Classificação de Domínios Recém-Registrados por meio de DNS Passivo

Leandro Marcos da Silva
Universidade Estadual Paulista
(UNESP)
leandro.marcos@unesp.br

MSc. Marcos Rogério Silveira
Universidade Estadual Paulista
(UNESP)
marcos.r.silveira@unesp.br

PhD. Adriano Mauro Cansian
Universidade Estadual Paulista
(UNESP)
adriano.cansian@unesp.br

Hugo Koji Kobayashi
Núcleo de Informação e
Coordenação do Ponto BR (NIC.BR)
koji@registro.br

lacnog 2021 LACNIC36

Universidade Estadual Paulista (UNESP)
Departamento de Ciências de Computação e Estatística (DCCE)

Laboratório ACME! de Pesquisa em Cibersegurança

Núcleo de Informação e Coordenação do Ponto BR (NIC.br)
Projeto: Detecção de Registro Fraudulento de Nomes de Domínio

Agenda

- Introdução;
- Desenvolvimento;
- Resultados;
- Conclusões.

1.

Introdução

Introdução

- *Domain Name System* (DNS);
- 524 milhões de domínios registrados (DOMAIN NAME STAT, 2021);
- Domínios são registrados para fins maliciosos;
- Um em cada dez URLs são maliciosos (SYMANTEC, 2019);
- Utilização de *blocklists*;
- Técnicas de aprendizado de máquina.
  - Análise de características léxicas, DNS ativo e passivo.

Introdução

- DNS passivo (WEIMER, 2005):
  - *Sniffers* instalados na rede que coletam consultas e respostas reais dos servidores DNS;
  - Recursos significativos para identificar domínios maliciosos;
  - Possibilidade de enriquecer os dados;
  - Possíveis locais de coleta:
    - Servidores recursivos de *Internet Service Provider* (ISP);
    - Servidores autoritativos de *Top-Level Domains* (TLDs).

- **Objetivo deste trabalho:** um sistema eficaz para classificar domínios recém-registrados nos primeiros três dias.

3.

Desenvolvimento

Desenvolvimento

- Tráfego DNS coletado de um servidor autoritativo de TLD;
  - Maior visibilidade global;
  - 12 meses de coleta;
  - **Sistema de coleta:** ENTRADA (WULLINK *et al.*, 2016):
    - *Data streaming* de alto-desempenho que analisa tráfego de rede.

- ENTRADA:
  - Responsável por limpar, enriquecer e compactar os dados;
  - Converte os arquivos do formato PCAP para Apache Parquet;
  - Processo de enriquecimento resulta nas colunas:
    - Código de país e *Autonomous System Number* (ASN) (GeoIP).

Desenvolvimento

- 20 características exclusivas do DNS passivo em conjunto com os dados enriquecidos no ENTRADA;
- Tratamento do desbalanceamento de classes;
- Uso de algoritmos de aprendizado de máquina de ponta;
  - XGBoost e LightGBM.

- A metodologia do sistema divide-se em:
  - Preparação do modelo;
  - Modelo em produção.

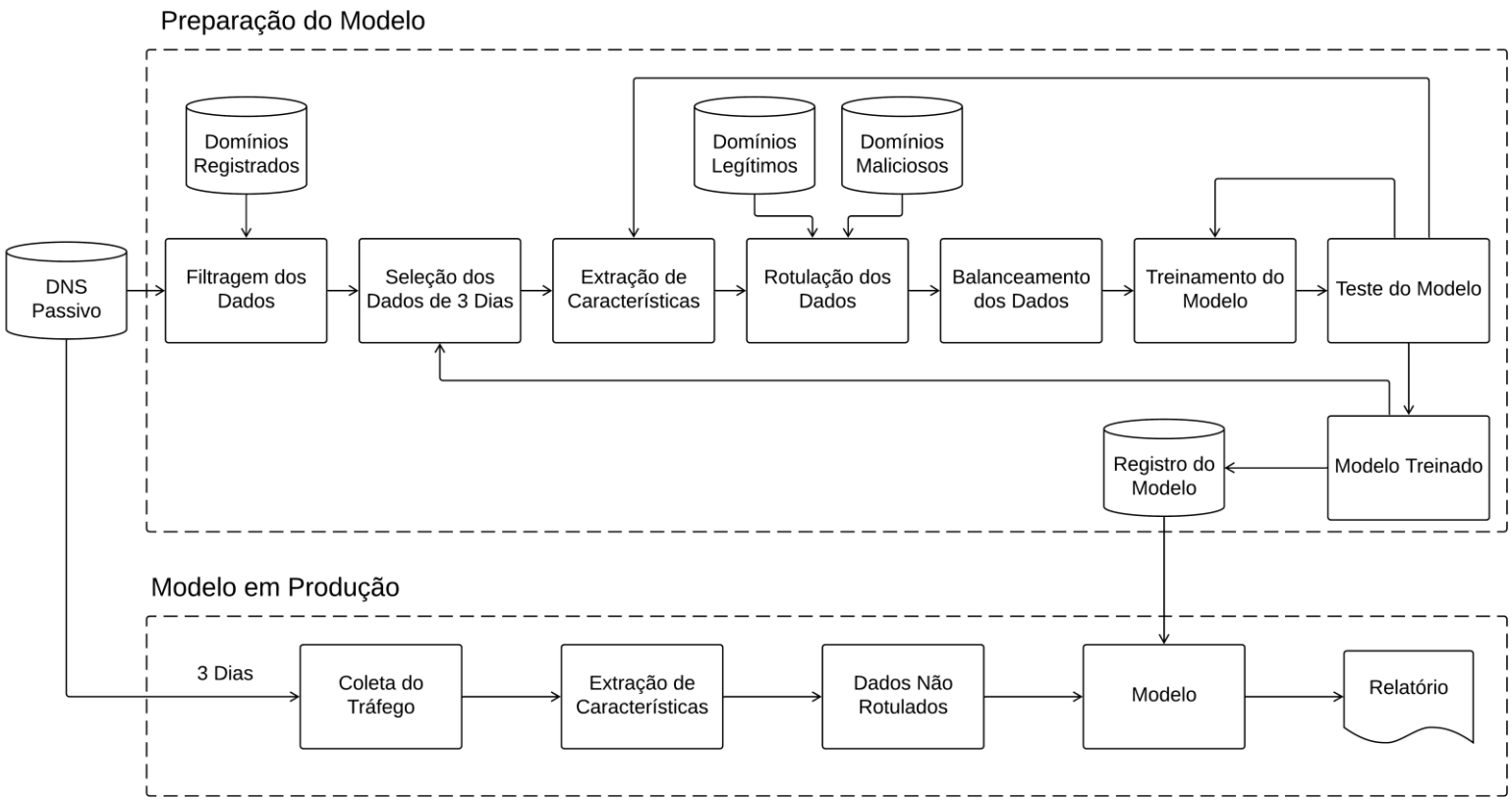

Figura 1: Diagrama do funcionamento do sistema

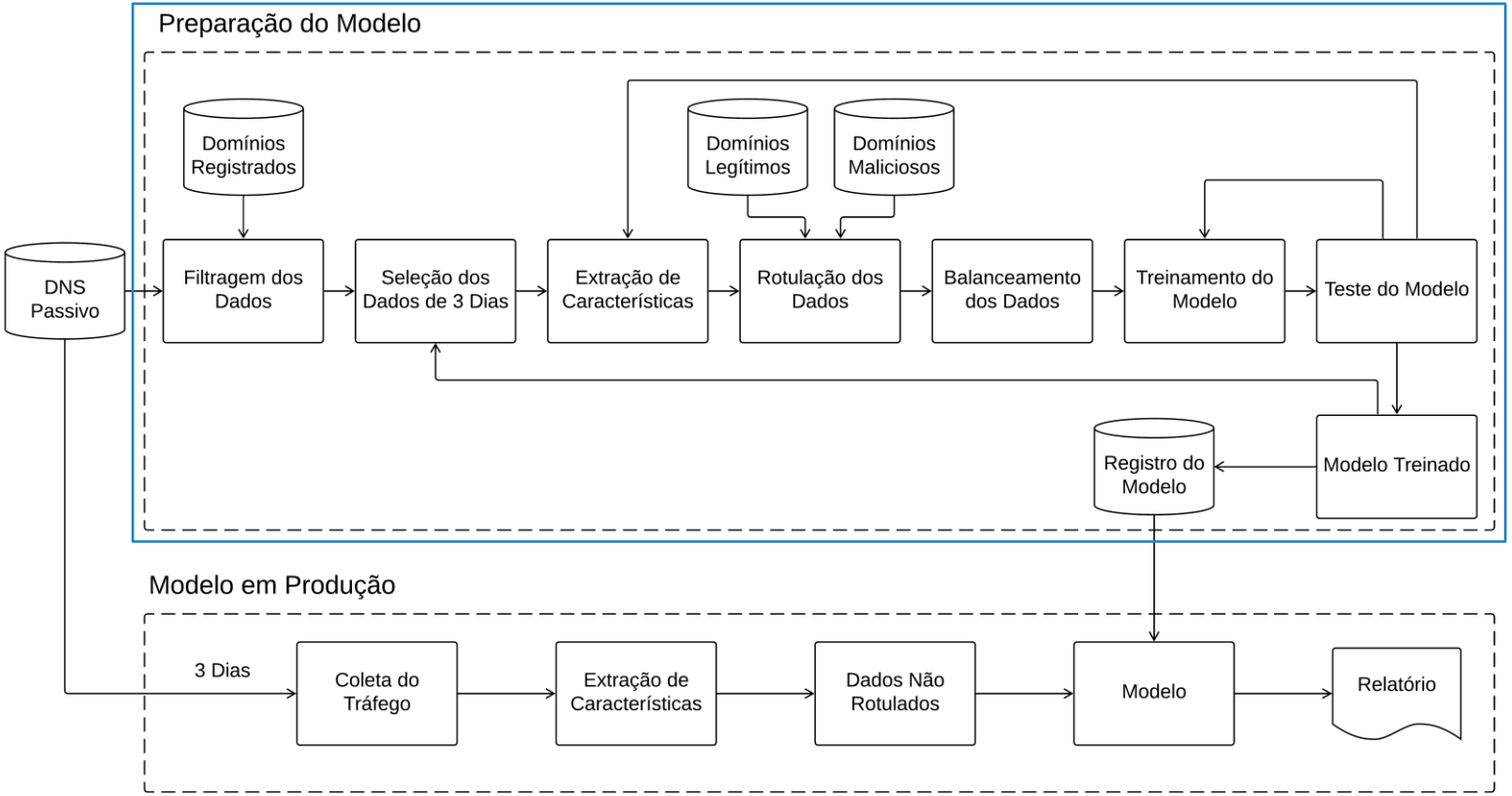

Figura 1: Diagrama do funcionamento do sistema

Desenvolvimento

- Desbalanceamento de classes:
  - 88.926 domínios legítimos;
  - 1.062 domínios maliciosos.

- Combinação das técnicas de:
  - **Subamostragem:** *Cluster Centroids*;
  - **Sobreamostragem:** K-*Means* SMOTE;
  - Ao balancear as classes:
    - 2.124 domínios legítimos;
    - 2.125 domínios maliciosos.

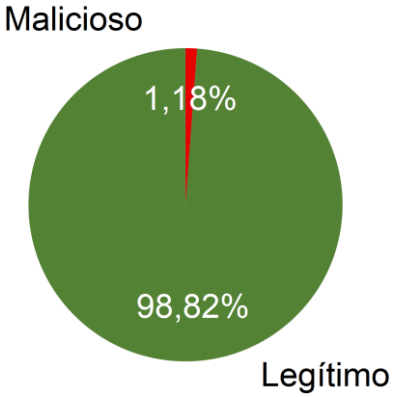

Figura 2: Desbalanceamento de classes no conjunto de dados

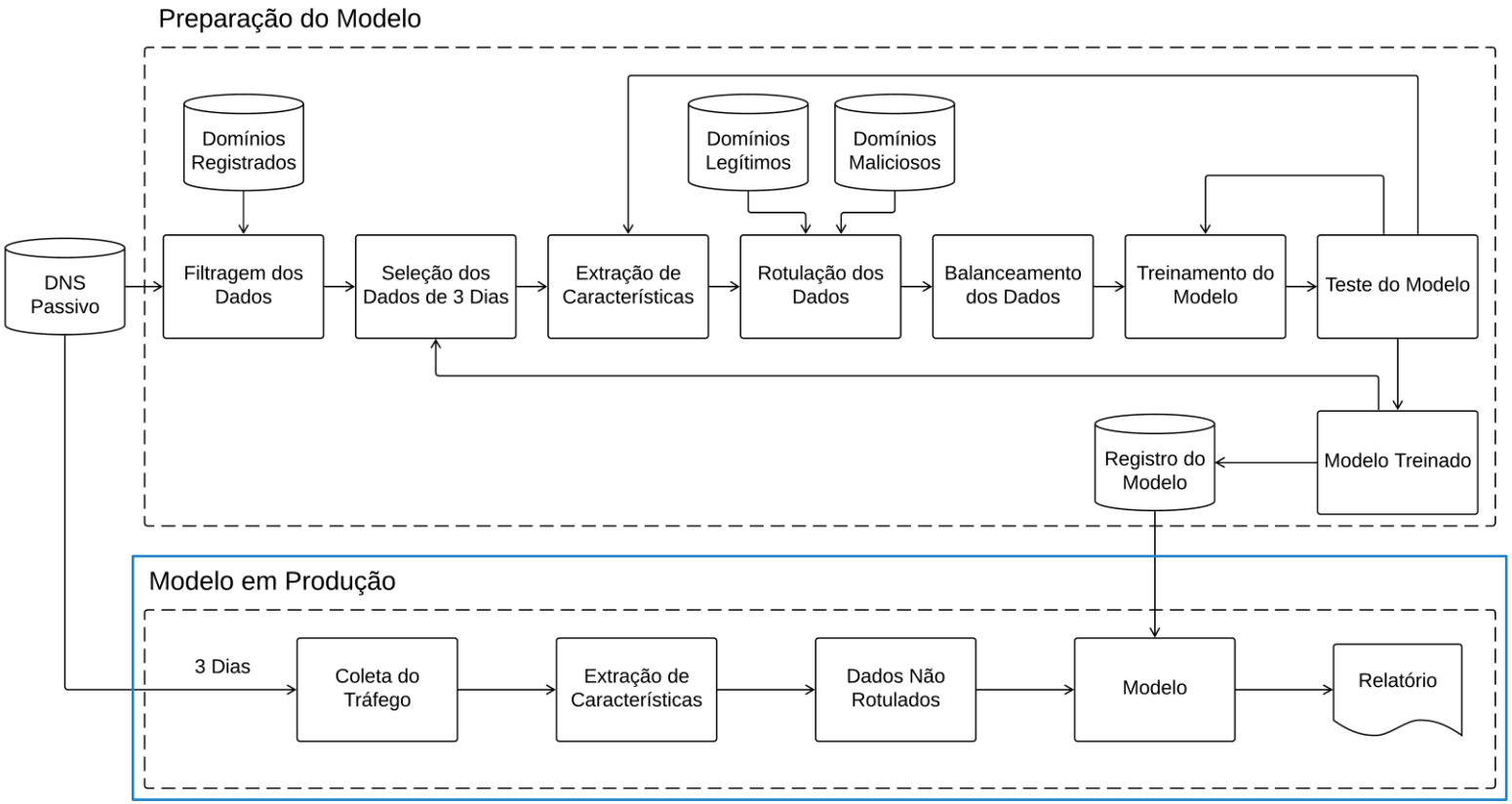

Figura 1: Diagrama do funcionamento do sistema

4.

Resultados

Resultados

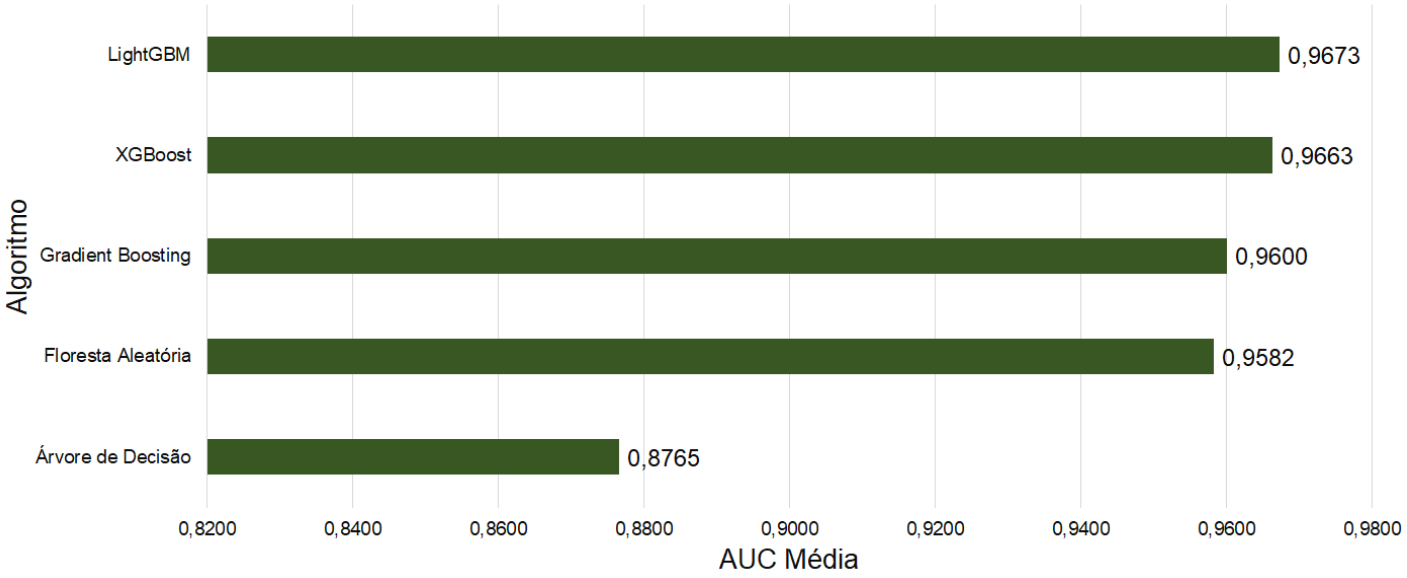

Figura 3: *Area Under the* ROC *Curve* (AUC) média em cada algoritmo

ROC: *Receiver Operating Characteristic*

Resultados

- Melhor resultado:
  - **AUC média:** 0,9673;
  - Algoritmo LightGBM;
  - **Tempo:** 1,89855 segundos;
  - Uso de otimização Bayesiana:
    - Sete hiperparâmetros;
    - 50 pontos iniciais;
    - 500 iterações.

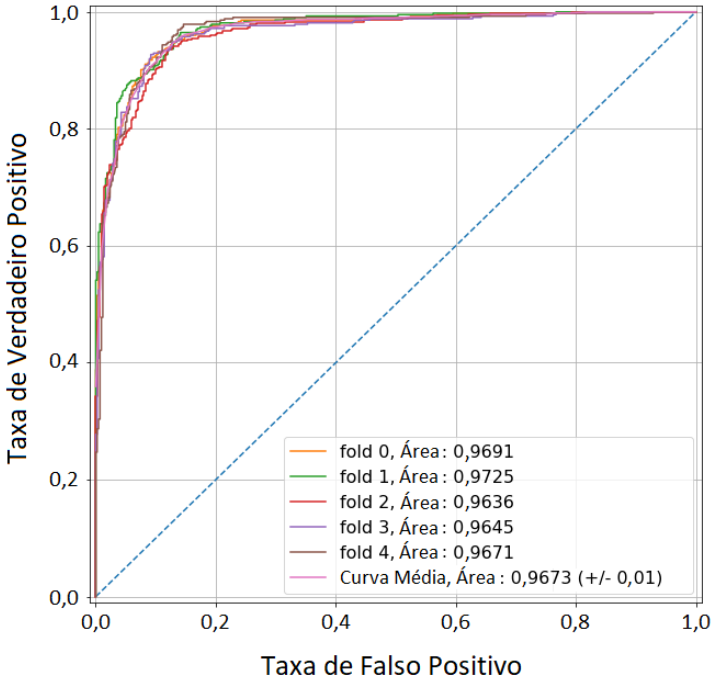

Figura 4: Curva ROC e AUC – LightGBM

Resultados

- Melhor resultado:
  - **AUC média:** 0,9673;
  - Algoritmo LightGBM;
  - **Tempo:** 1,89855 segundos;
  - Uso de otimização Bayesiana:
    - Sete hiperparâmetros;
    - 50 pontos iniciais;
    - 500 iterações.

- Destaque em determinadas características.

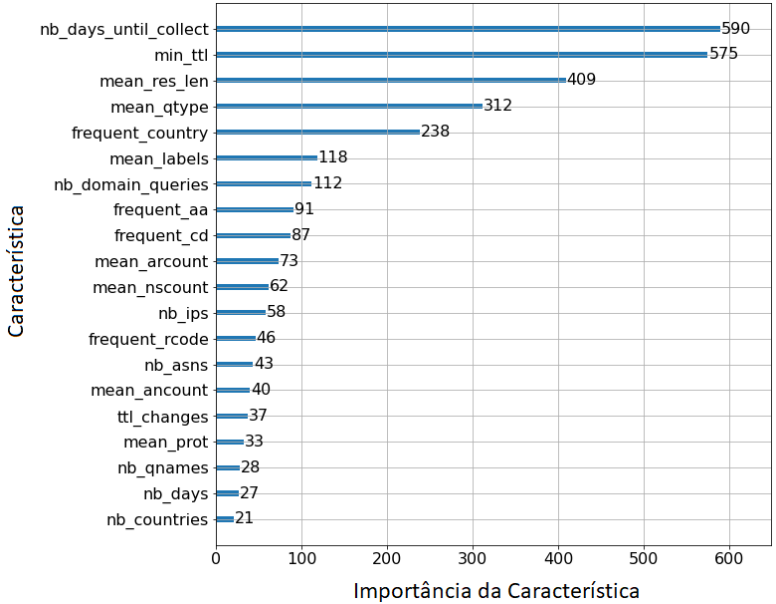

Figura 5: Importância de cada característica

Resultados

- Validação do modelo:
  - Dados coletados em 8 meses;
  - TVP de 0,8656 e TFP de 0,3471;
  - Resultados interessantes na detecção de domínios maliciosos;
  - Ocorrência de muitos falsos positivos.
    - Provavelmente por conta da sobreamostragem nos dados.

		Classe Predita	
Classe Real		Malicioso	Legítimo
	Malicioso	335	52
	Legítimo	9.917	18.657

Tabela 1: Matriz de confusão da validação do modelo

TVP: Taxa de Verdadeiro Positivo
TFP: Taxa de Falso Positivo

5.

Conclusões

Conclusões

- Classificação de domínios recém-registrados em três dias;
  - Alta AUC média no treino e teste do modelo (0,9673);
  - TVP de 0,8656 em ambiente de teste.

- Características do DNS passivo com os dados enriquecidos;
  - Coleta do tráfego DNS de um servidor autoritativo de TLD.

- Aplicação das técnicas de balanceamento de classes;
- Uso do LightGBM com otimização Bayesiana.

Conclusões

- Importância de um TLD detectar domínios maliciosos recém-registrados rapidamente;

- Próximos passos:
  - Mais dados de domínios maliciosos ao longo do tempo;
    - Auxílio do aprendizado não supervisionado.
  - Treinamento incremental;
  - Monitoramento dos domínios nas primeiras quatro semanas.

6.

Agradecimento

Agradecimento

Núcleo de Informação e Coordenação do Ponto BR (NIC.br), por financiar esta pesquisa, sob processo Fundação para o Desenvolvimento da UNESP (Fundunesp), número 2764/2018.

7.

Referências

Referências

1. LYNN, M. S. A Unique, Authoritative Root for the DNS. *The Internet Protocol Journal*, v. 4, n. 3, 2001. Disponível em: <https://www.icann.org/resources/pages/unique-authoritative-root-2012-02-25-en>.
2. DOMAIN NAME STATE. *Domain Name Registration's Statistics*. Domain Name Stat, 2021. Disponível em: <https://domainnamestat.com/statistics/overview>. Acesso em: 15 de set. de 2021.
3. SYMANTEC. *Internet Security Threat Report – Volume 24 (February 2019)*. Disponível em: <https://docs.broadcom.com/doc/istr-24-2019-en>. Acesso em: 23 de ago. de 2021.
4. DESMET, L.; SPOOREN, J.; VISSERS, T.; JANSSEN, P.; JOOSEN, W. Premadoma: An Operational Solution to Prevent Malicious Domain Name Registrations in the .eu TLD. In: *Digital Threats: Research and Practice*, v. 2, n. 1, p. 1-24, 2021.
5. KOUNTOURAS, A.; KINTIS, P.; LEVER, C.; CHEN, Y., NADJI, Y.; DAGON, D.; ANTONAKAKIS, M.; JOFFE, R. Enabling Network Security through Active DNS Datasets. In: *International Symposium on Research in Attacks, Intrusions, and Defenses*, p. 188-208. Springer, 2016.
6. WEIMER, F. Passive DNS Replication. In: *FIRST Conference on Computer Security Incident*. p. 1-14, 2005.
7. ANTONAKAKIS, M.; PERDISCI, R.; DAGON, D.; LEE, W.; FEAMSTER, N. Building a Dynamic Reputation System for DNS. In: *Proceedings of the 19th USENIX Security Symposium*, p. 273-290, 2010.
8. BILGE, L.; KIRDA, E.; KRUEGEL, C.; BALDUZZI, M. EXPOSURE: Finding Malicious Domains Using Passive DNS Analysis. In: *Ndss*, 2011, p. 1-17.
9. ANTONAKAKIS, M.; PERDISCI, R.; LEE, W.; VASILOGLOU, N.; DAGON, D. Detecting Malware Domains at the Upper DNS Hierarchy. In: *Proceedings of the 20th USENIX Security Symposium*, p. 1-16, 2011.

Referências

9. BAO, Z.; WANG, W.; LAN, Y. Using Passive DNS to Detect Malicious Domain Name. In: *Proceedings of the 3rd International Conference on Vision, Image and Signal Processing*, p. 1-8, 2019.
10. WANG, Q.; LI, L.; JIANG, B.; LU, Z.; LIU, J.; JIAN, S. Malicious Domain Detection Based on K-means and SMOTE. In: *International Conference on Computational Science*, p. 468-481. Springer, 2020.
11. SILVEIRA, M. R.; DA SILVA, L. M.; CANSIAN, A. M.; KOBAYASHI, H. K. XGBoost Applied to Identify Malicious Domains Using Passive DNS. In: *2020 IEEE 19th International Symposium on Network Computing and Applications (NCA)*, p. 1-4. IEEE, 2020.
12. WULLINK, M.; MOURA, G. C. M.; MÜLLER, M.; HESSELMAN, C. ENTRADA: A High-Performance Network Traffic Data Streaming Warehouse. In: *NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium*, p. 913-918. IEEE, 2016.
13. KE, G.; MENG, Q.; FINLEY, T.; WANG, T.; CHEN, W.; MA, W.; YE, Q.; LIU, T. Y. LightGBM: A Highly Efficient Gradient Boosting Decision Tree. In: *Advances in Neural Information Processing Systems 30 (NIPS 2017)*, v. 30, p. 3146-3154, 2017.
14. FERNÁNDEZ, A.; GARCÍA, S.; GALAR, M.; PRATI, R. C.; KRAWCZYK, B.; HERRERA, F. *Learning from Imbalanced Data Sets*. Berlin: Springer, 2018.
15. YEN, S. J.; LEE, Y. S. Cluster-based Under-Sampling Approaches for Imbalanced Data Distributions. In: *Expert Systems with Applications*, v. 36, n. 3, p. 5718-5727, 2009.
16. DOUZAS, G.; BACAO, F.; LAST, F. Improving Imbalanced Learning through a Heuristic Oversampling Method based on K-Means and SMOTE. In: *Information Sciences*, v. 465, p. 1-20, 2018.

Muito obrigado!

Leandro Marcos da Silva
leandro.marcos@unesp.br

PGP Key ID: 0x807DE4B5

Dúvidas?

lacnog 2021 LACNIC36