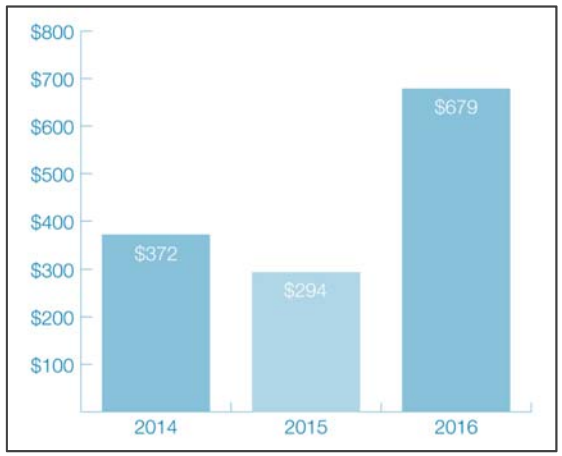
The Importance of DNS in Preventing Global Cyber Attacks

Ricardo Rodrigues

nominum

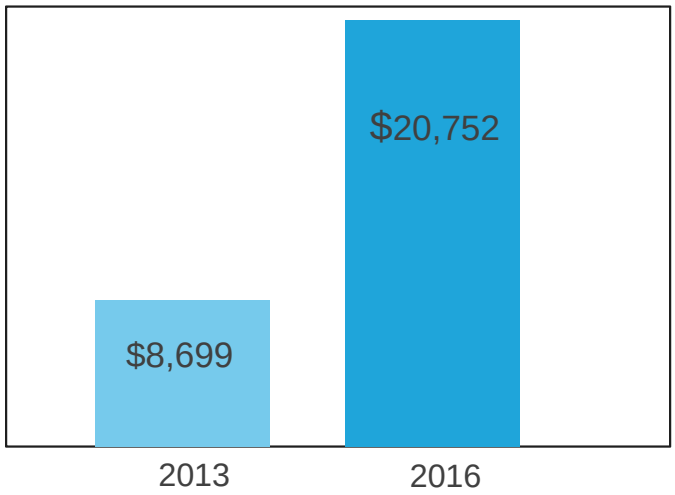
Effective Internet Security Has Never Been More Important

The cost of security incidents has increased, driven by Ransomware



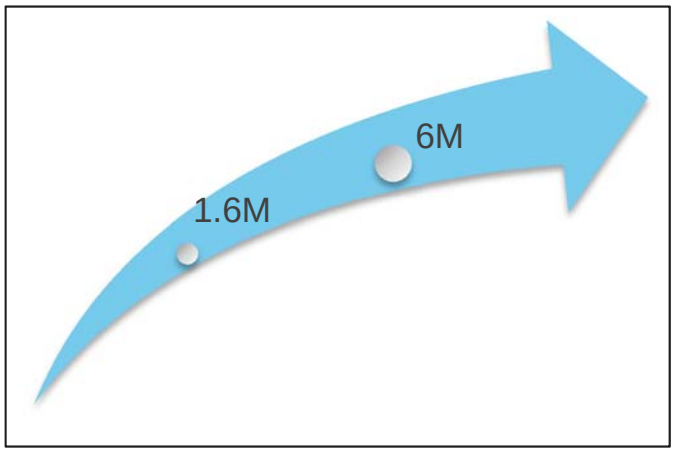
Average ransomware cost to a **consumer**

Source: Symantec



Average ransomware cost to a **business**

Source: SBIR

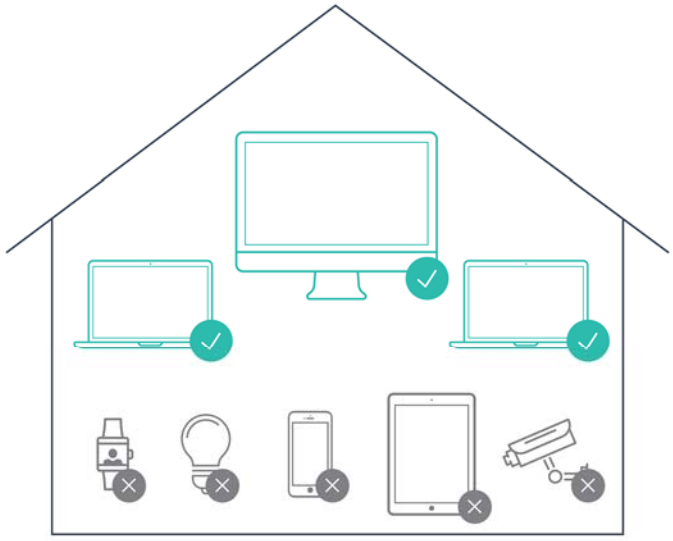


Attack queries grew **270 percent** from Fall 2016 to Spring 2017

Source: Nominum

Mobile & IoT Devices Are At Risk

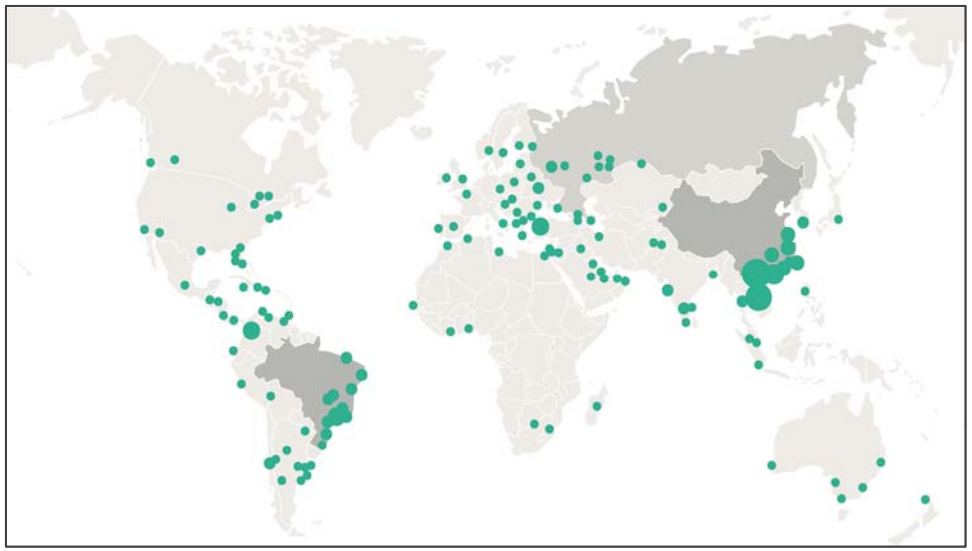
End-user Devices Remain Unprotected



END POINT SECURITY
Protects limited devices like laptops.

As IoT Attacks Are on the Rise

Worldwide Mirai Infections



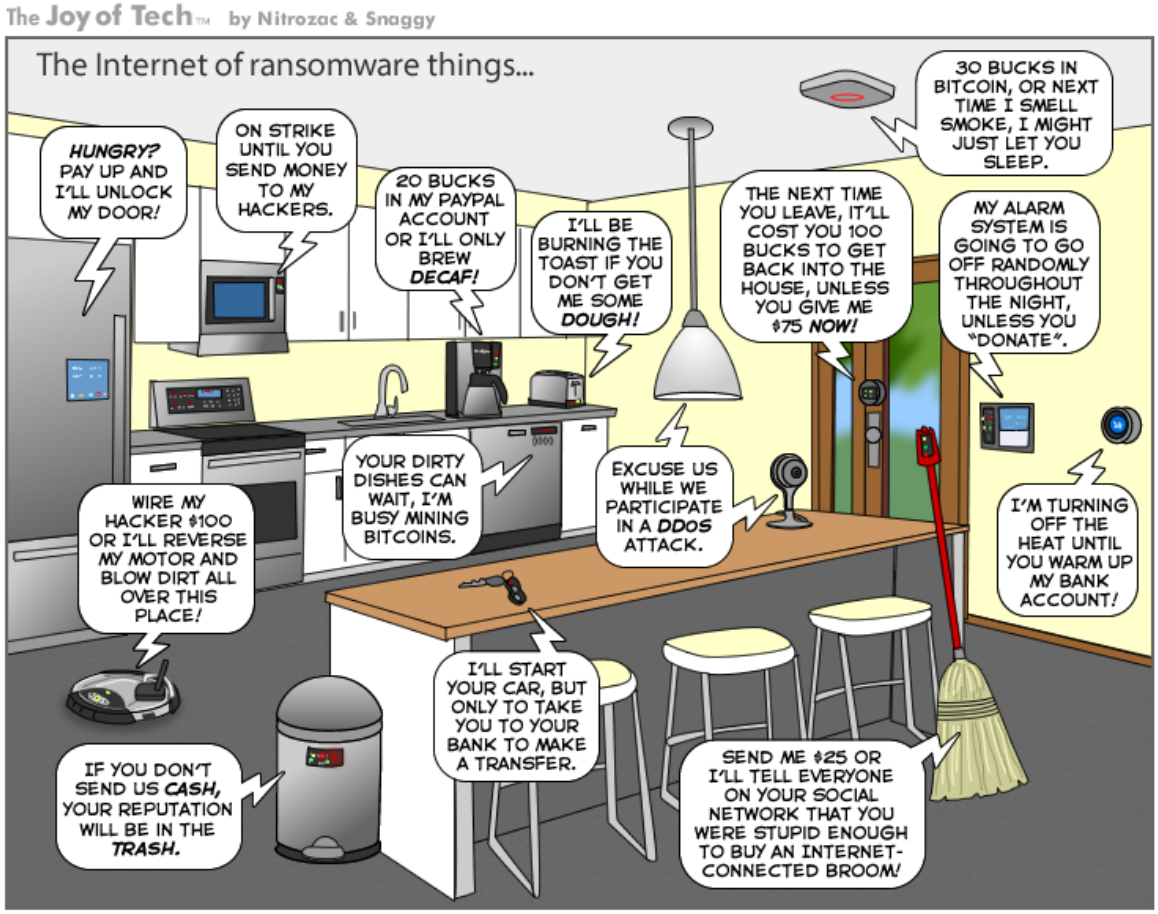
Source: 360 and Nominum

nominum

The Dream of the Connected Life

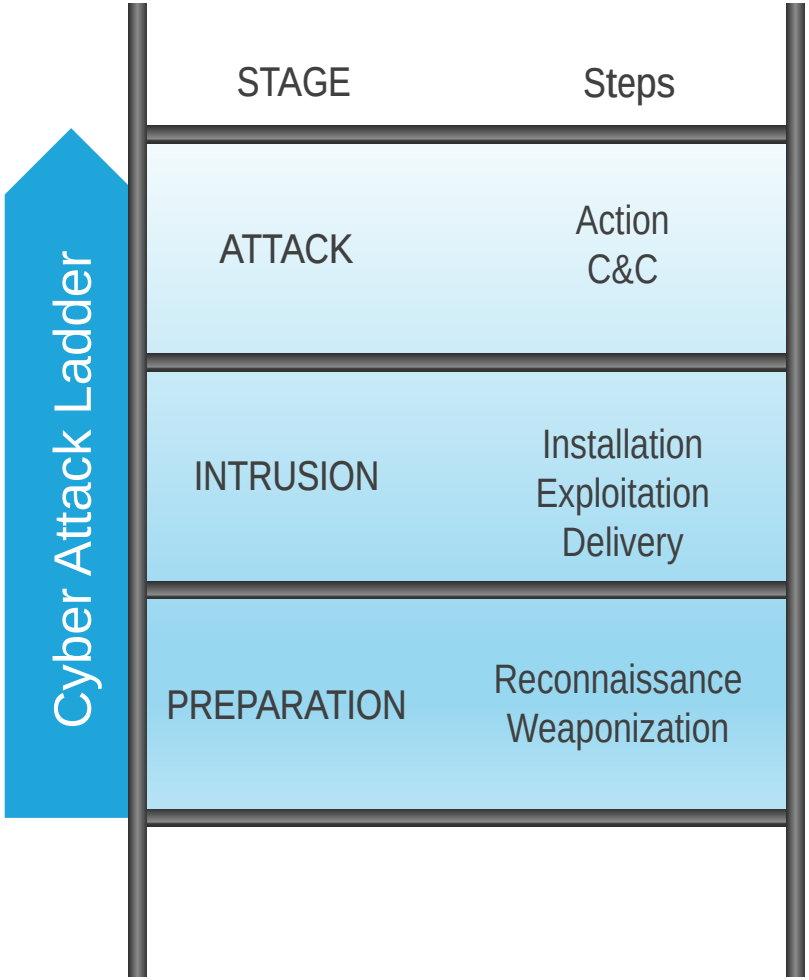
nominum

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



nominum

Cyber Attack Ladder



nominum

Cyber Attacks

BYOD, IoT and botnets bring new challenges

- What to do if the attack comes from inside your network?
  - Block thousands of infected subscribers?
- How to mitigate the attack without harm to the subscriber?
  - It is imperative to block the malicious traffic and allow the good

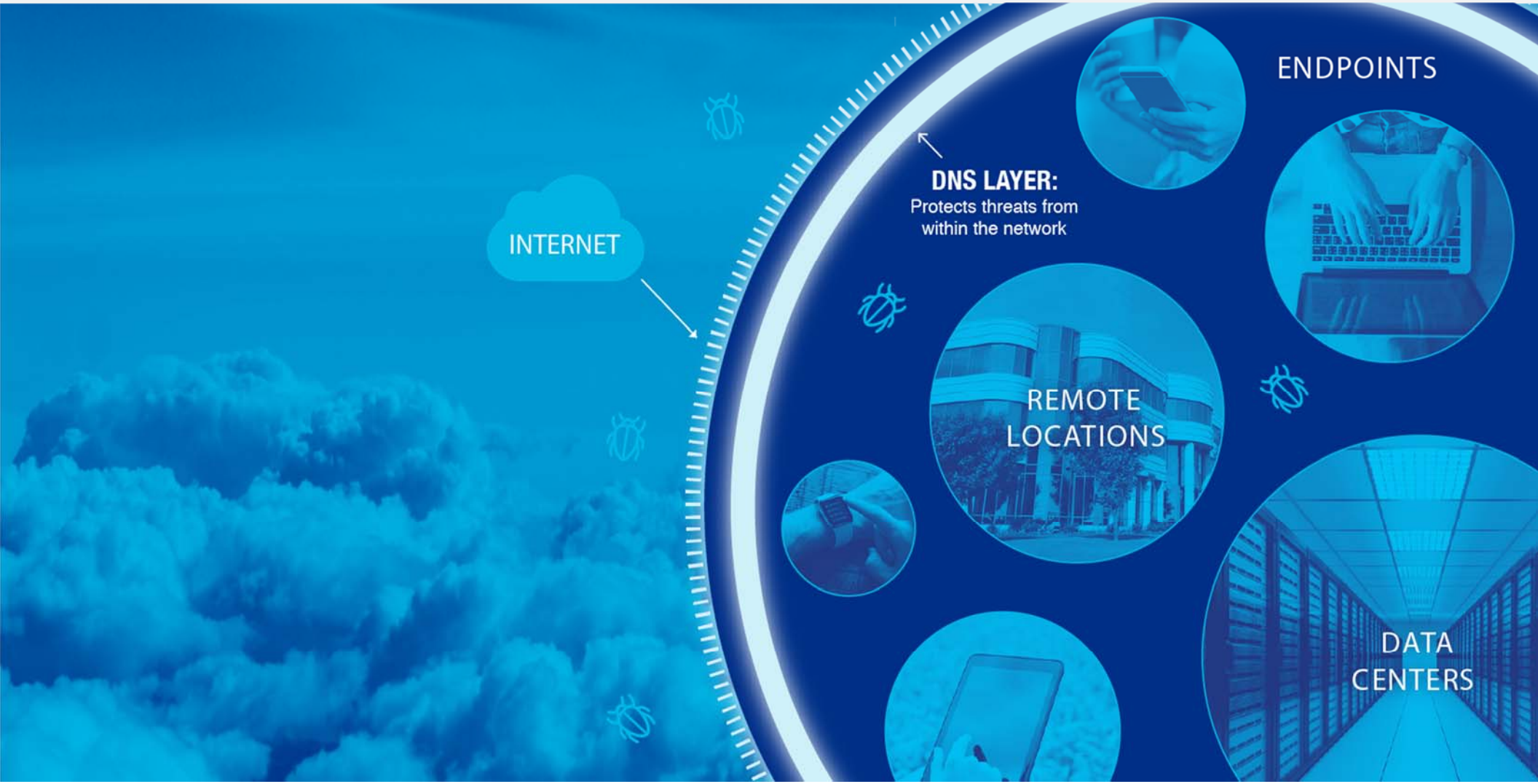
Is this possible to be proactive?

- How to identify infected subscribers?
- Is this possible to avoid that infected subscribers generate attacks?

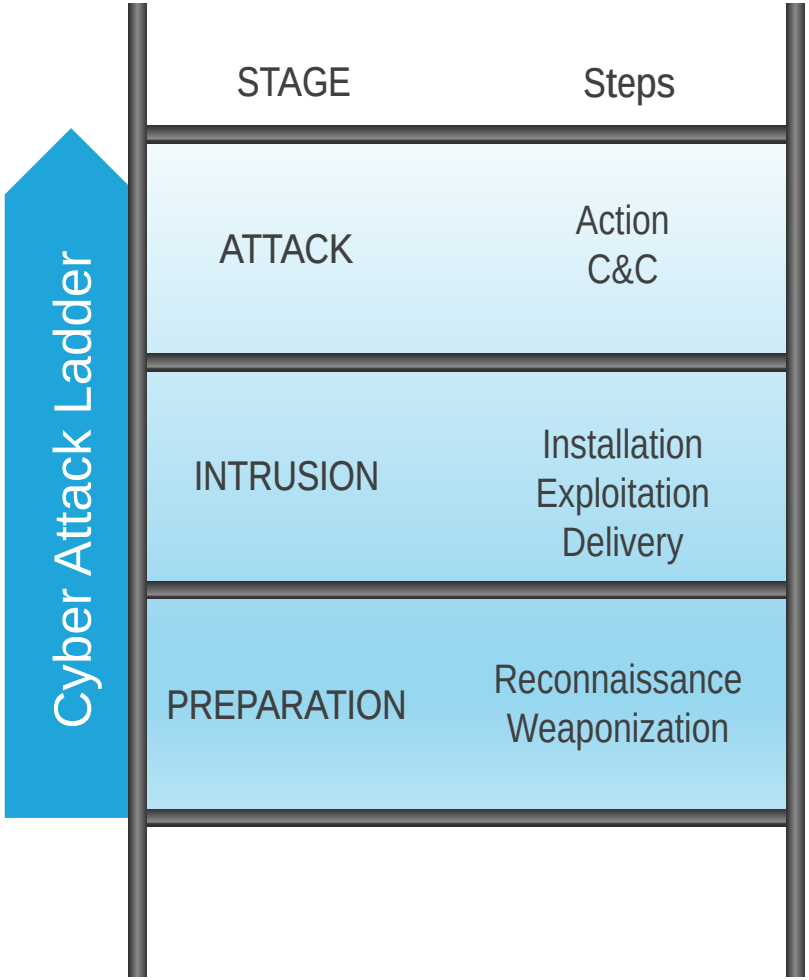
Is this required to change the network architecture?

- Or can we have a better usage of the existing elements?

DNS and the Security Architecture



DNS Can Help at Every Stage of an Attack



How DNS Helps

- Block purpose-built DNS Amp domains
- Rate-limit dual-use DNS Amp domains
- Block malicious subdomains (PRSD)
- Block DNS tunneling domains
- Block command and control domains

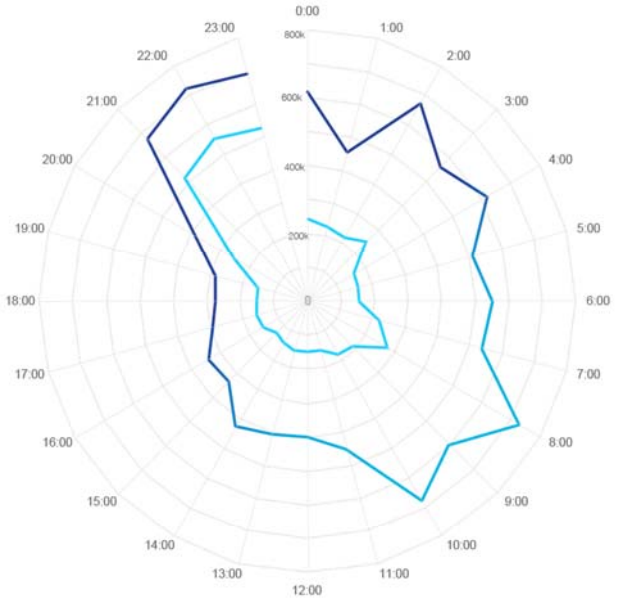
- Block phishing domains
- Block domains hosting exploit kits
- Block malware download domains
- Redirect & block HTTP paths for compromised websites
- Block malware drop sites
- Block domains used to download files for encryption

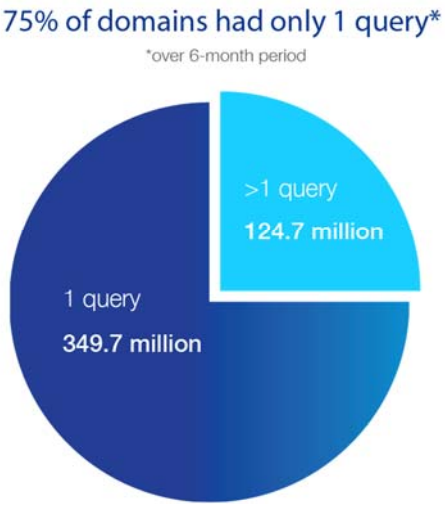
- Monitor or block domains assoc. with criminal infrastructure
- Monitor or block traffic to illegal download sites
- Block categories of domains frequently serving malware
- Identify anomalous DNS request for further investigation

nominum

01 Threat Landscape

New DNS Domains – every 24 hours





NEW DOMAINS PER DAY

5 million

NEW DOMAINS PER MONTH

150 million

NEW DOMAINS MARCH – AUG 2016

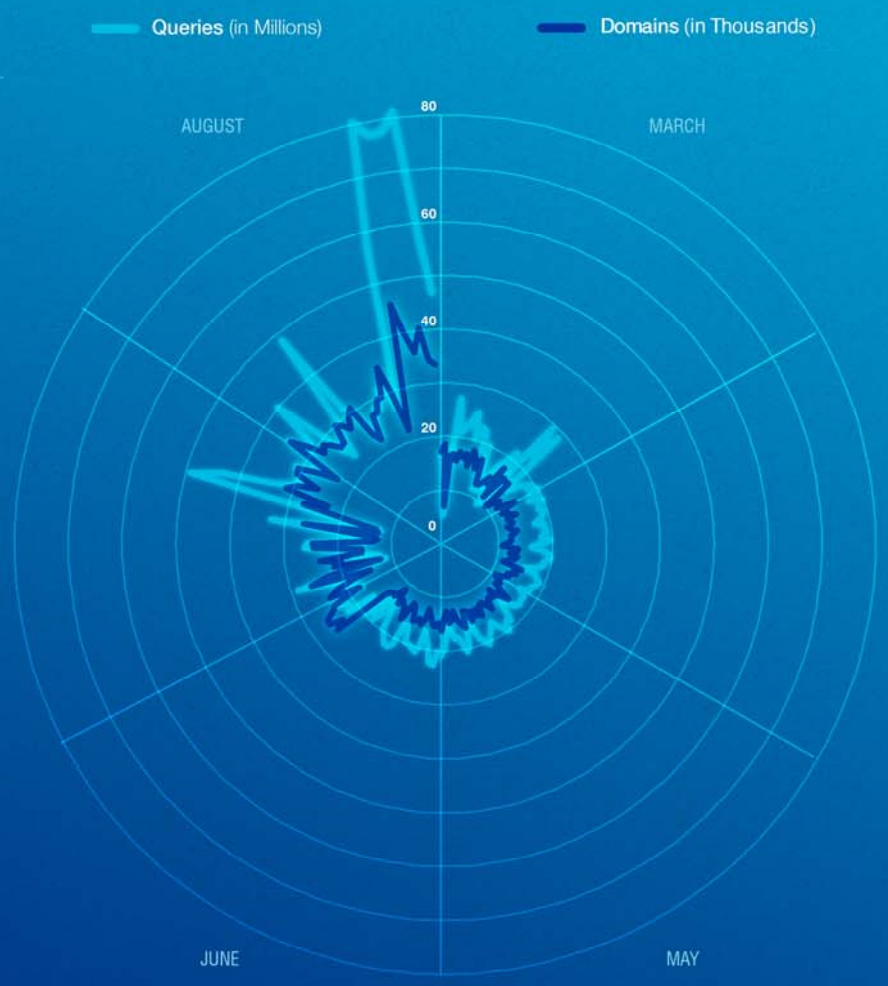
1 billion

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

Threat Tracker 2017

HIGHEST MALICIOUS QUERIES IN A SINGLE DAY

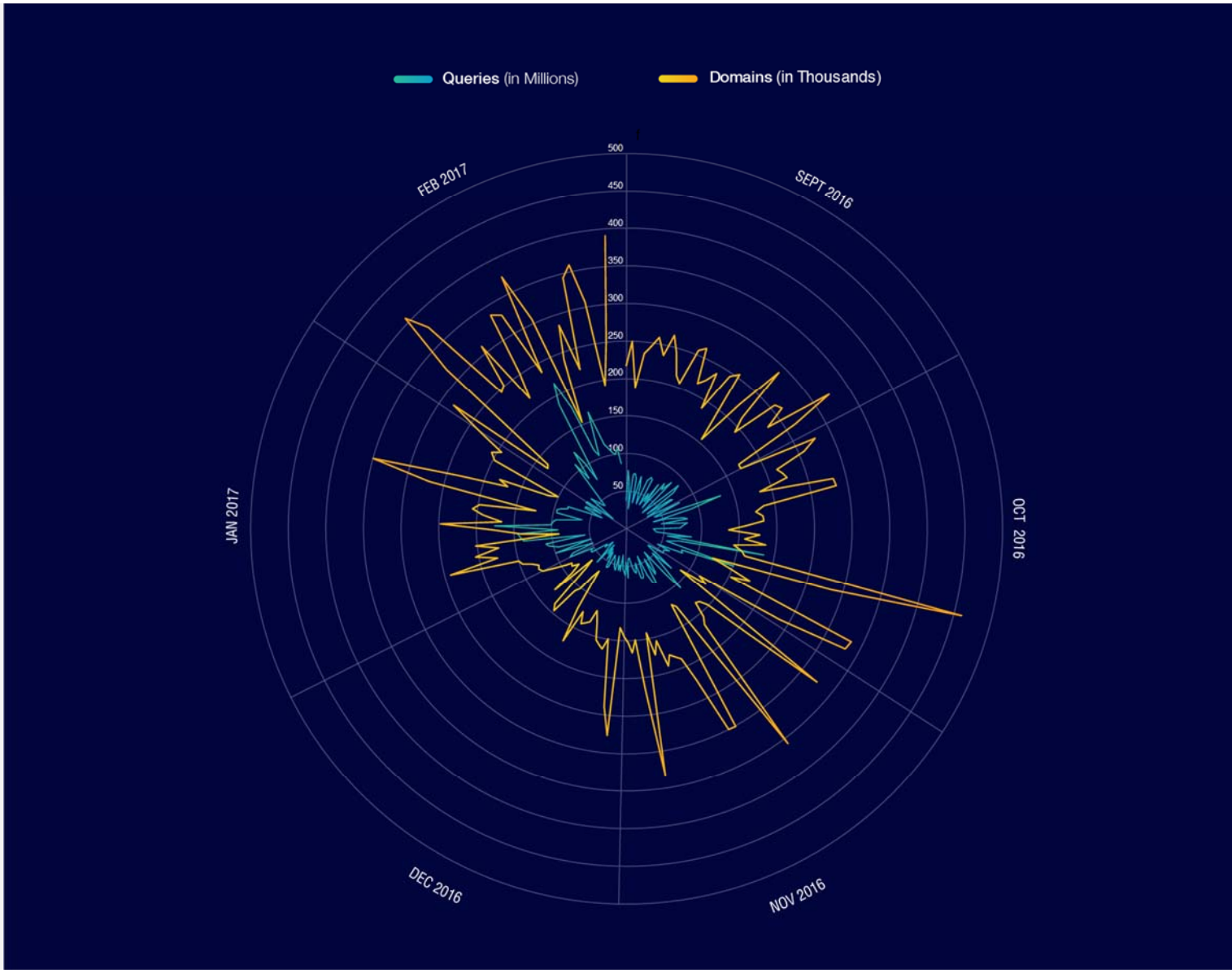
217 M

GROWTH IN AVERAGE MONTHLY MALICIOUS QUERIES

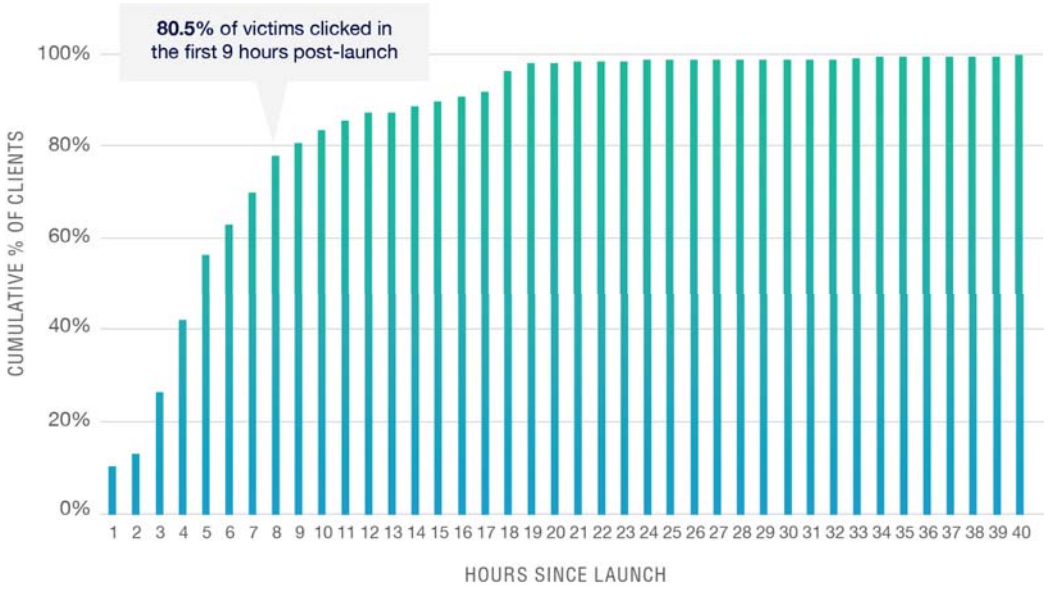
47%

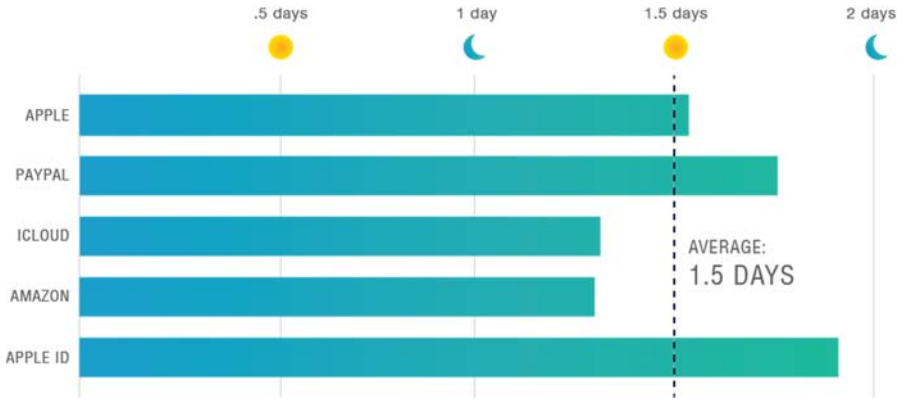
GROWTH IN AVERAGE MONTHLY MALICIOUS DOMAINS

18%



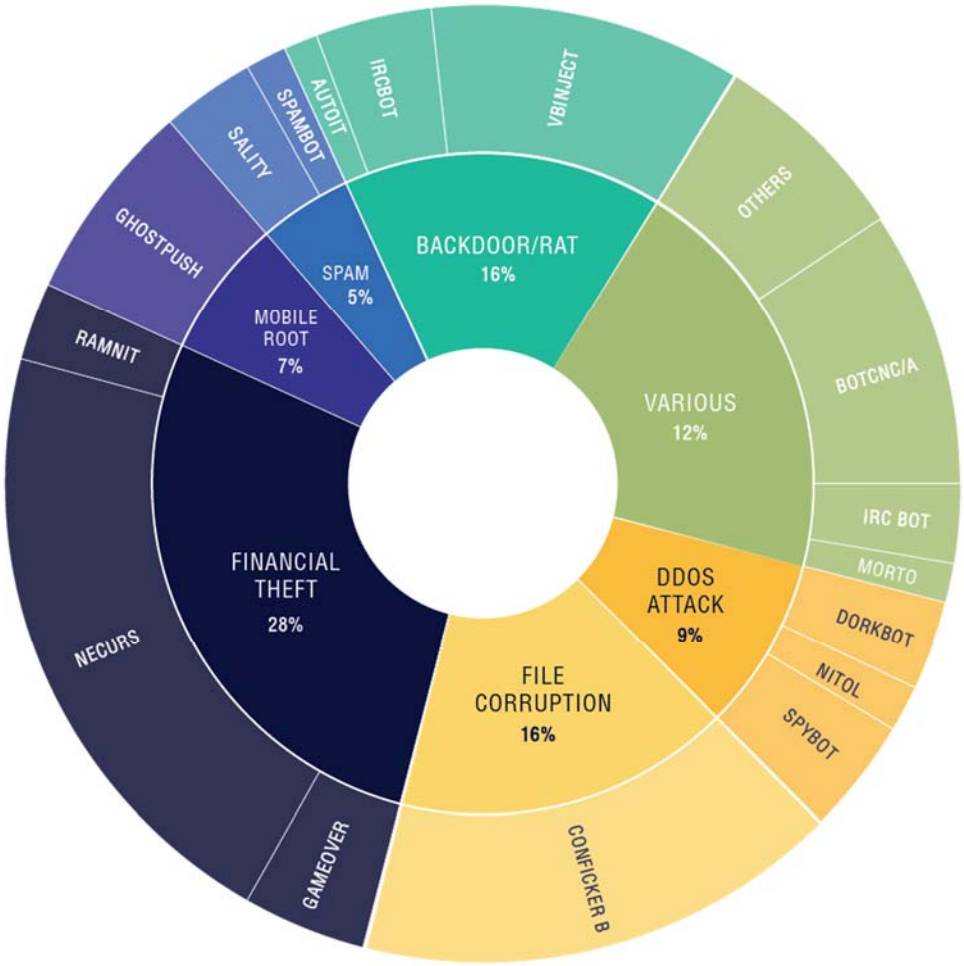
Phishing - Time to Block





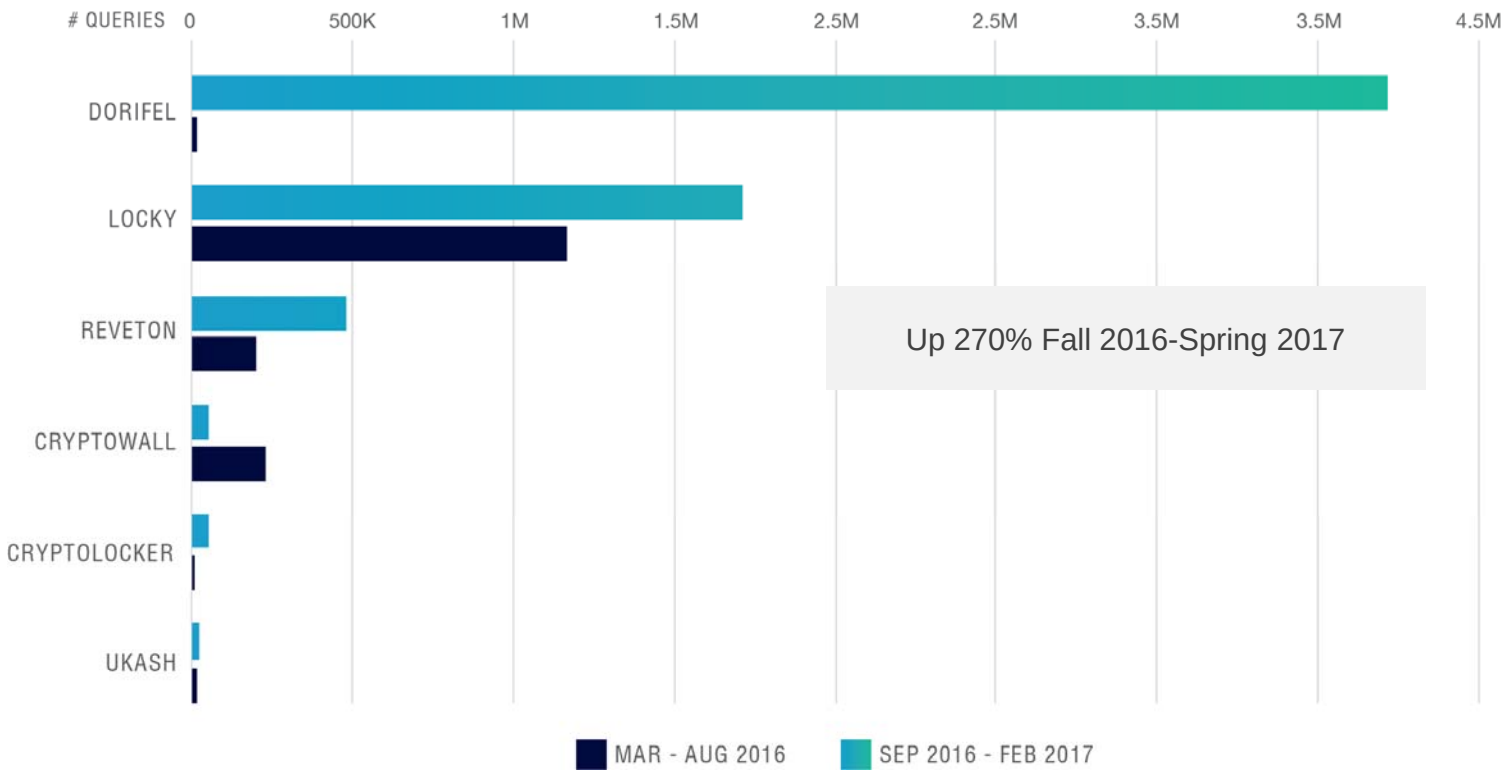
02 Main Threats Identified

Top Threats by Function



nominum

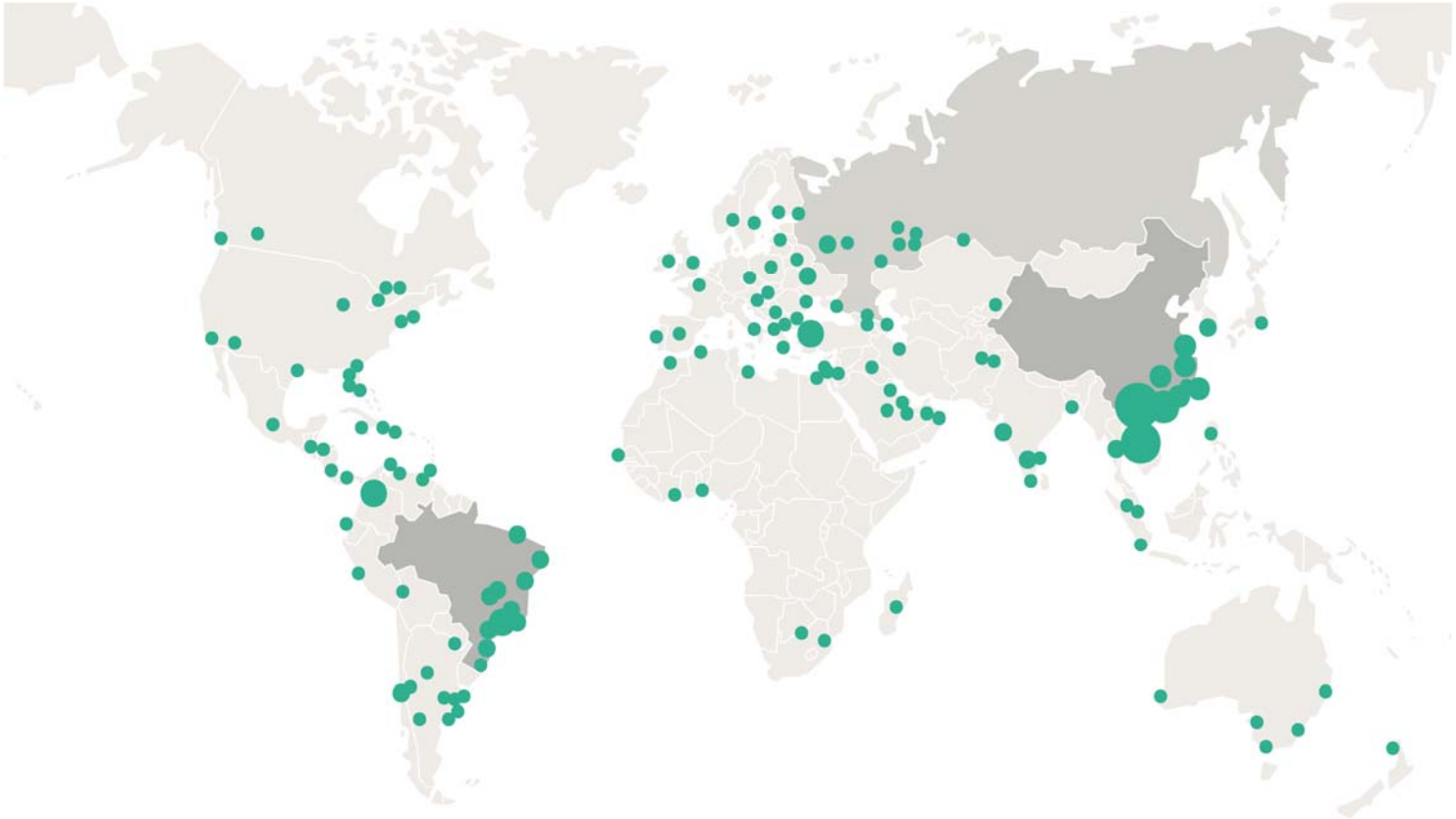
ATTACK STAGE | Ransomware Attacks



Up 270% Fall 2016-Spring 2017

nominum

ATTACK STAGE | Mirai Across the Globe



nominum

ATTACK STAGE | Mirai Source Code

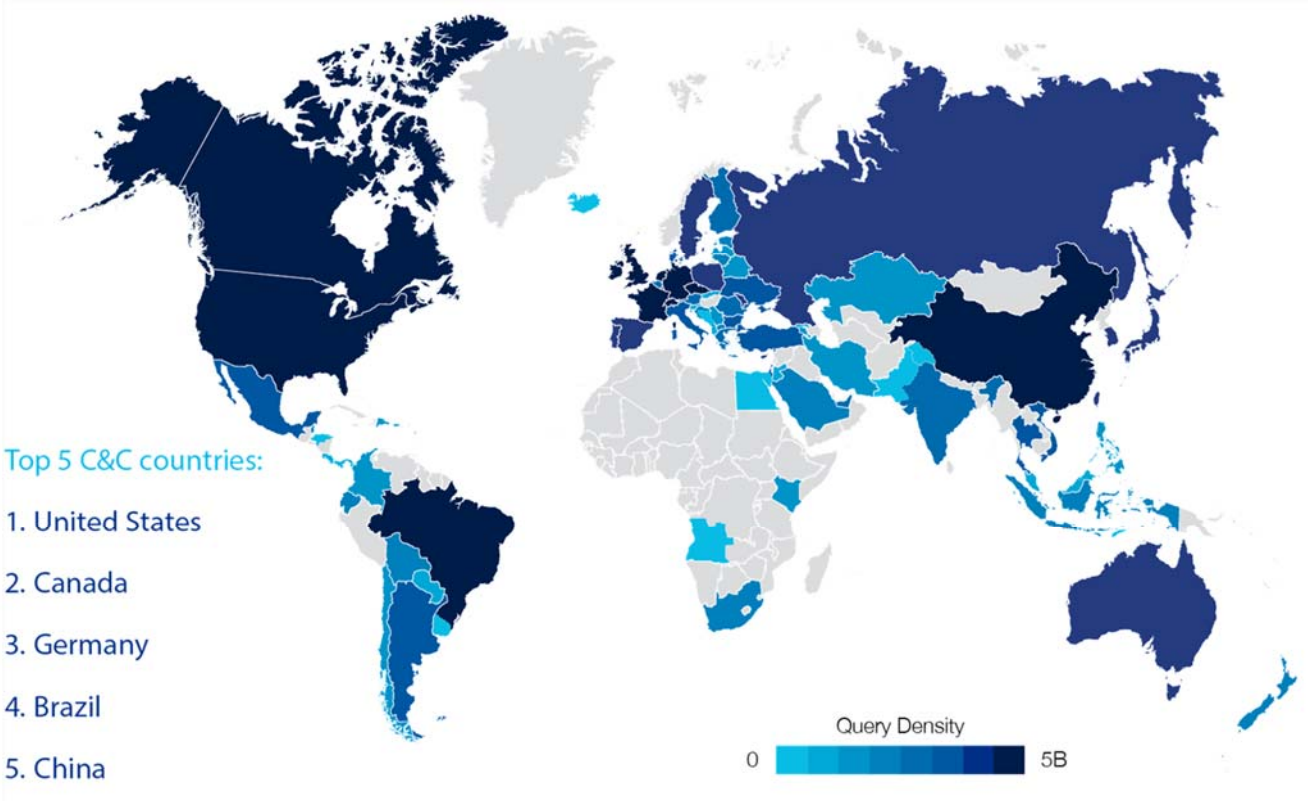
```
56  void rand_alphastr(uint8_t *str, int len) // Random alphanumeric string, more expensive than rand_str
57  {
58      const char alphaset[] = "abcdefghijklmnopqrstuvw012345678";
59
60      while (len > 0)
61      {
62          if (len >= sizeof (uint32_t))
63          {
64              int i;
65              uint32_t entropy = rand_next();
66
67              for (i = 0; i < sizeof (uint32_t); i++)
68              {
69                  uint8_t tmp = entropy & 0xff;
70
71                  entropy = entropy >> 8;
72                  tmp = tmp >> 3;
73
74                  *str++ = alphaset[tmp];
75              }
76              len -= sizeof (uint32_t);
77          }
78          else
79          {
80              *str++ = rand_next() % (sizeof (alphaset));
81              len--;
82          }
83      }
84  }
```

Right shifts of 3 bits from an 8-bit number means that the result is between 0-31 characters, which corresponds exactly to the 32-character string above.

nominum

03 Localization of the Threats

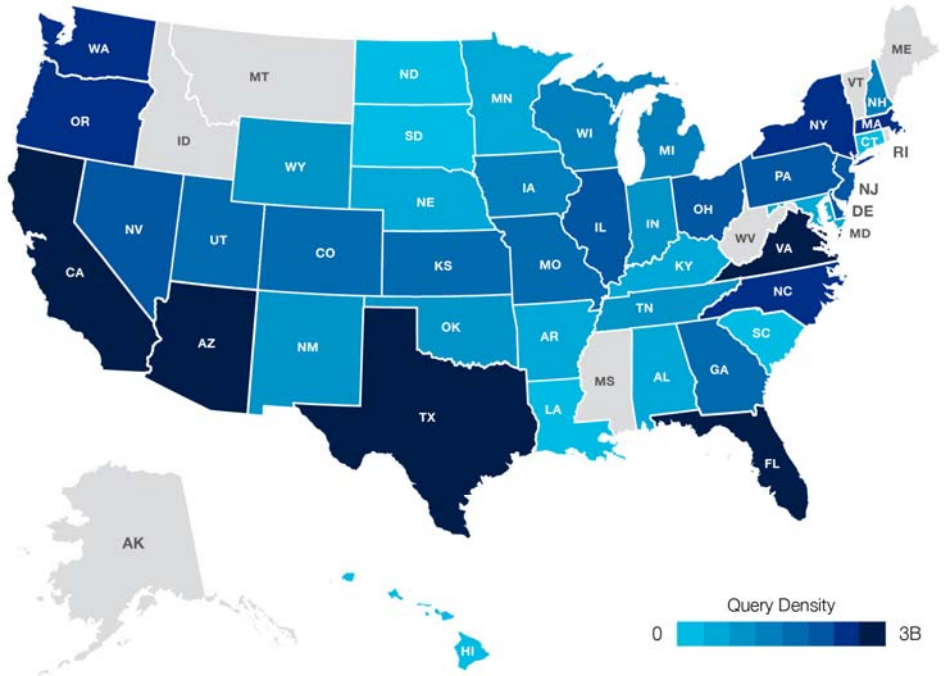
C&C – World



nominum

C&C – USA

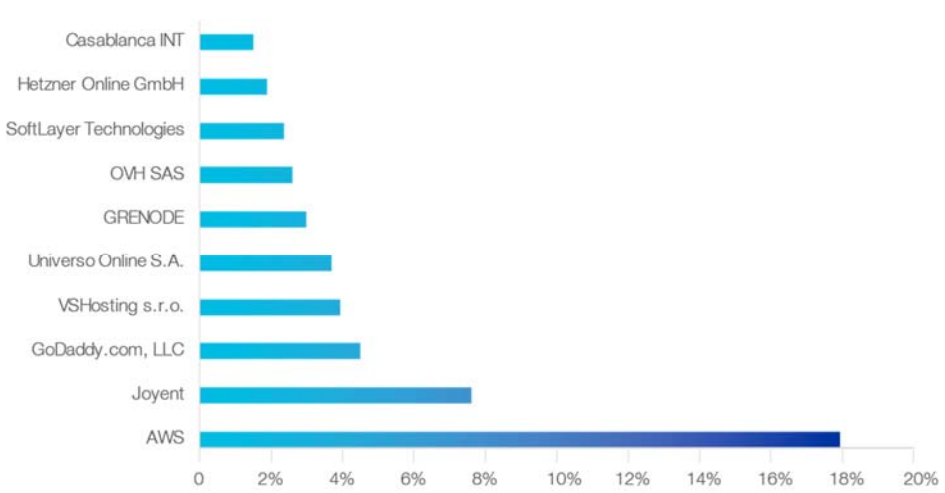
1. California
2. Virginia
3. Arizona
4. Texas
5. Florida



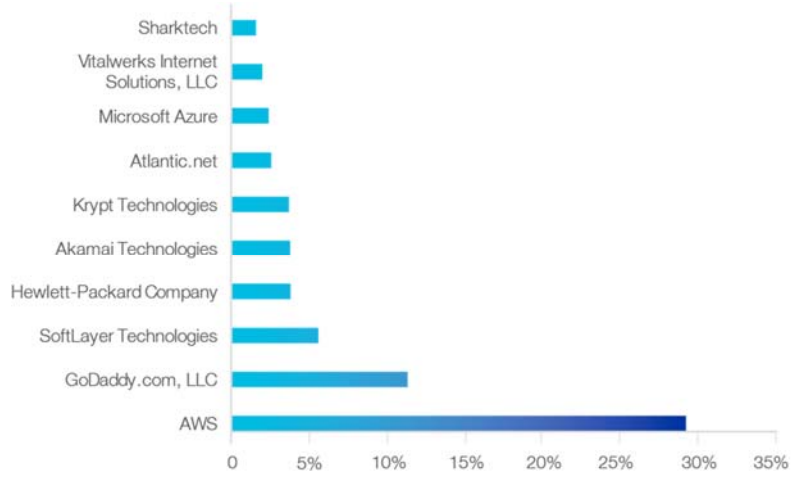
nominum

Hosting of Malware

World



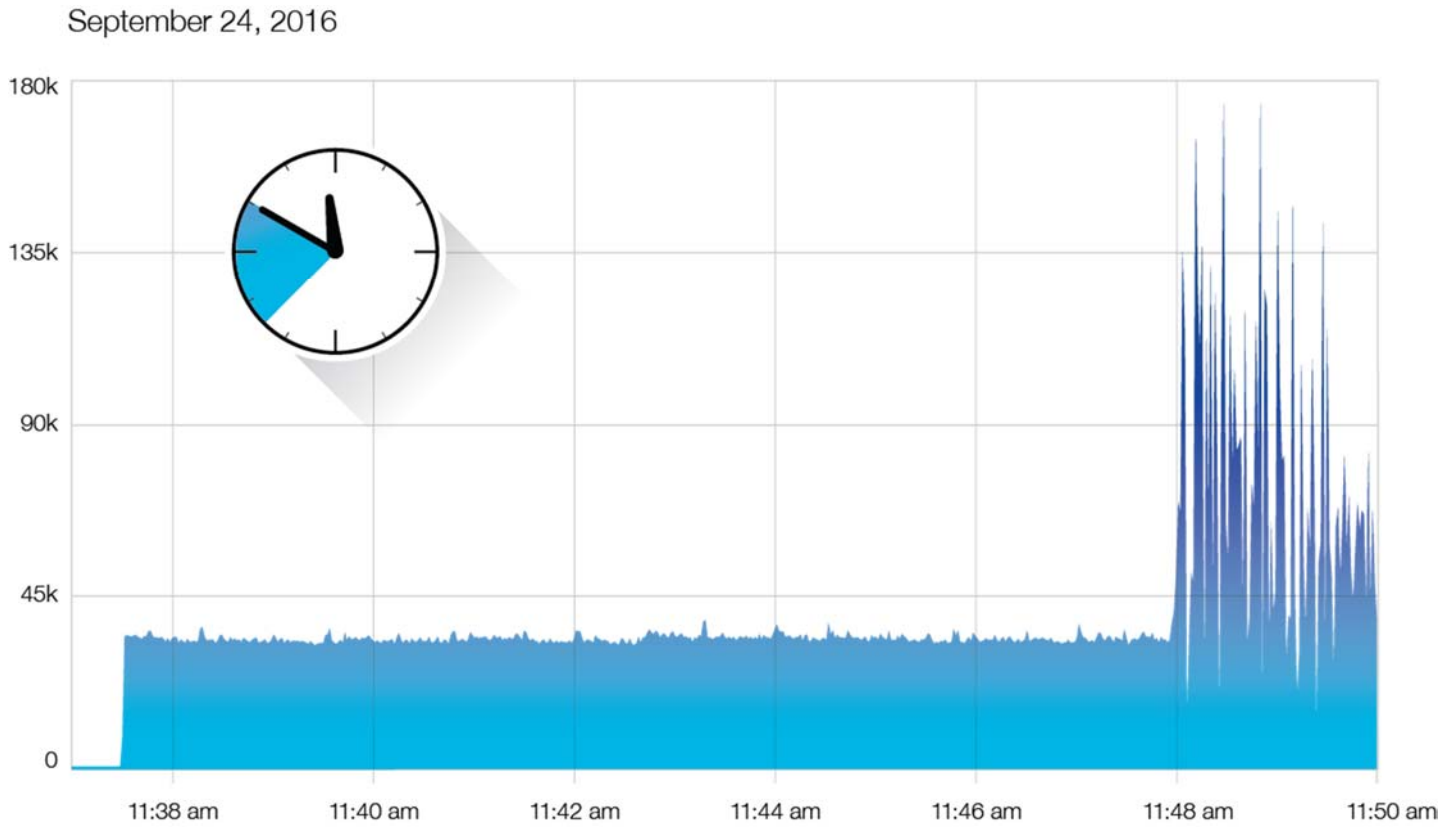
USA



nominum

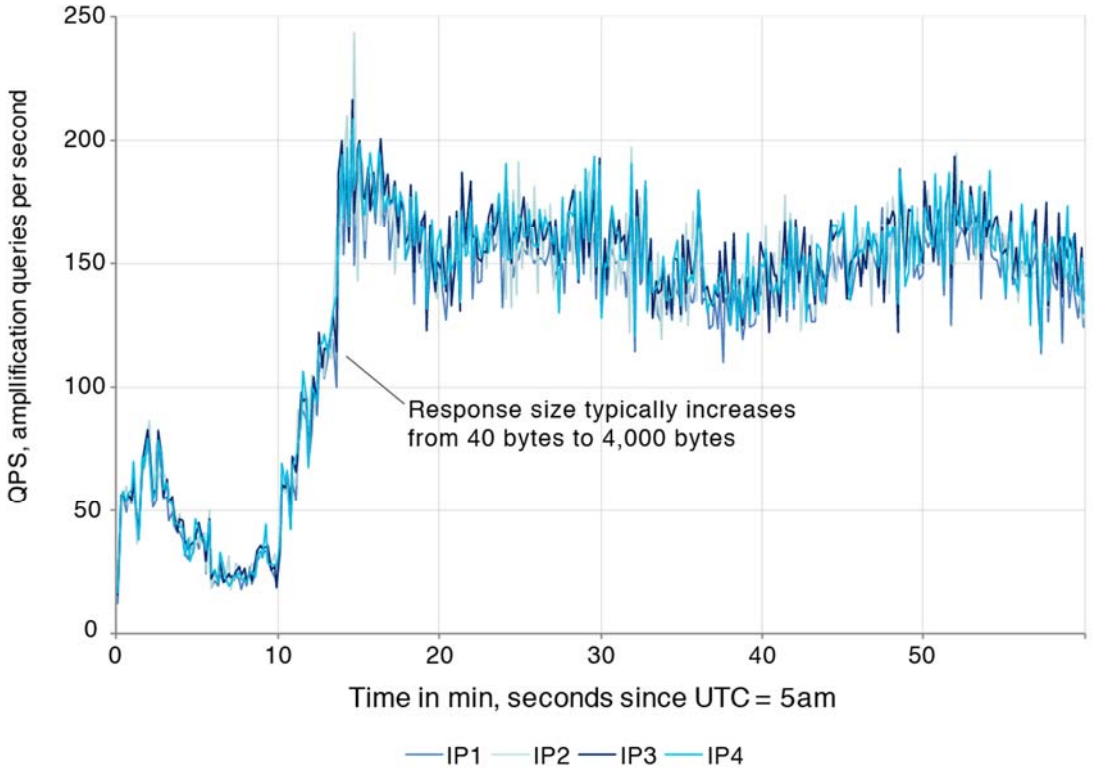
04 Deep Dive in DNS-Based DDoS

12 Minutes of a PRSD Attack



nominum

DNS Amplification



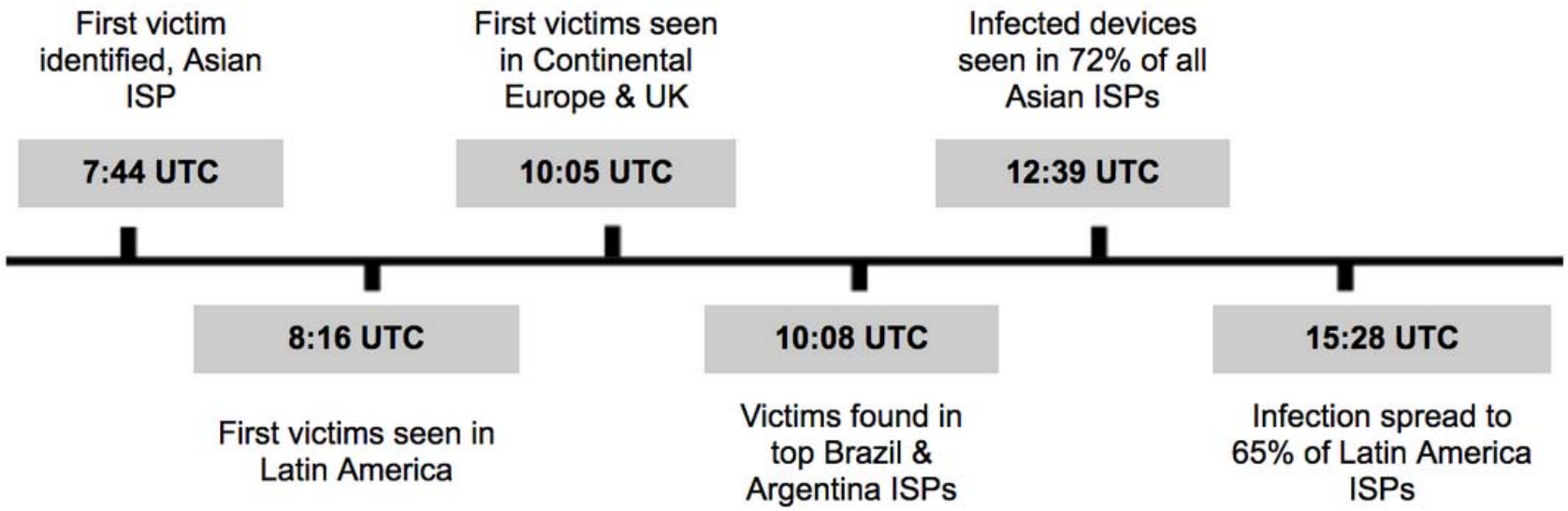
nominum

04 WannaCry: views from the DNS frontline

http://www.nominum.com/tech-blog/wannacry-views-dns-frontline

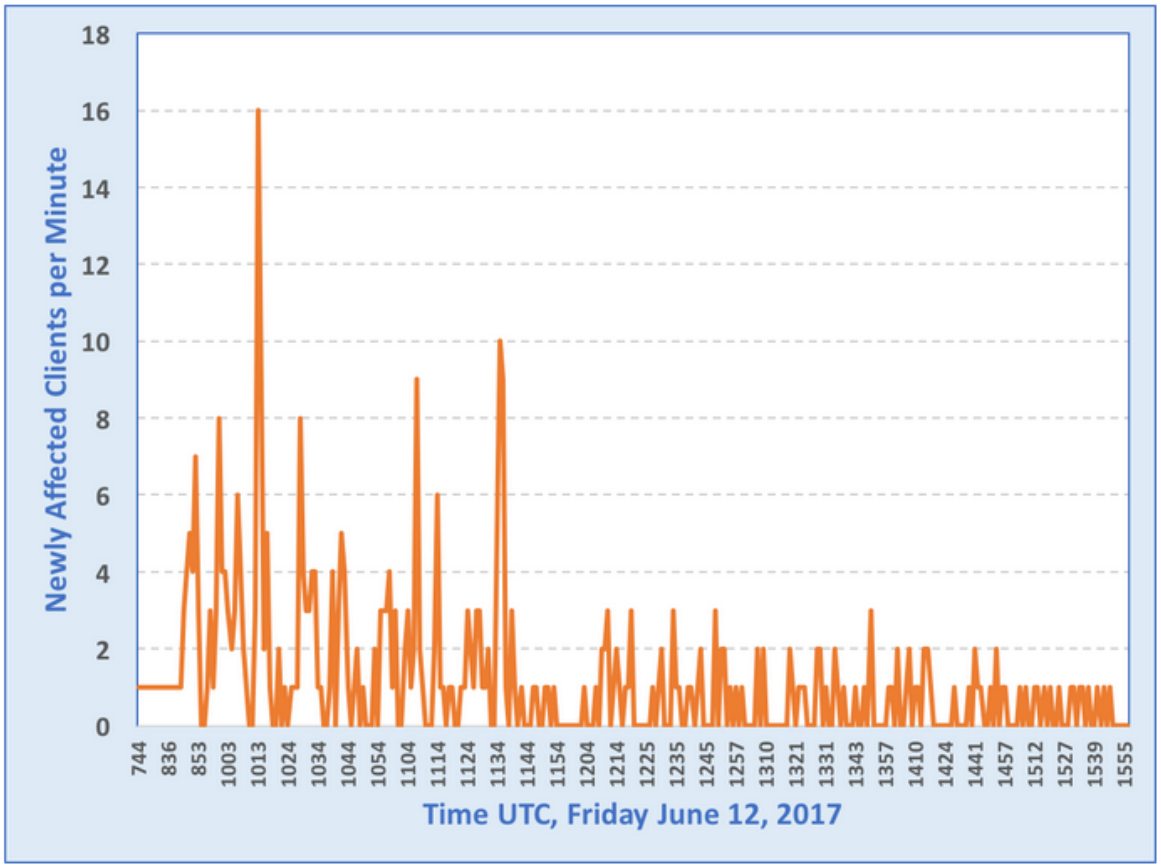
WannaCry Timeline

Kill-switch domain: iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com



nominum

WannaCry: Newly Affected Clients per Minute

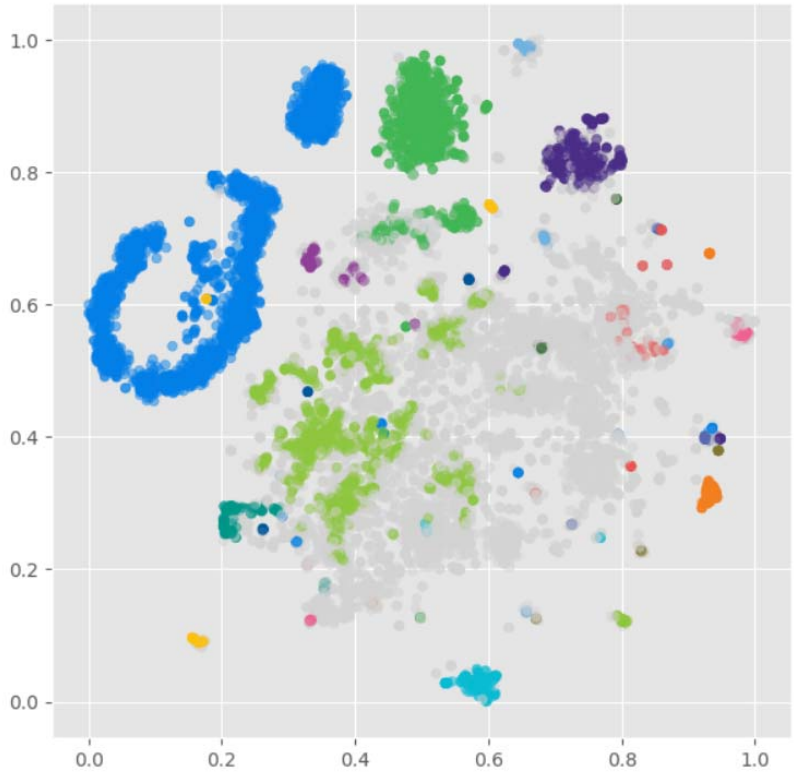


nominum

WannaCry: Top 3 Groups of Infected Subscribers

Top 3 groups identified:

- Gamers
- Teamviewer users
- Previously infected subscribers



nominum

Conclusions

High growth of DDoS, botnet and ransomware attacks

BYOD and IoT bring new challenges

DNS is key for Prevention and Mitigation

nominum

Final Thoughts

Download Nominum Data Science Security Reports:

http://nominum.com/resource/security-report-nn - Spring 2017

http://nominum.com/resource/security-report-home - Fall 2016

For Thought:

- Does your DNS Server always answer the correct answer?
- Does the correct answer protects the subscriber?