Detecção de Domínios Maliciosos com Passive DNS e Aprendizado Profundo

João Rafael Gregório

GTER52/GTS38 - 2023

unesp

ACME!
Cybersecurity Research

Quem são os Domínios Gerados por Algoritmo?

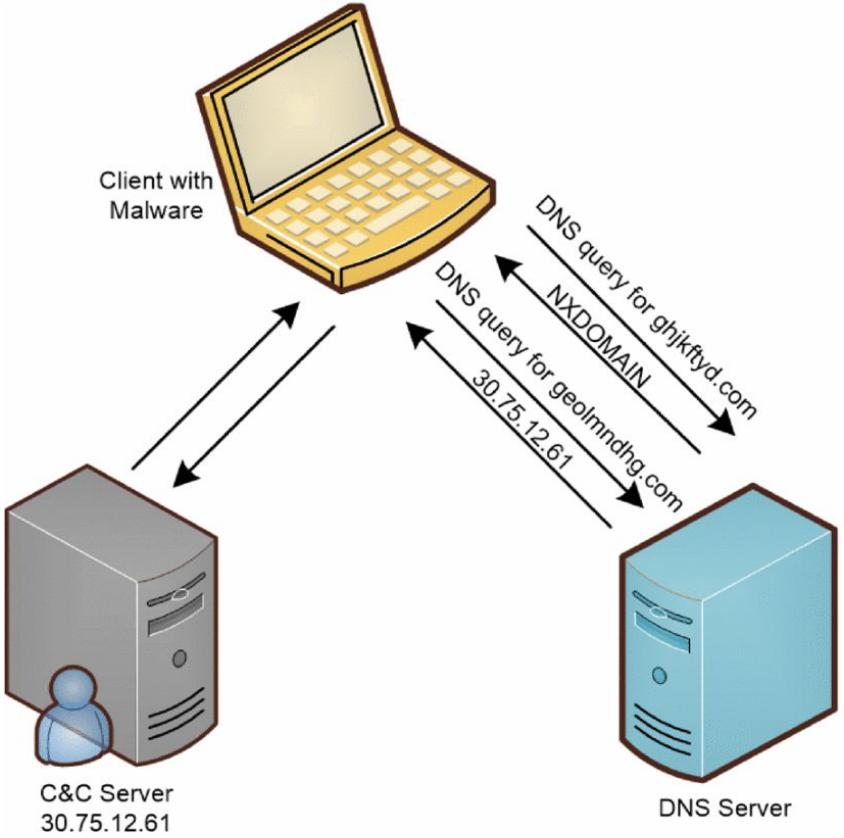
-Botnets e Ameaças Persistentes Avançadas

-Manutenção e ofuscação da comunicação

-Evadir camadas de segurança

Ex: vmdefmnsdoj.tech, 1pb98u4egqbcwzes185mpfyvc.com, u035zy.com

Quem são os Domínios Gerados por Algoritmo?



Fonte: H. Shahzad; A. R. Sattar and J. Skandaraniyam. DGA Domain Detection using Deep Learning.(2021).

Por que Detectá-los e Classificá-los?

-Infraestrutura de ataque de ameaças importantes:

- Sunburst (2020) - DGA Especialista
- Mirai Botnet (2017 - ?) - Botnet Open Source
- Cryptolocker e Gameover Zeus (2013 - ?) - Ransomware "Most Wanted"

Por que Detectá-los e Classificá-los?

DGArchive: ~ 120 famílias

Bambenek Consulting: ~ 60 famílias

NetLab360: ~60 famílias

Por que Detectá-los e Classificá-los?

Família	**Tipo DGA**	**Exemplos**
Suppobox	Lista de Palavras	windowafraid.net perhapsmeasure.net
Banjori	Domínio Semente	ekwallaabettingk.com fnramen.com
Mirai	Pseudo-randômico	xpknpxmywqsr.online oornsduuwjli.tech

Por que Aprendizado Profundo?

-No Feature Engineering

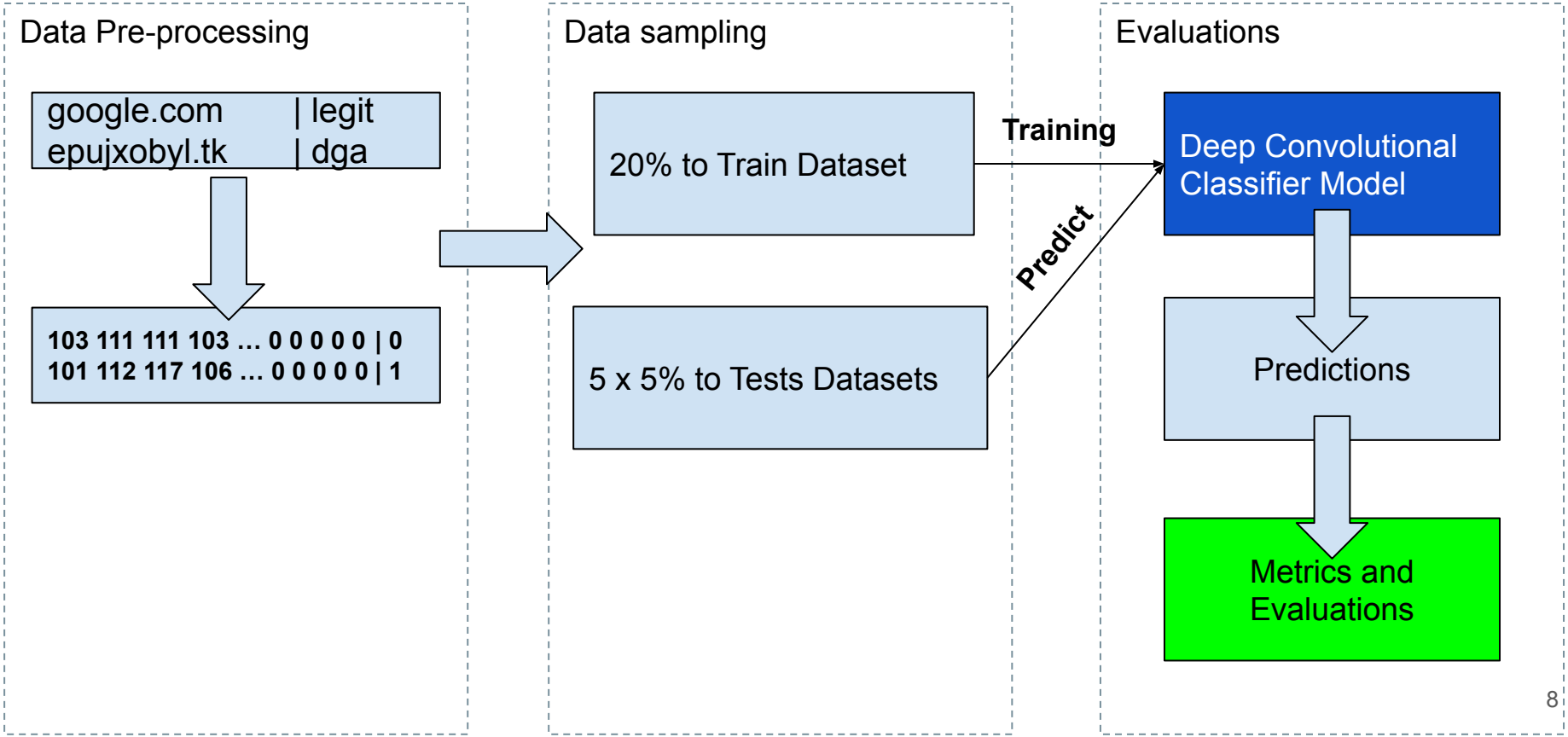
-Performance for large data volume

-High precision for pattern recognition

-and more…

Ahmed, S.F., Alam, M.S.B., Hassan, M. et al. Deep learning modelling techniques: current progress, applications, advantages, and challenges. Artif Intell Rev 56, 13521–13617 (2023). https://doi.org/10.1007/s10462-023-10466-8

Processo Modelo

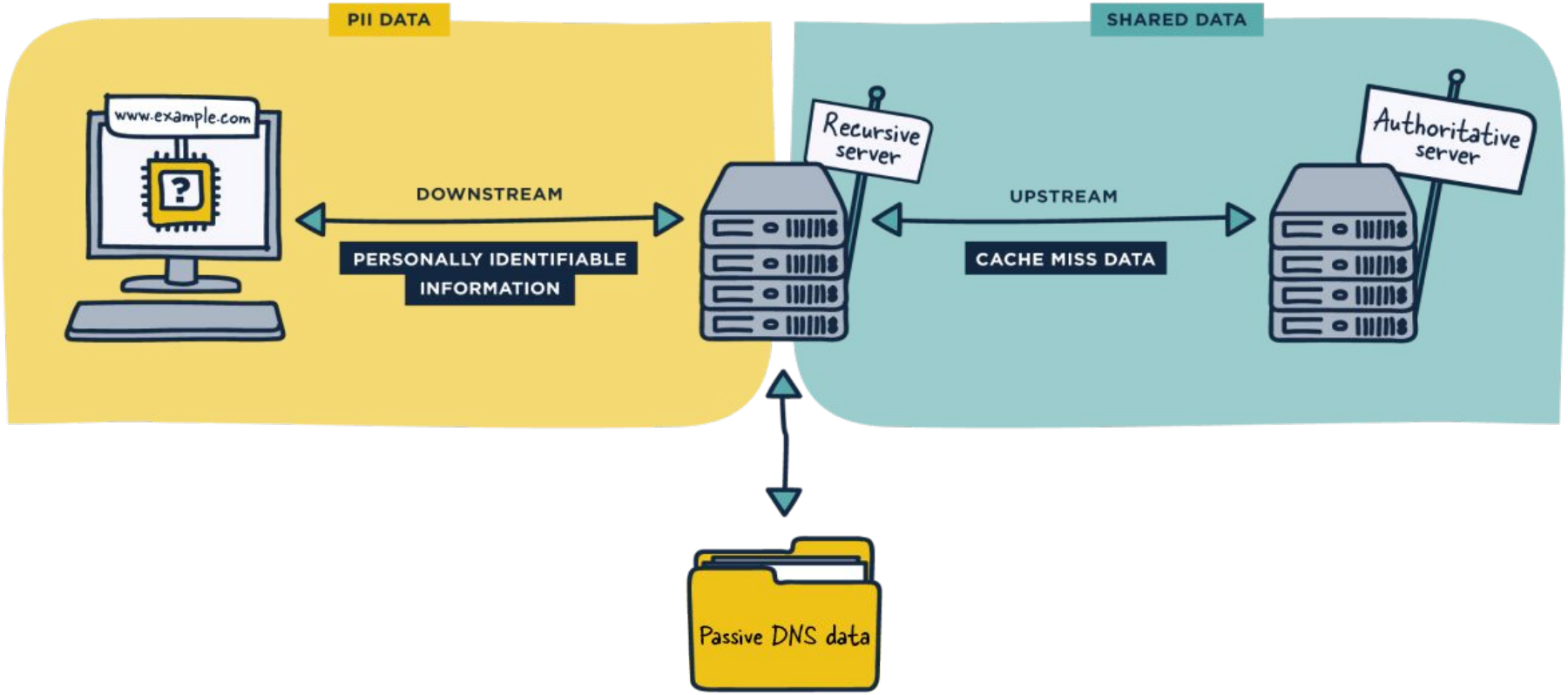


Resultados Preliminares

Classe	Precision	Recall	F1-Score
Legit	98,84%	99,35%	99,13%
DGA	99,36%	98,86%	99,11%

Accuracy	**99,10%**
ROC AUC	**99,10%**

E o DNS Passivo?



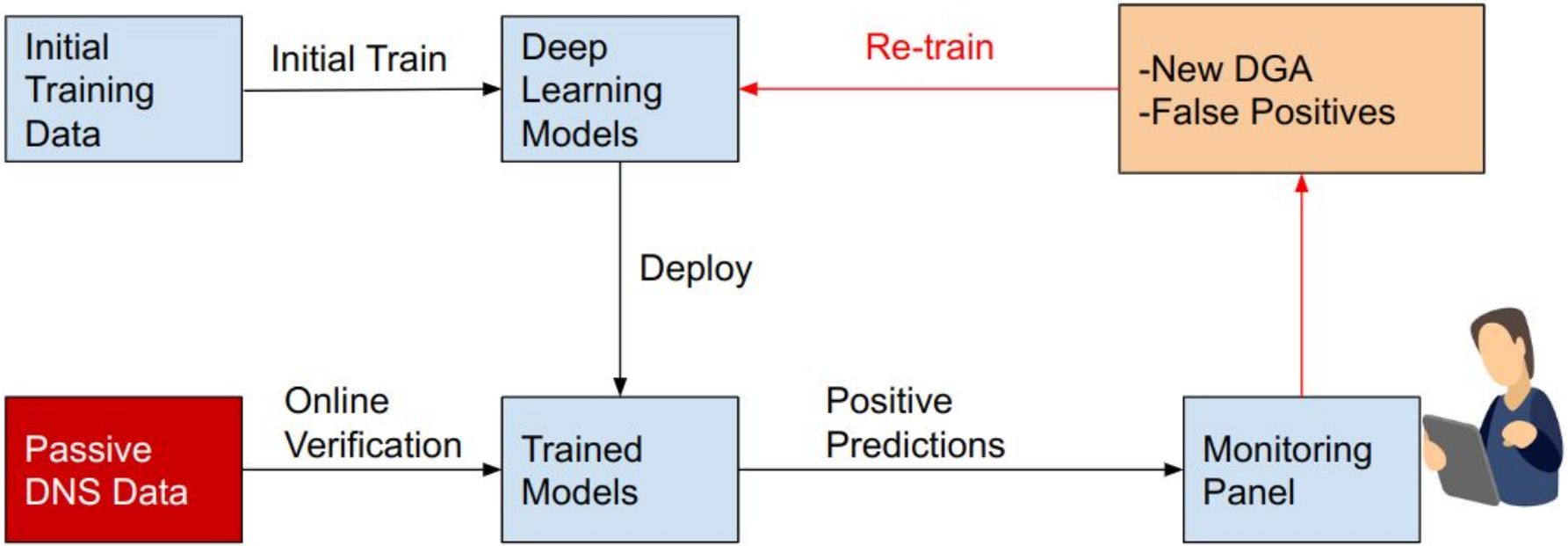
Fonte: https://www.spamhaus.com/resource-center/what-is-passive-dns-a-beginners-guide/

E o DNS Passivo?

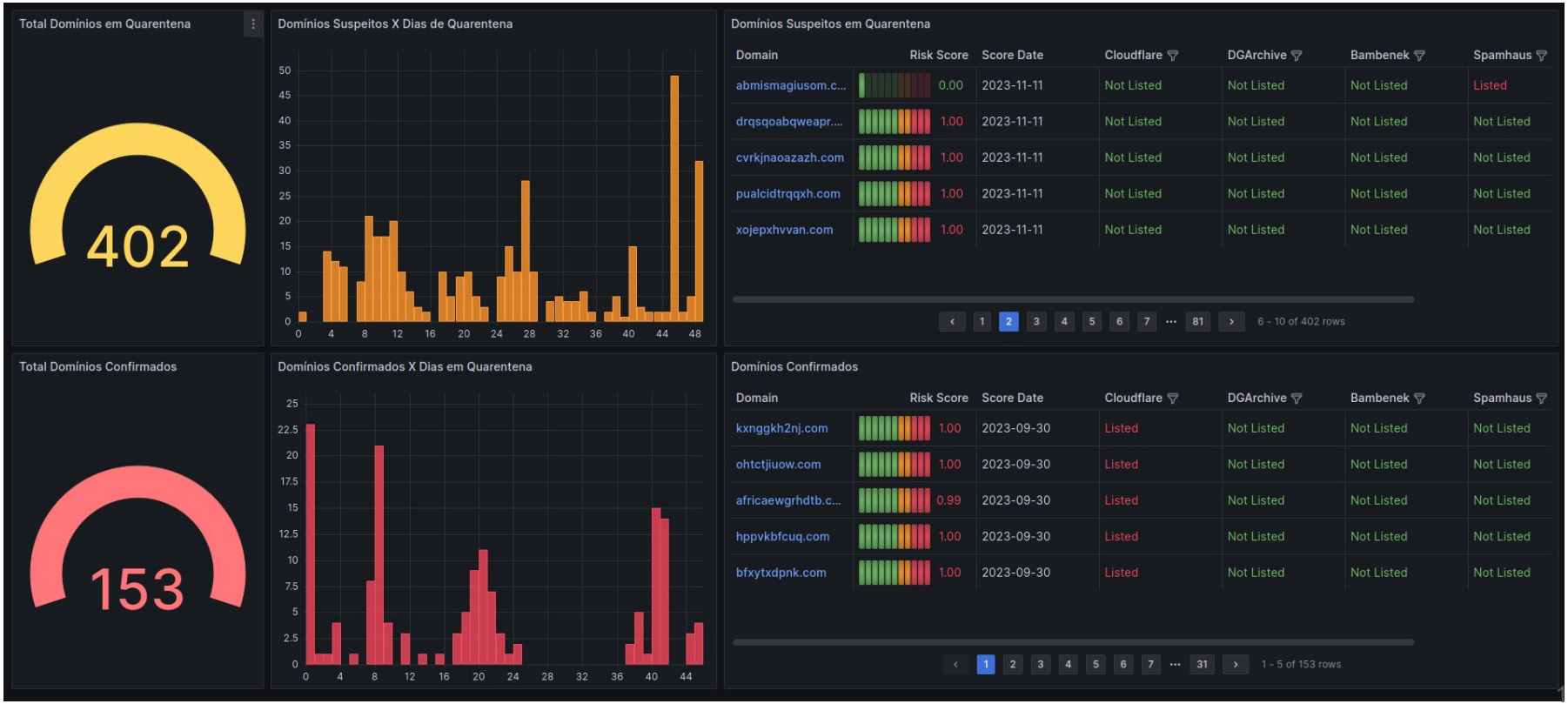
IP Cliente || IP DNS || Consulta || Tipo || Resposta || TTL

200.145.x.x || 200.145.x.x || north-america.pool.ntp.org. || A || 45.33.53.84 || 140

Incremental Monitor Schema



pDNS Monitor



Status

- Modelo Convolucional (Detecção e Classificação) - OK
- Modelo Incremental - Avançado…
- Integração DNS Passivo - Avançado…
- Painel de Monitoramento - Avançado…

Referências

- SILVEIRA, M. R. et al. Detection of newly registered malicious domains through passive dns. In: 2021 IEEE International Conference on Big Data (Big Data). [S.l.: s.n.], 2021. p. 3360–3369
- SUN, X.; LIU, Z. Domain generation algorithms detection with feature extraction and domain center construction. PLOS ONE, Public Library of Science, v. 18, p. 1–25, 01 2023. Disponível em: <https://doi.org/10.1371/journal.pone.0279866>.
- Computer Incident Response Center Luxembourg (CIRCL) Passive DNS 2.0. Disponível em : https://www.circl.lu/services/passive-dns
- Research and Education Networks Information Sharing and Analysis Center (REN-ISAC). Disponível em: https://www.ren-isac.net/member-resources/pDNS.html

Obrigado!

rafael.gregorio@unesp.br