Infoblox

Rapid Domain Triage

Prepared by: Darin Johnson

Motivation: Get ahead of rapidly created infrastructure used in phishing attacks.

BleepingComputer: Coinbase cyberattack targeted employees with fake SMS alert

Infoblox: Recent SMS Phishing Attacks Reveal the Dangers of MFA Lookalike Domains

Increasingly these attacks are happening in less than 4 hours.

Obligatory LLM Slide

LLMs like WormGPT and FraudGPT can help generate phishing content.

Also:
Infrastructure automation like Terraform is equally if not more important.

This is a change in tactics which avoids newly observed domain feeds: ie SURBL Fresh, Farsight NOD, Infoblox NOED.

Idea: We block things we haven't seen before for a small window of time

If:

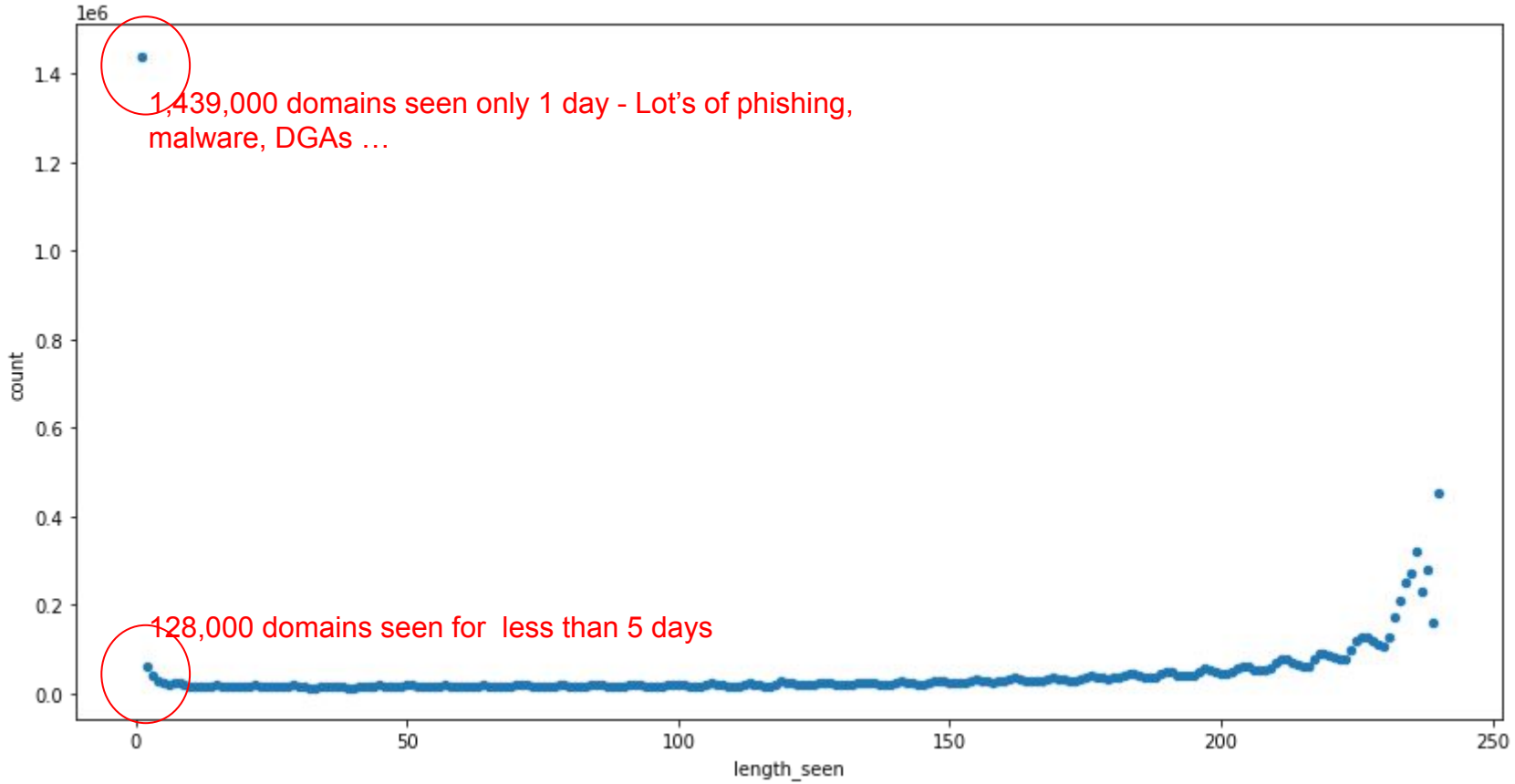
- The domain isn't in the last 60 days of traffic.
- The domain isn't in a set of recommended feeds.
- The domain isn't already blocked

Do we just block immediately, or maybe do a few VERY QUICK checks

- Whois: registrar and creation date maybe?
- A DGA check?

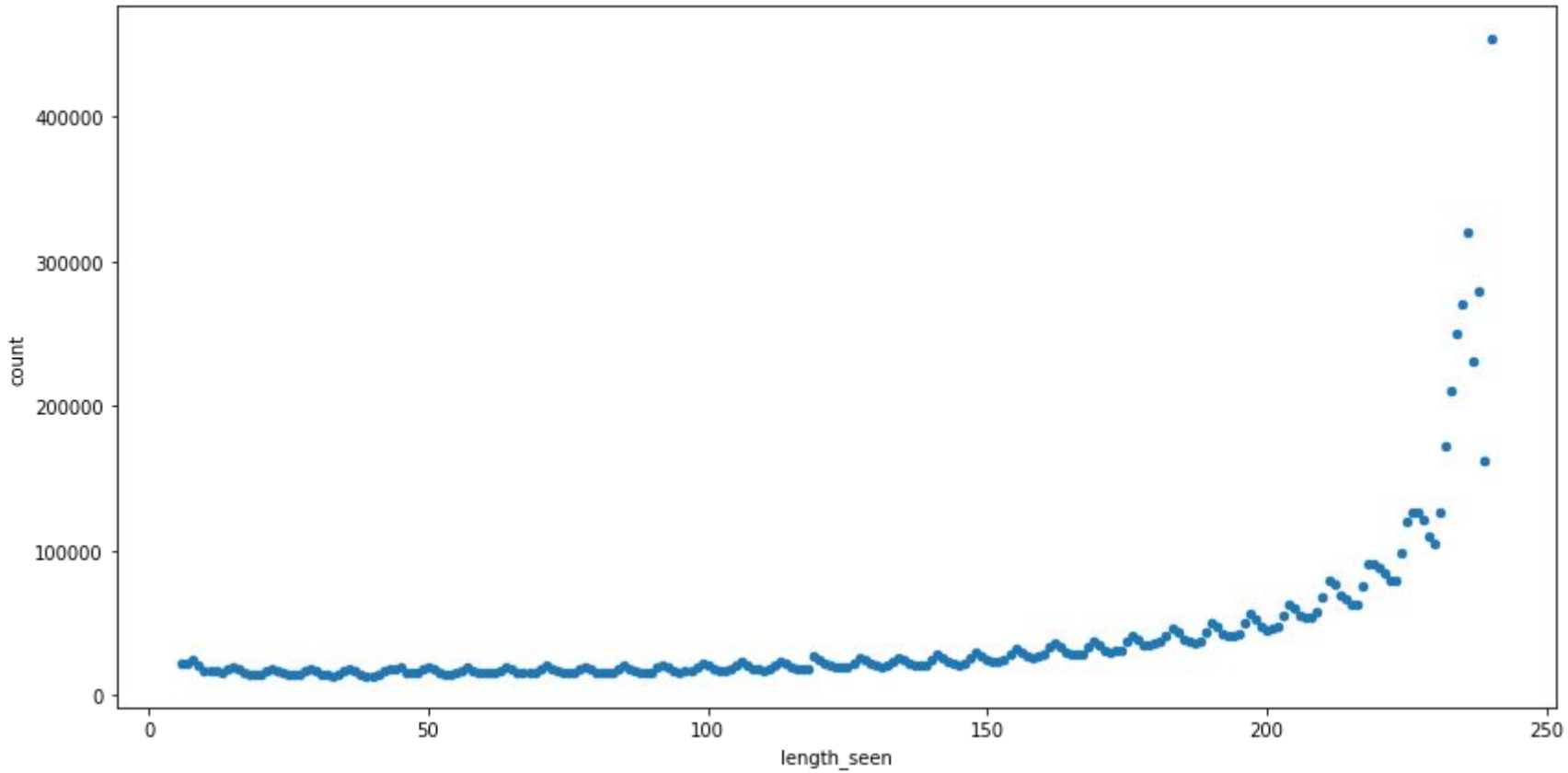
What could possibly go wrong?

How many support tickets will I get? Over 240 days, 6 networks.



Number domains seen per length of time (days)

Over 240 days, 6 networks: How long is a domain seen?



Number domains seen per length of time (days)
(removing those seen less than 5 days)

What could possibly go wrong?

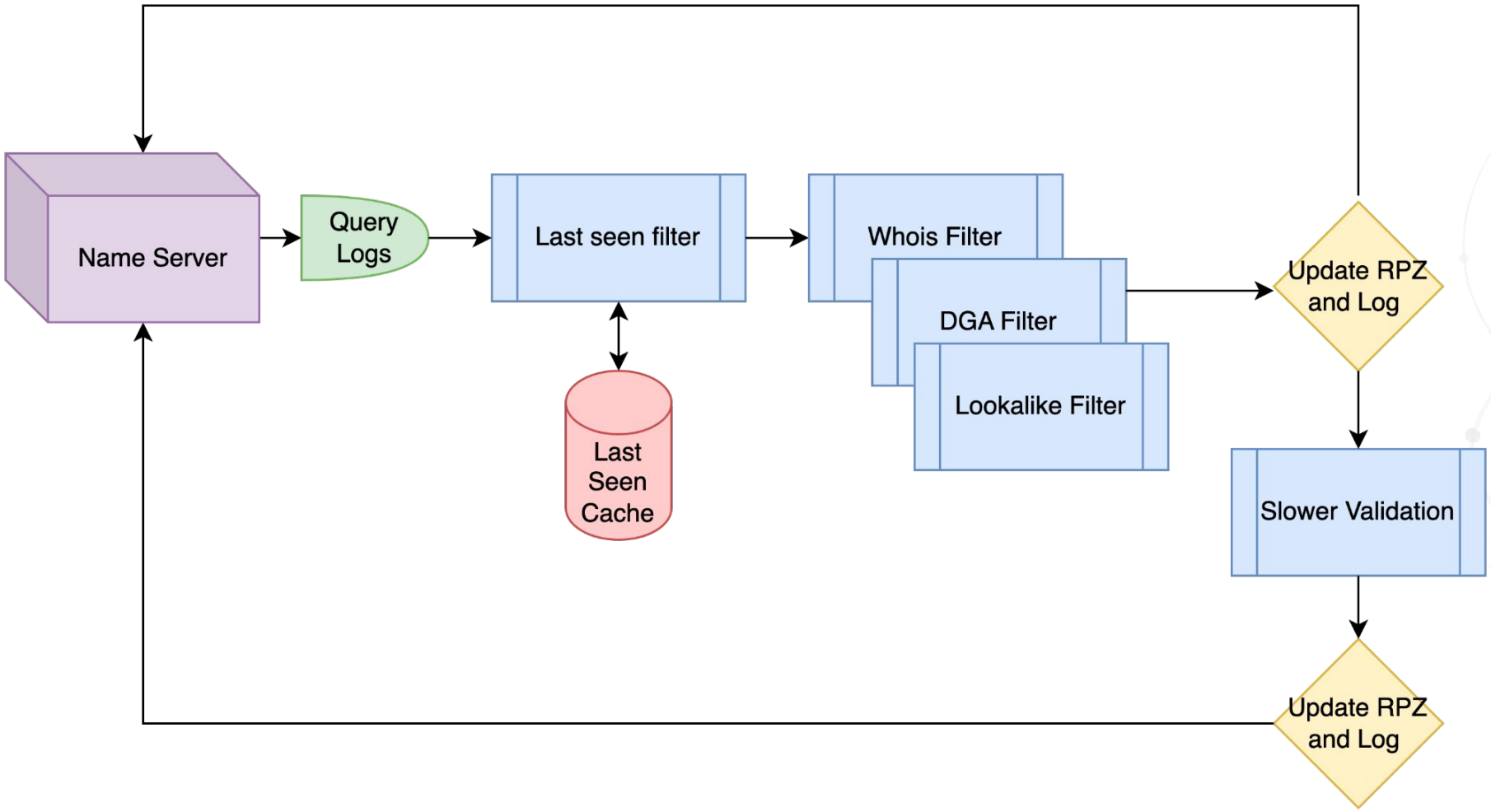
It won't cause an outage, as the domains weren't seen for 50 days. But it could be an inconvenience.

Roughly 16,000 unique domains/day (only 6 networks).

Maybe do a few VERY QUICK checks

- Name server?
- Whois: registrar and creation date maybe?
- A DGA check?

Basic Flow


Name Server
Query Logs
Last seen filter
Last Seen Cache
Whois Filter
DGA Filter
Lookalike Filter
Update RPZ and Log
Slower Validation
Update RPZ and Log

Case Study: Over 10 days, 6 networks

Category	Unique Domain Count	Total Query Count
Uncategorized	800 (also the total)	11464
farsight-nod	409	4913
noed	113	1310
Other (mostly IP based blocks) exist		

Case Study: Top 10 most queried of the 800

Domain	Count	Notes
drvishalchestclinic.com	692	Previously registered and parked. Reactivated on 2023-11-12 with new name server (Cloudflare) no longer resolving (2023-11-21).
techdiscoverys.com	645	Reactivated Reg: 2023-11-13, Moderate Risk (Posible Phishing/Spam)
jbbjw.com	595	Reactivated Reg 2023-11-13, Moderate Risk (Possible Phishing/Spam) Previously used in Kaseya Ransomware attack
thairoob.com	298	Reg 2023-11-12, Omnatuor, High Risk Malvertising
0c15ee8124.com	152	DGA 2023-10-24 see “Blatant Cherry Picking”
clrtktwfgq.com	139	Reg 2023-11-20, Omnatuor, High Risk Malvertising
w3ll.site	130	Parked
7010888f85.com	122	DGA 2023-10-23 see “Blatant Cherry Picking”
qbxofhwixlxnxer.com	117	Reg 2023-11-20, Omnatuor, High Risk Malvertising
xcrhcyytkarfwab.buzz	92	DGA 2023-11-16
vid1shar.shop	88	Created 2023-11-15, Suspicious-NOED on 2023-11-16

Case Study: After 48 hours from last day

Category	SLD Count
Infoblox Newly Observed	631
Malvertising Download	157
Parked Domain	152
Suspicious Noed	70
Suspicious Nameserver	59
Phishing	37
Generic Malware Download	36
Sinkholed Host	30
Generic Malware C2	21
Suspicious_DGAs	20
Lookalike Domain	22
Spam	11
Unwanted Content (Porn, Gambling)	7
Suspicious_Generic	3

130 domains were not added any list

Case Study: Remaining 130 domains

Category	SLD Count
DGAs	93
Reactivated (High risk)	13
Reactivated (Low to moderate)	11
New (High risk)	4
New (Low to moderate)	8
No longer in whois	1

Notes:
DGA Detection was based on an sll length > 10 and a ratio of word segments to sll length greater than 0.58. While this is not the most sophisticated DGA detection algorithm, it works surprisingly well.

Case Study: Blatant Cherry Picking from the 130

Domain	Notes
REACTED	Lookalike (missing a character) of **REACTED**, a customer domain different registrar.
businesslfx.com.br	First Seen by Infoblox, had create record from RDAP whois 2023-11-16. First Seen in Domain Tools pDNS 2023-11-22. This is low threat but emphasizes the issues with observability.
0c15ee8124.com 7010888f85.com 984335278d.com	These were in NOED, obvious DGA, suspicious nameserver. Looks like 1 month to go from registration to requesting an ssl certificate. New Threat Actor: Infapush, Malvertising.

Conclusions:

- We were able to detect and could stop a number of threats in near real time.
- Not a replacement for Newly Observed/Emergent Feeds it supplements them.
- Only minor inconveniences possible, most are mitigated.


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