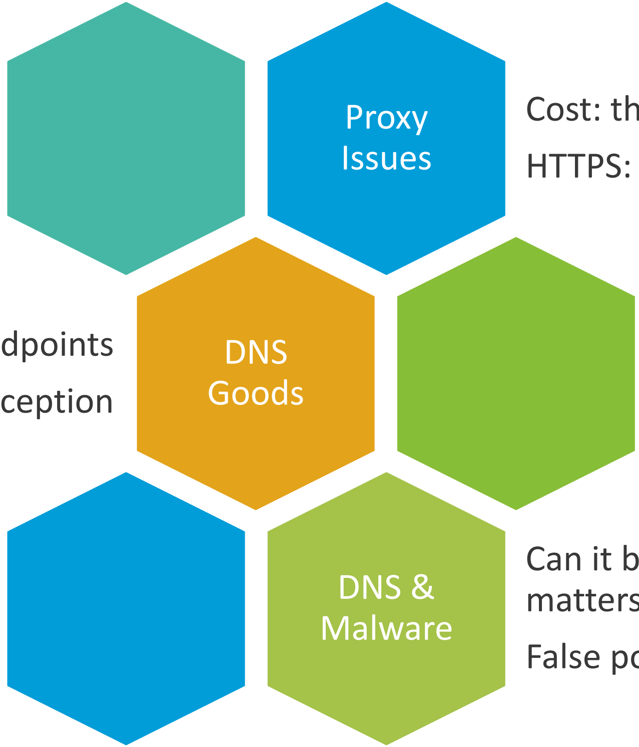
Infoblox
NEXT LEVEL NETWORKING

Effectiveness of DNS as an enforcement point for security and content filtering service

Date: November 29, 2018

Motivations and Fundamental Questions



Proxy Issues

Cost: throughput

HTTPS: 80%+

DNS Goods

Cost: endpoints

No interception

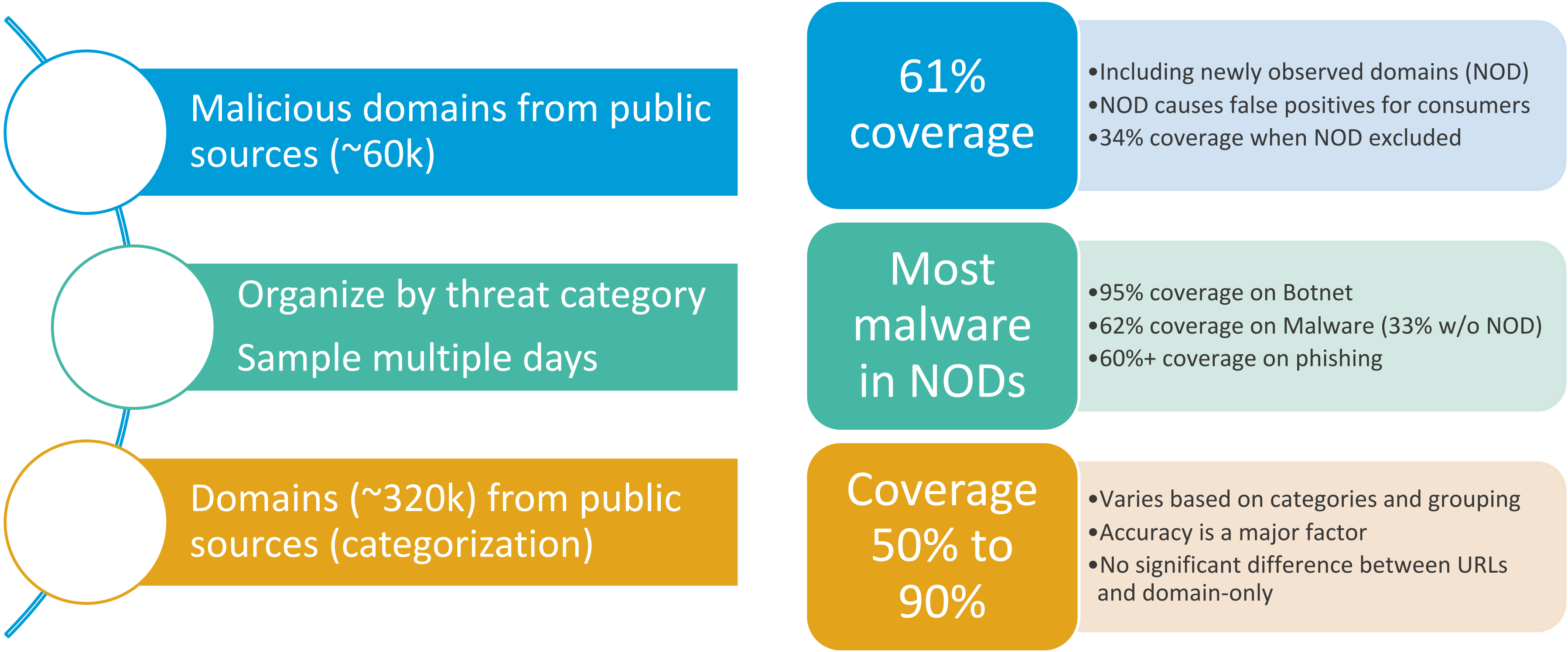
DNS & Malware

Can it block what matters?

False positives?

Case 1: European Mobile and Fixed operator

Methodology and Results



Malicious domains from public sources (~60k)

Organize by threat category

Sample multiple days

Domains (~320k) from public sources (categorization)

61% coverage

- Including newly observed domains (NOD)
- NOD causes false positives for consumers
- 34% coverage when NOD excluded

Most malware in NODs

- 95% coverage on Botnet
- 62% coverage on Malware (33% w/o NOD)
- 60%+ coverage on phishing

Coverage 50% to 90%

- Varies based on categories and grouping
- Accuracy is a major factor
- No significant difference between URLs and domain-only

Case 2: European Mobile and Fixed operator

Methodology and Results

- Mixed list of malicious domains from external assessor (AV benchmark)
- Sample multiple days
- Domains & IPs (~140k) from own network (categorization: DPI benchmark)

94% coverage

- Including newly observed domains (NOD)
- <1% false positives

Most phishing in NODs

- Different NOD vendors catch and time out threats differently

Coverage 84%

- Unknown domains to be measured in a second step

Conclusions

Adjust Methodology for Market

- Coverage and false positive impact heavily dependent on use case (consumer vs corporate)

Multi-vendor Approach for Threat Intel

- Non-uniform coverage across feeds from same vendor
- Vendor bias can give false sense of security

URLs are NOT Better than Domains

- Benchmark against AV and DPI shows no significant coverage gap

Thank You

Vinaka köszönöm Kiitos Maake Asante Shukria Dhanyavadagalu

감사합니다 Dankscheen спасибо Kam Sah Hammida شكرا Manana Dankon Terima Kasih Matondo

Dank Je Mauruuru Biyan Diolch i Chi Taiku Tack

Blagodaram Ngiyabonga Dziekuje Chokrane Grazie

Juspaxar Arigato Mochchakkeram

நன்றி धन्यवाद Bedankt Dakujem Gracias Khap Paldies Tingki

Ua Tsaug Rau Koj Grazas Di Ou Mèsi cảm ơn bạn Gratias Tibi

Děkuji Nirringrazzjak Kia Ora Khun Obrigado

Suksama Nuwun Hvala Kop ありがとう

Rahmat Matur 谢谢 хвала Welalin Djiere Dieuf

Misaotra Danke Merci Go Raibh Maith Agat Tuke Eskerrik Asko

Salamat ขอบคุณ Najis