---------------------------------------------------------------

加密流量恶意性检测：

--------------------------------------------------------------

Feasibility of Malware Traffic Analysis through TLS-Encrypted Flow Visualization【加密流量恶意性检测】

作者与单位：Dongeon Kim, Jihun Han, Jinwoo Lee, and Heejun Roh ,Wonjun Lee (Seoul,Korea University, KOREA)

出处：[10.1109/ICNP49622.2020.9259387](https://doi.org/10.1109/ICNP49622.2020.9259387" \t "_blank) [2020 IEEE 28th International Conference on Network Protocols (ICNP)] (13-16 Oct. 2020)  [[https://icnp20.cs.ucr.edu/proceedings/poster/Feasibility of Malware Traffic Analysis through TLS-Encrypted Flow Visualization.pdf](https://icnp20.cs.ucr.edu/proceedings/poster/Feasibility%20of%20Malware%20Traffic%20Analysis%20through%20TLS-Encrypted%20Flow%20Visualization.pdf)](https://arxiv.org/abs/1607.01639)

描述：现有的关于TLS特征提取的方法过于繁琐，文中提出将TLS加密流的元数据进行可视化，以作为恶意流量分析和分类的更好方法。提出了粗粒度的方法，称为TLS加密流可视化。

[A distance-based method for building an encrypted malware traffic identification framework](https://ieeexplore.ieee.org/abstract/document/8771116/)【加密流量恶意性检测（识别）】

作者与单位：JIAYONG LIU, ZHIYI TIAN, RONGFENG ZHENG, LIANG LIU(Sichuan University, China)

出处：arXiv:2010.11627[IEEE Access,2019](Submitted on May 27, 2019) <https://ieeexplore.ieee.org/abstract/document/8771116>

描述：提出了一种基于距离的方法，利用无监督学习算法高斯混合模型（GMM）和排序点来识别聚类结构，用以计算恶意软件之间的distance参数。利用此参数定义名为FClass的新恶意软件类。用新算法XGBoost训练模型与其他的四种方法进行比较评估，证明为最佳。

MalDetect:A\_Structure\_of\_Encrypted\_Malware\_Traffic\_Detection【加密流量恶意性检测】

作者与单位：Jiyuan Liu , Yingzhi Zeng , Jiangyong Shi , Yuexiang Yang , Rui Wang and Liangzhong He (National University of Defence Technology, China)

出处：doi:10.32604/cmc.2019.05610[Computers, Materials and Continua] (January 2019) <https://www.researchgate.net/profile/Jiyuan_Liu7/publication/334697582_MalDetect_A_Structure_of_Encrypted_Malware_Traffic_Detection/links/5d3ad28a92851cd046871c67/MalDetect-A-Structure-of-Encrypted-Malware-Traffic-Detection.pdf>

描述：提出了新的检测框架MalDectct，从8个数据包提取特征。由于应对新流量样本的检测效率低下，部署了随机森林树的检测手段。

【arXiv preprint arXiv:1705.09044, 2017】Detecting Malignant TLS Servers Using Machine Learning Techniques【基于机器学习，检测恶意的TLS证书服务器】

【IEEE 2019】Deep-full-range:A deep learning based network encrypted traffic classification and intrusion【基于深度学习的流量分类，以及入侵检测框架】(顾华玺导师团队)

描述:提出基于深度学习的轻量级框架，用于加密流量分类和入侵检测。深度全范围（DFR方法）从原始流量学习，取得了良好的效果，且对存储要求不高。

【CM&Continua 2019】MalDetect： A Structure of Encrypted Malware Traffic Detection【恶意流量检测】

描述:提出并部署了随机森林树，在TLS握手结束之前从包中提取特征，而不使用完整的流

【ICL 2019】Detection of Malware in TLS Traffic【恶意流量检测】

描述:从元数据、TLS参数、证书三个数据特征列举恶性和良性TLS流的差异，并以此作为分类标准

【NDSS 2021】FARE: Enabling Finegrained Attack Categorization under Low-quality Labeled Data【把机器学习用于攻击检测】

描述: 监督机器学习分类器已广泛用于攻击检测，但它们的训练需要大量的高质量标签。不幸的是，由于数据标记的高成本和攻击者的不断演变，在实践中很难获得高质量的标签。如果没有这样的标签，训练和部署有针对性的对策是很有挑战性的。

【Cisco 2018】Deciphering Malware’s use of TLS (without

Decryption）【恶意流量检测】

描述:如何在不解密的情况下快速识别TLS流量，即只需要在握手前从包中提取特征

【AISec 2016】Identifying Encrypted Malware Traffic with Contextual Flow Data【恶意流量检测】（承上，思科团队）

描述:提出了独特的获取数据的方法，只需要在TLS握手结束前从包中提取特征

【ICNP 2016】Enhanced telemetry for encrypted threat analytics【威胁分析检测】（承上，思科团队）

描述:提出了网络流量检测系统，新的数据特征被搜集并作为数据集，增加了**数据特征**的使用

【IEEE ACCESS 2020】A Deep Hierarchical Network for Packet-Level

Malicious Traffic Detection【恶意流量检测，基于数据包】

描述:设计了一个在数据包层次上进行恶意留了检测的深度分层网络，能够从原始数据包学习流量特征

【IEEE 2018】Classification of malicious traffic using tensorflow machine learning

【恶意流量分类】

描述: 利用TensorFlow平台，设计了一个基于TensorFlow的深度学习模型框架来对恶意流量进行分类

【Computer&Science 2017】Detecting Malignant TLS Servers Using Machine Learning Techniques【基于机器学习的流量检测】

描述: 提出基于关于机器学习的方法，能够验证web证书是否为恶性，解决了人工无法解决的问题

-------------------------------------------------------

**增量学习、集成学习、迁移学习方法：**

-------------------------------------------------------

在二分类任务中，如需要引入加密恶意流量的恶意样本，相当于在已知类中添加样本，使模型“认识”以前的恶意样本，是任务增量学习。

在多分类任务中，已经认识m个类，如何扩充至认识(m+n)个类，是难点。类增量学习有三大类别，正则、回放和参数隔离。由于参数隔离目前处于研究阶段且应用少，不展开。

**实现方式：正则化**

【ECCV 2016】Learning without Forgetting【基于深度学习的增量学习】

描述:改进的CNN方法，开山之作，后续方法都是在此的改进

基于正则化的增量学习方法通过引入额外损失的方式来修正梯度，保护模型学习到的旧知识，提供了一种缓解特定条件下的灾难性遗忘的方法

【ICCV 2017】Encoder Based Lifelong Learning【基于低维特征映射的EBLL算法，上述方法的改进】

PNAS 2017 Overcoming catastrophic forgetting in neural networks 【基于贝叶斯框架的EWC算法，对第一篇论文的改进】

ICPR 2018 Rotate your Networks: Better Weight Consolidation and Less Catastrophic Forgetting【对第一篇论文的改进】

-------------------------------------------------------------------

**实现方式：回放 能够保留原有的模型进行预测，尽可能保留之前训练样本的信息，并随时加入训练**

【CVPR 2017】iCaRL: Incremental Classifier and Representation Learning

描述: 和LwF比较相似，它同样引入了蒸馏损失来更新模型参数，但又放松了完全不能使用旧数据的限制

【CVPR 2019】Large Scale Incremental Learning

描述: 借鉴了知识蒸馏技术，从不同的角度来缓解灾难性遗忘问题

【NIPS 2019】Experience Replay for Continual Learning

描述: 指出这类模型可以动态调整旧数据的保留数量，从而避免了LwF算法随着任务数量的增大，计算成本线性增长的缺点

【NIPS 2017】Gradient Episodic Memory for Continual Learning

描述: 提出了梯度片段记忆算法(GEM)

-------------------------------------------------------

IoT、CPS、工控恶意与异常检测：

-------------------------------------------------------

【IEEE Access 2021】Integrated Fuzzy Based Computational Mechanism for the Selection of Effective Malicious Traffic Detection Approach【恶意流量检测】

描述:针对使用关于模糊测试的网络恶意流量检测，评价各变量机器相互依存关系，解决的是识别未知恶意流量家族的问题

【USS 2019】iOS, Your OS, Everybody’s OS: Vetting and Analyzing

Network Services of iOS Applications【隐私保护】

描述: 对于智能手机的监听可能会带来严重的安全隐患，本文基于iOS系统进行的测试，弥补了相关研究的空白

【Computer&Secuity 2020】IoT malicious traffic identification using wrapper-based feature selection mechanisms【IoT流量检测】

描述: 对于物联网安全中特征选择不够精确的问题，本文提出了新的特征度量方法

【IEEE 2020】CorrAUC: a Malicious Bot-IoT Traffic Detection Method in IoT Network Using Machine Learning Techniques【IoT流量检测，接上】

描述: 详细描述了特征选择算法Corracc，优化性能

【IEEE 2020】IoT-KEEPER: Detecting Malicious IoT Network Activity using Online Traffic Analysis at the Edge【IoT流量检测】

描述: 提出了一种IoT系统，在网关执行流量分析，检测恶意网络活动

-------------------------------------------------------

**其他恶意与异常检测：**

-------------------------------------------------------

【USS 2020】Measuring and Modeling the Label Dynamics of

Online Anti-Malware Engines【防恶意软件检测钓鱼攻击】

描述:对由于安全威胁产生的恶意软件进行检测分类，验证了基于阈值的标签聚合的作用

【CSS 2018】Measuring and Modeling the Label Dynamics of

Online Anti-Malware Engines【利用递归神经网络预测恶意攻击】

描述:对复杂系统的潜在威胁与攻击检测和预测，同时提供攻击者遵循技术与顺序

【SSP 2017】A Lustrum of Malware Network Communication Evolution and Insights【恶意软件通信】

描述:恶意软件分析是对抗互联网威胁的重要前沿领域，基于恶意软件的动态执行，能够对软件域的特征和时态网络特性进行观察

-------------------------------------------------------

其他应用的恶意性检测（邮件、钓鱼网站）

-------------------------------------------------------

【USS 2019】Detecting and Characterizing Lateral Phishing at Scale【在众多电子邮件中识别钓鱼邮件】

描述:考虑建立了相关的攻击者模型（即模拟了若干种如何使用钓鱼邮件进行欺诈）和检测相关攻击

【USS 2019】High Precision Detection of Business Email Compromise【恶意电子邮件攻击检测，邮件是主要的入口，这方面的研究也很多】

描述:设计了一个依赖于监督学习的系统，依赖于大量的BEC电子邮件数据集

【USS 2020】On Training Robust PDF Malware Classifiers【关于PDF格式文档的恶意软件分类器】