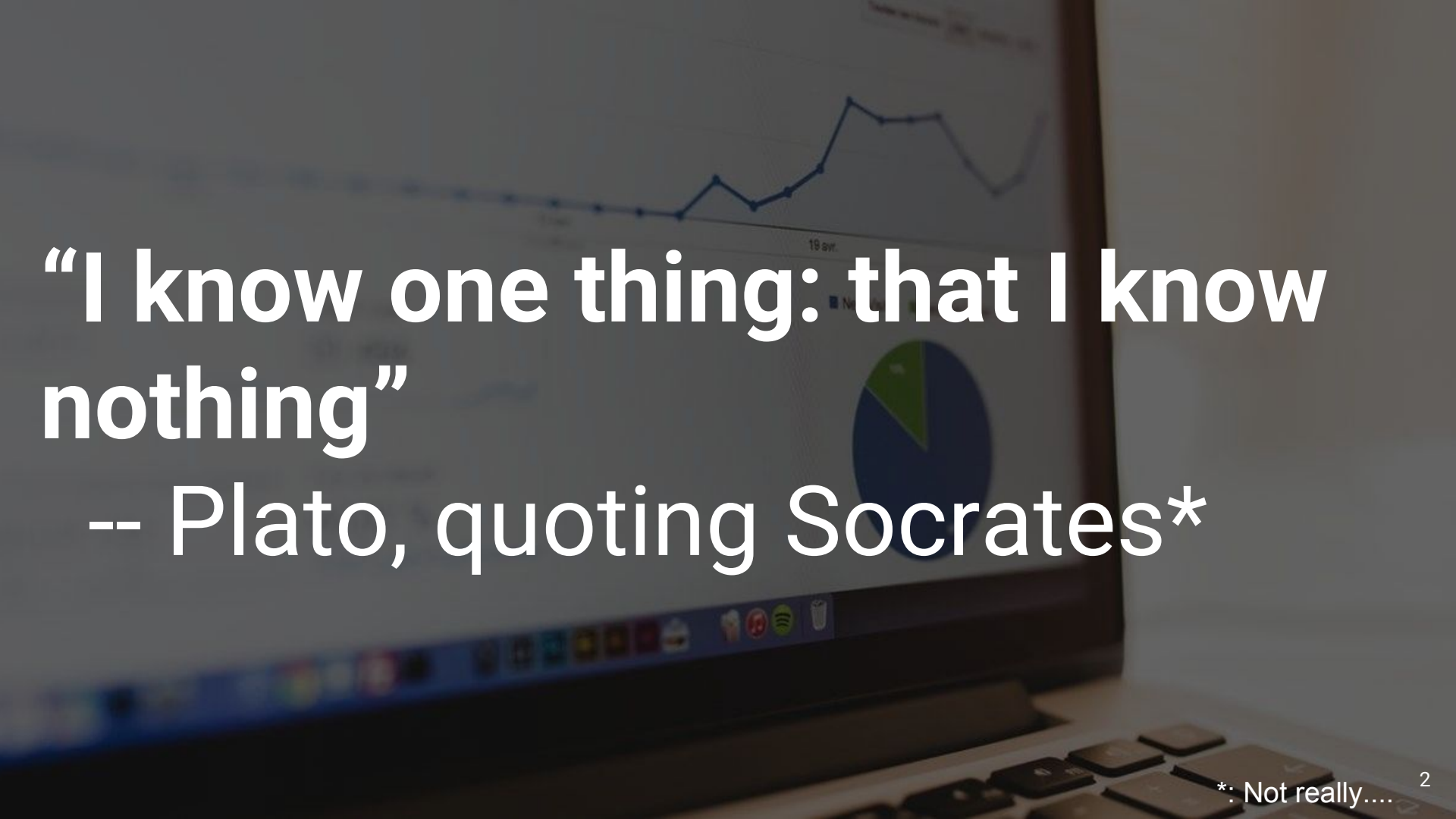


# draft-ietf-dnsop-nsec-aggressiveuse

and

draft-wkumari-dnsop-cheese-shop

A laptop screen is shown with a dark overlay. The screen displays a line graph with a blue line and a pie chart with a green slice. The text "I know one thing: that I know nothing" is written in large white font across the screen. Below it, the text "-- Plato, quoting Socrates\*" is also in white font. The background of the screen shows a line graph with a blue line and a pie chart with a green slice. The text "19 av." is visible on the screen. The laptop keyboard is visible at the bottom of the image.

**“I know one thing: that I know nothing”**

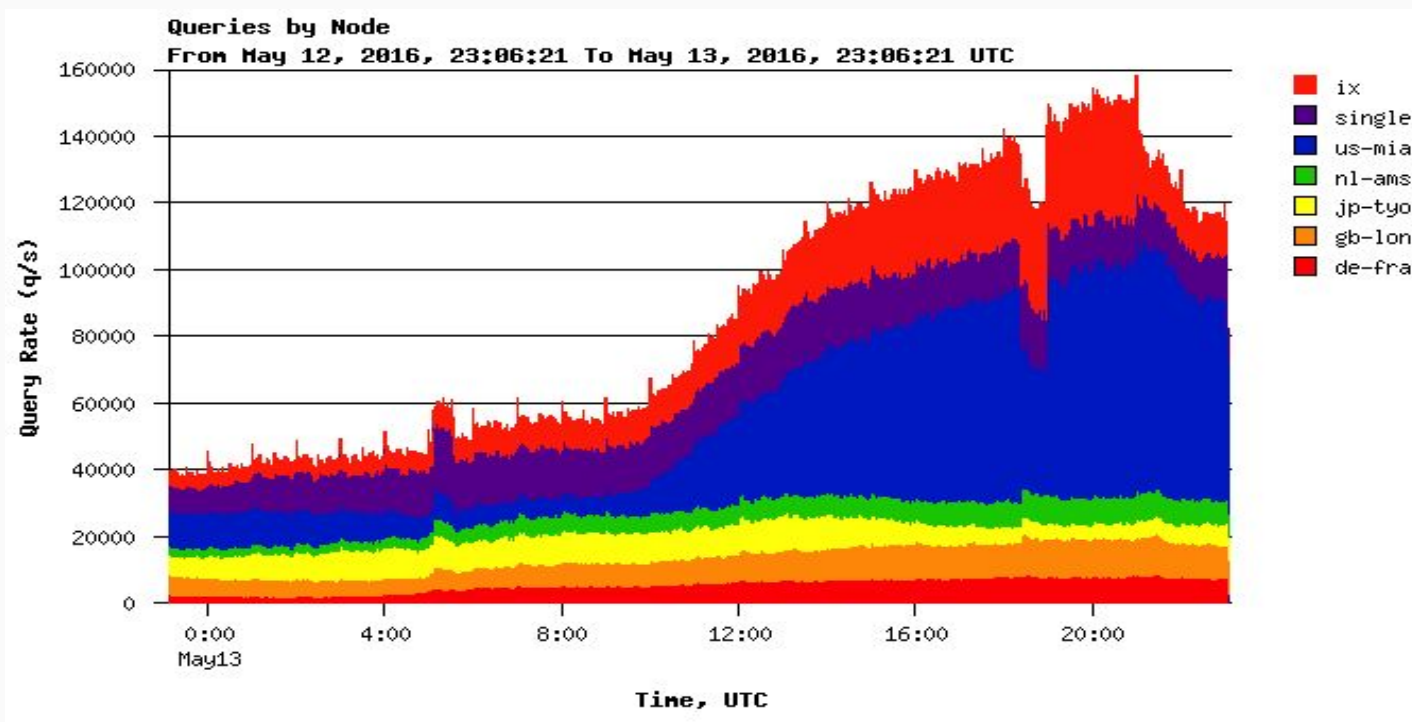
**-- Plato, quoting Socrates\***

```
wkumari$ dig +dnssec belkin
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 41230
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 6, ADDITIONAL: 1
;; QUESTION SECTION:
;belkin.                IN      A
;; AUTHORITY SECTION:
.                1795 IN      SOA  a.root-servers.net. nstld.verisign-grs.com.
2016070901 1800 900 604800 86400
beer.                21512   IN      NSEC  bentley. NS DS RRSIG NSEC
beer.                21512   IN      RRSIG  NSEC 8 1 86400 20160719170000
20160709160000 46551 .
AoT20e3eVZ3pC1DousLXDYABGuTTvkyP4rbBXvquGp3T/Lg7Rer3Vx2g
oC9p5u6T+lj/3u879htWNRO62wSdODkvOdtVFA5iJxN9DJ5EtuJdbuL/
xJuPhoin+0Fc6Vtf0X017e5TBtxYAYpZqUq6dxm6qE/NW6Ft1nAv3GYX jlg=
;; Query time: 222 msec
```

# The problem

*Couldn't have made a better example if I'd planned it...*

- May 12, a Friday afternoon, Colin Petrie / Kaveh Ranjbar from RIPE poked me: “Google is suddenly sending K-root way more junk queries, e.g ‘nq0nnjzba-fn.357.225.340.251’. It burns us, please make it stop...”



# Well, that's not good....

- What's causing this?
  - Have we got some bug?
  - Did anyone change anything?!
  - Are we being used as a DoS reflector?
  - Why does the graph look more like organic growth than a DoS?
- Phew, it's not just Google Public DNS, just we show up towards the top...  
...still, what's causing this? And why? And can we make it stop?

# Ugh, unpatched CPE...

## Thousands of Ubiquiti AirOS routers hit with worm attacks

A worm is exploiting an old v firmware.

By: **Symantec Security Response**  

Created 19 May 2016 | 0 Comments



A worm is reportedly spreading across thousands of Ubiquiti Networks routers run advisory, a Ubiquiti spokesperson said that over the past week, the worm has been devices. The worm creates its own account on the compromised device and, from t routers both within the same subnet and on other networks.



Home / Security

## Worm infects unpatched Ubiquiti wireless

The vulnerability has been kn many users haven't applied t



The Ubiquiti Networks AirRouter Credit: UB

## Foul-mouthed worm takes control of wireless ISPs around the globe

Active attack targets Internet-connected radios from Ubiquiti Networks.

by Dan Goodin - May 19, 2016 4:14pm EDT



**21 June 2016**

Alert Number  
**MC-000075-MW**

**WE NEED YOUR HELP!**

If you find any of these indicators on your networks, or have related information, please contact  
**FBI CYWATCH**

In furtherance of public-private partnerships, the FBI routinely advises private industry of various cyber threat indicators observed during the course of our investigations. This data is provided in order to help cyber security professionals and system administrators to guard against the persistent malicious actions of cyber criminals.

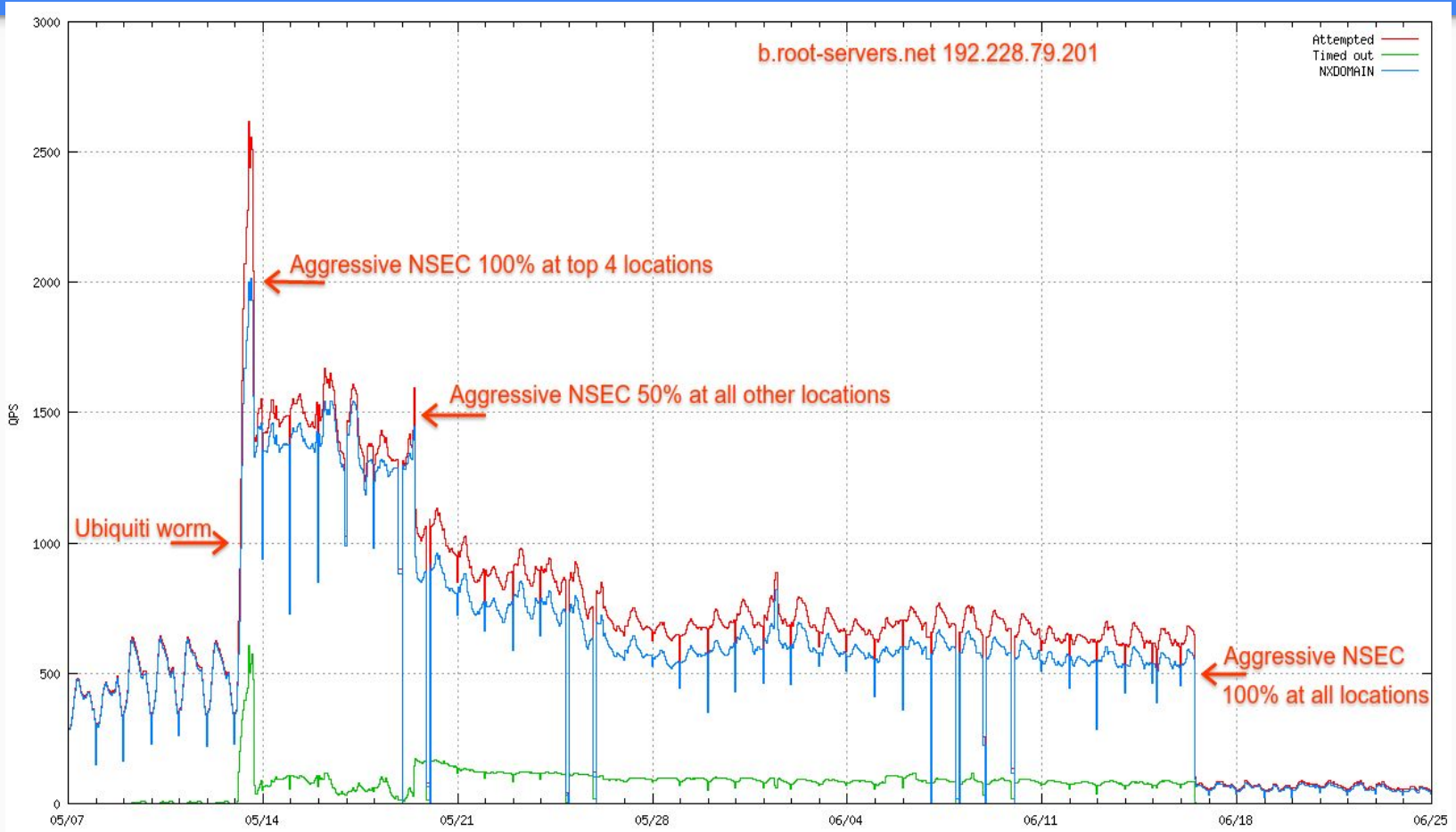
This FLASH has been released **TLP: GREEN**: The information in this product is useful for the awareness off all participating organizations within their sector or community, but not via publicly accessible channels.

## Unpatched Ubiquiti Network Devices Subject to Virus Attack Resulting in Denial of Service

### Summary

Self-propagating malware has infected thousands of devices from wireless equipment vendor Ubiquiti Networks running outdated airMAX,

# ... turning on Aggressive NSEC / Cheeseshop



A close-up photograph of a person's hands writing on a document with a pen. The background is blurred, showing some lights and a desk. The text 'Aggressive NSEC Draft' is overlaid in white on the left side of the image.

# Aggressive NSEC Draft

Rewritten to be more  
readable

Integrated comments / no  
longer applicable

Better examples

Seeing as this is moving  
along, no need for Cheese-  
shop



# Updates

- Document adopted by DNSOP WG
- Adoption comments
- Changed main purpose to performance
  - Thanks to Jinmei.
- Use NSEC3/Wildcard keywords
  - Thanks to Matthijs
- Improved wordings (from good comments)
- Simplified pseudo code for NSEC3
- Added Warren as co-author
- Reworded much of the problem statement
- Reworked examples to better explain the problem / solution

# Notes

- This technique may occlude newly added information
  - If you ask for foo.example.com, and it doesn't exist, it doesn't exist for the NSEC TTL
- NSEC3 is trickier than NSEC
  - So implementations may choose to only support this for NSEC
- Provide knobs for enabling / disabling on a per-domain basis

# Done?

## ***A few minor edits:***

*Jinmei provided some comments, mainly suggesting removing references to subdomain attacks.*

*Typos and grammar nits, fixing references*

*`https://github.com/wkumari/draft-ietf-dnsop-nsec-aggressiveuse`*