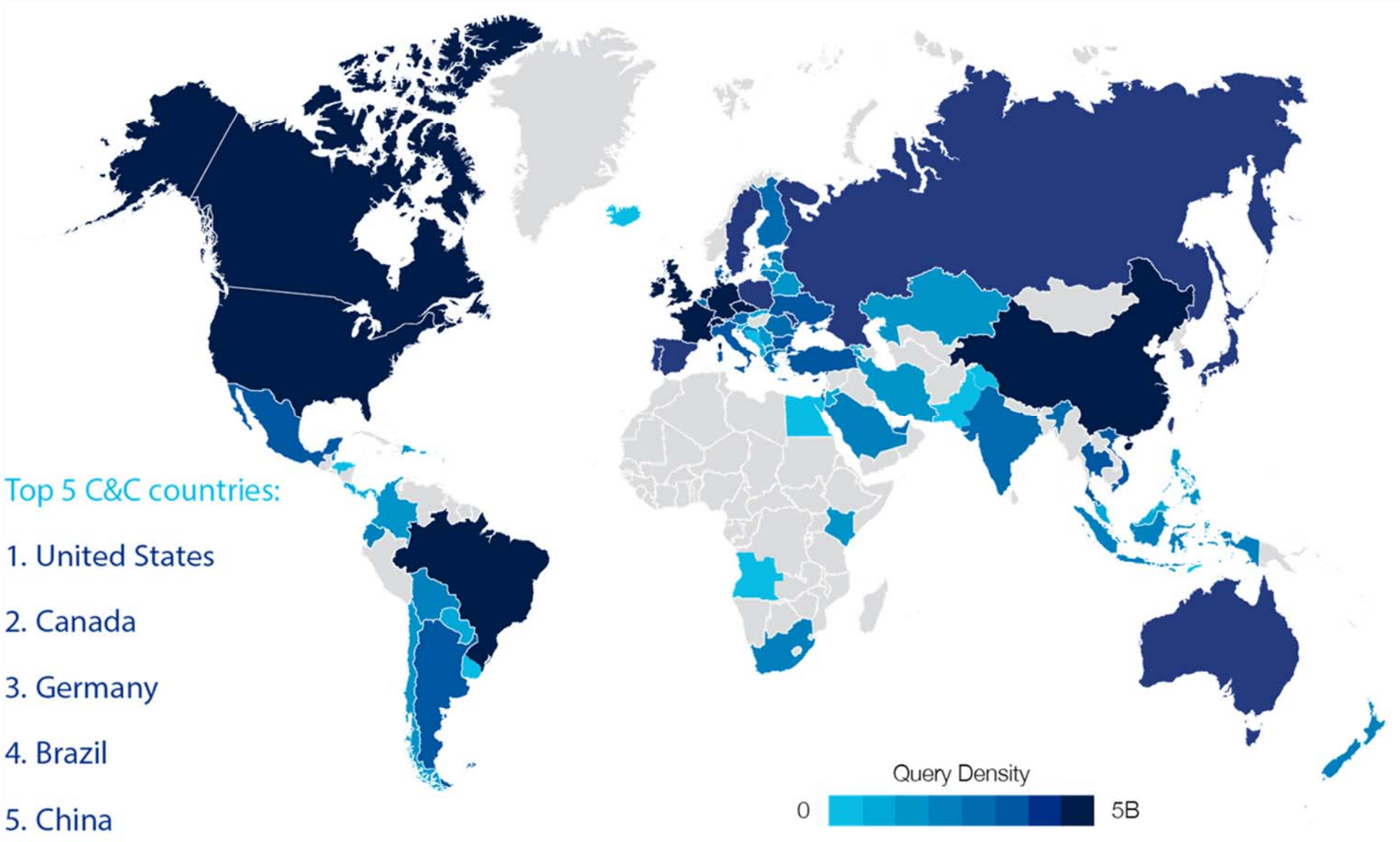


 # Alvos:
Up 5-6X

nominum

Localização das Ameaças

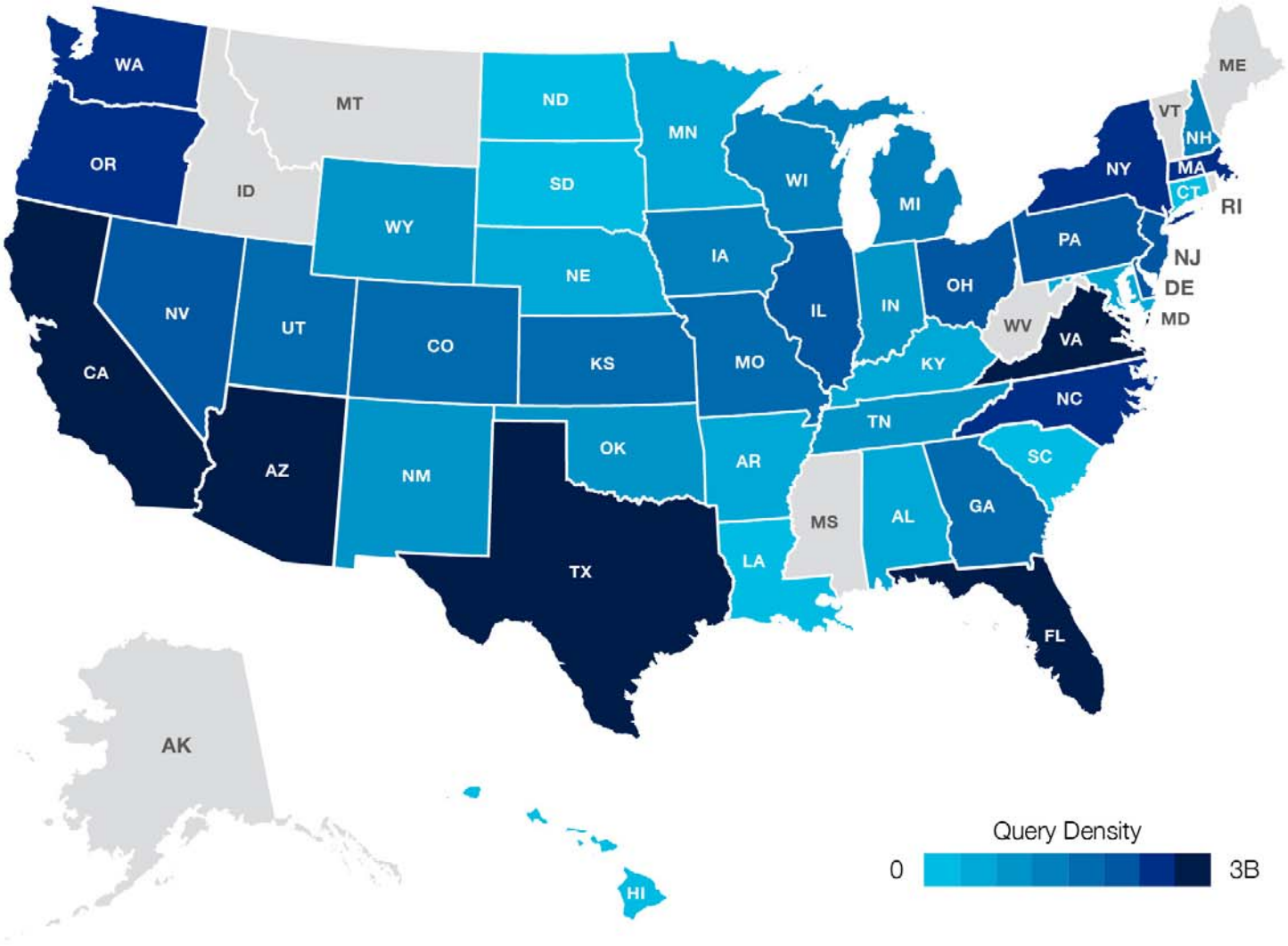
Localização de C&C – Mundo



nominum

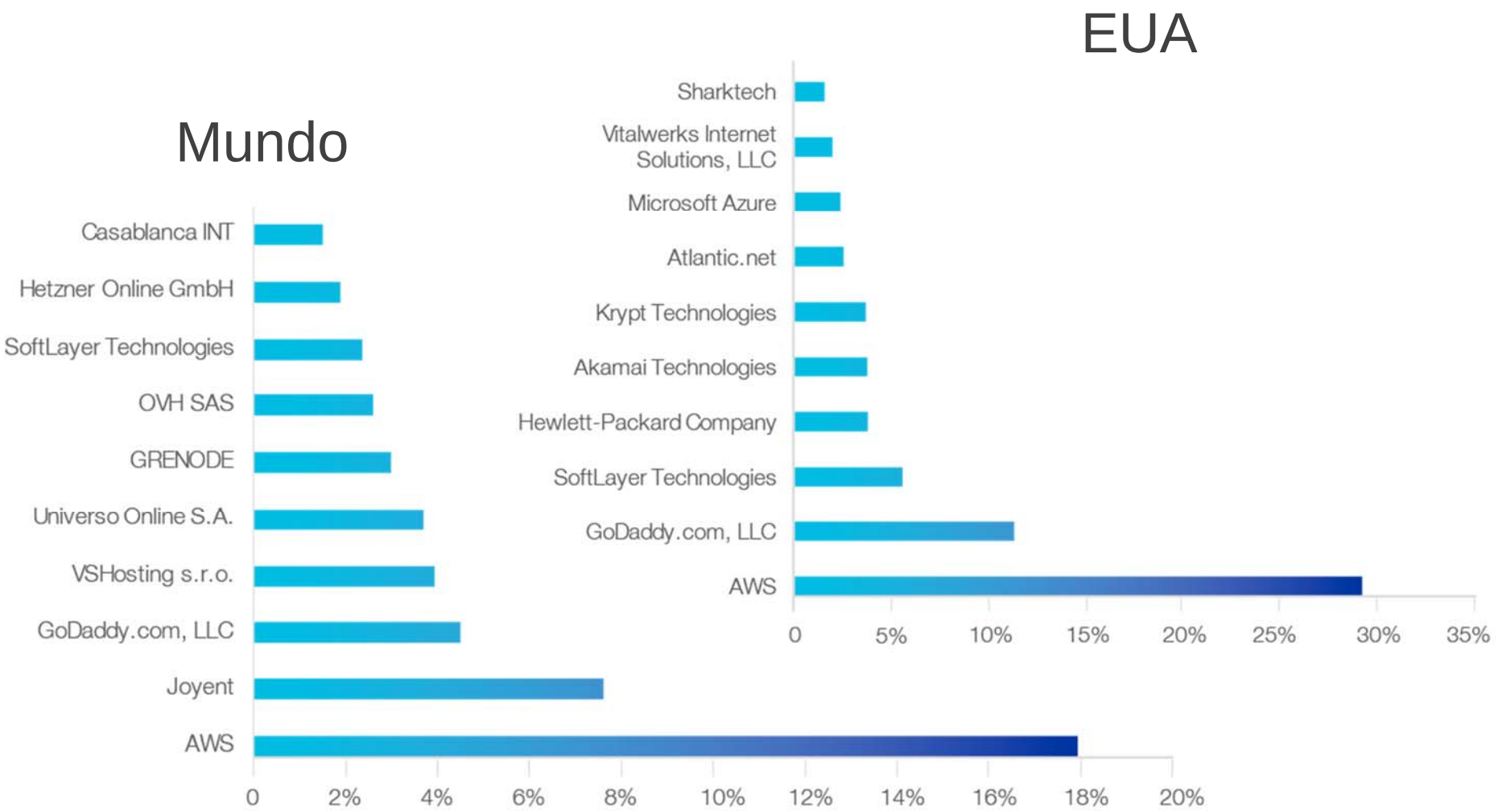
Localização de C&C – EUA

1. California
2. Virginia
3. Arizona
4. Texas
5. Florida



nominum

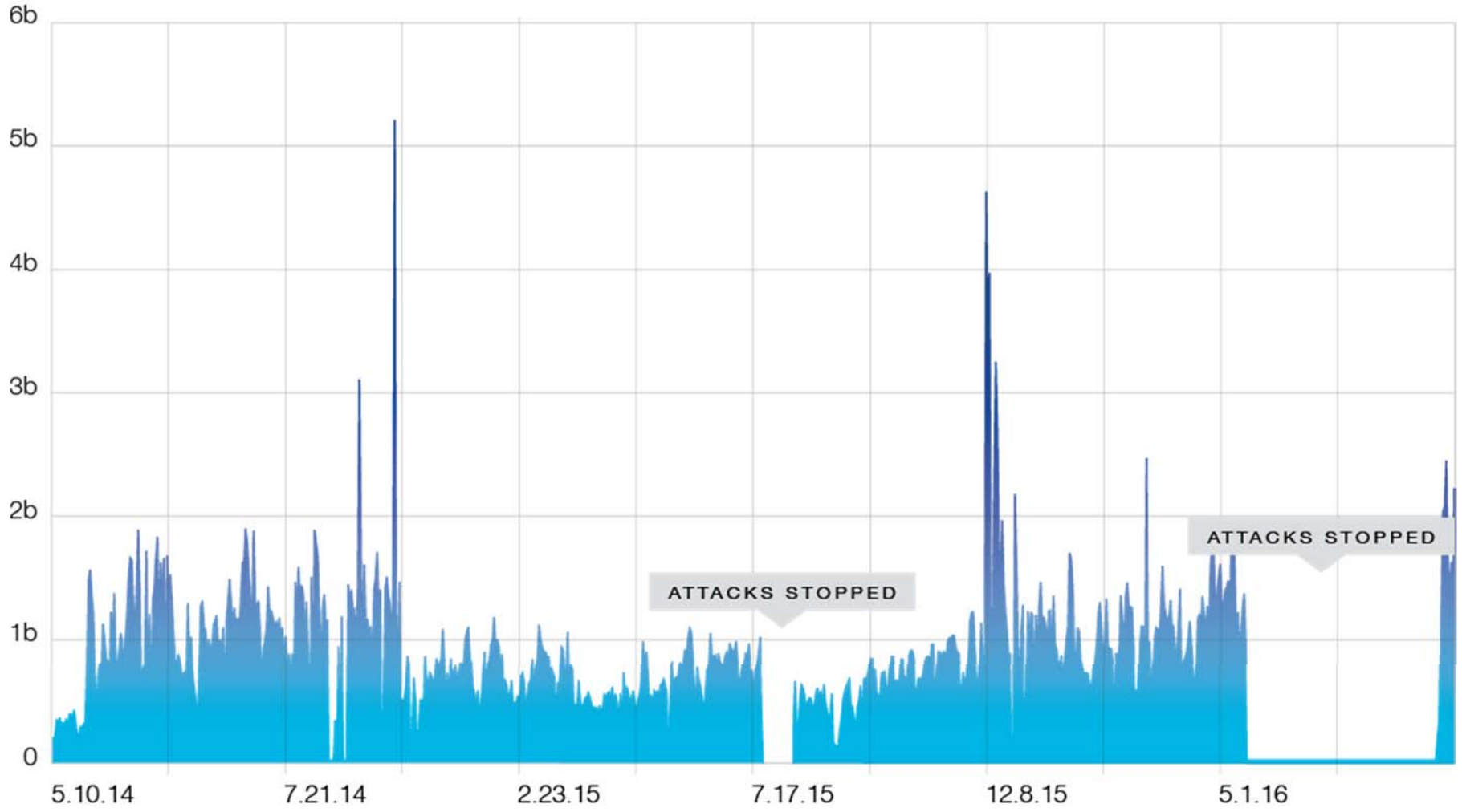
Hospedagem de Malware



nominum

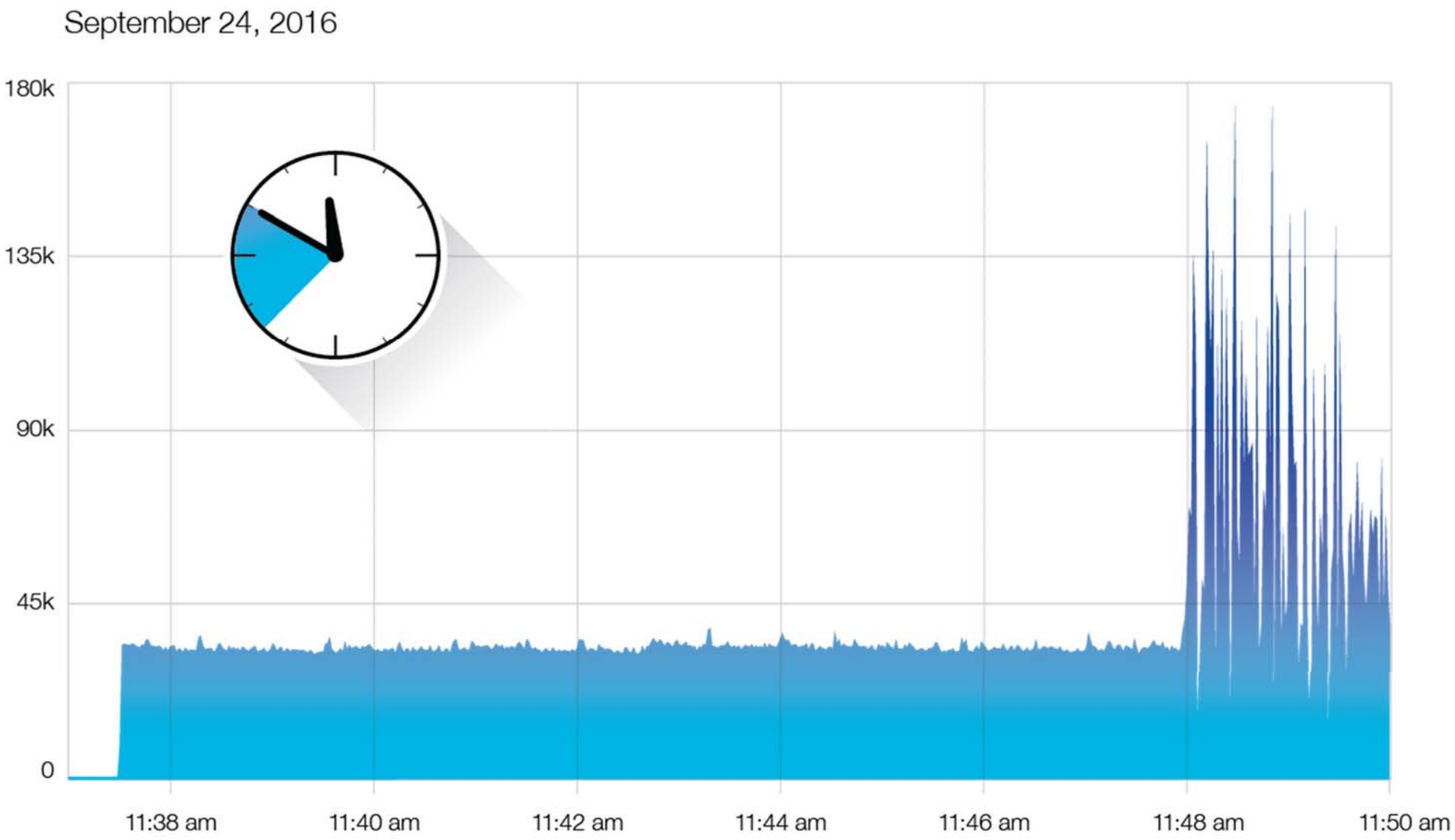

Mergulhando em
DDoS e Amplificação DNS

Ataques PRSD nos últimos 2 anos



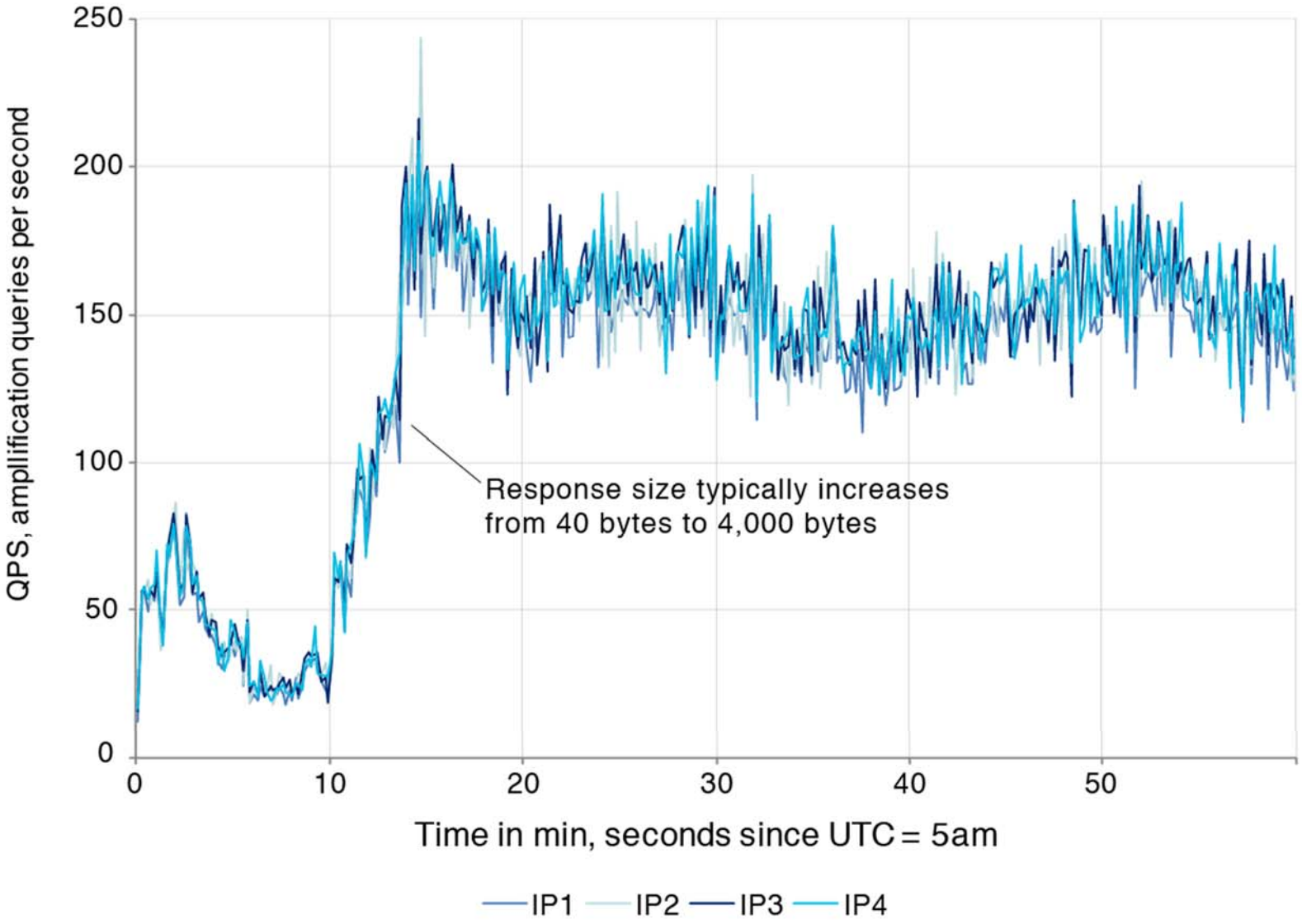
nominum

12 Minutos de um Ataque PRSD



nominum

Amplificação DNS



Conclusões

- Aumento significativo dos ataques DDoS e botnets
- BYOD e IoT introduzem novos desafios
- DNS é elemento chave para prevenção e mitigação

Considerações Finais

- Download do Nominum Data Science Security Report:

  http://nominum.com/resource/security-report-home

Considerações Finais

- Download do Nominum Data Science Security Report:

  http://nominum.com/resource/security-report-home

Para Pensar:

- Seu servidor DNS sempre responde a resposta correta?

Considerações Finais

- Download do Nominum Data Science Security Report:

  http://nominum.com/resource/security-report-home

Para Pensar:

- Seu servidor DNS sempre responde a resposta correta?
- A resposta correta protege o usuário?


Muito Obrigado !