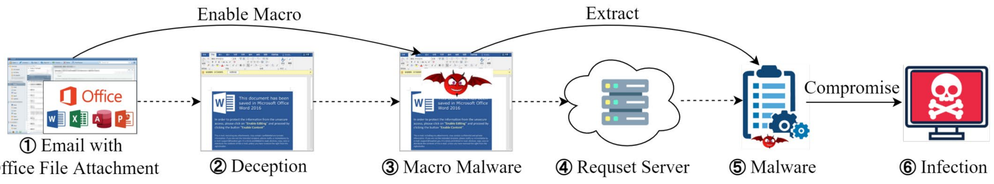
DitDetector: Bimodal Learning based on Deceptive Image and Text for Macro Malware Detection

基于诱骗图像和文本双模态学习的宏恶意代码检测 (ACSAC)

Jia Yan, Ming Wan, Xiangkun Jia, Lingyun Ying✉, Purui Su✉, Zhanyi Wang
(联系人：贾相堃，xiangkun@iscas.ac.cn)

问题描述



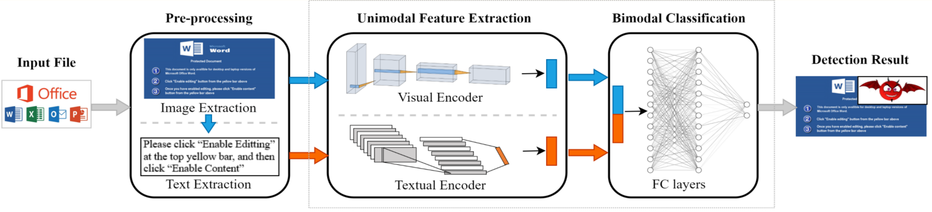
宏 (Macro)，是微软提供的进行自动化操作的接口，但是常被黑客用来编写恶意代码，因此微软设置了“默认关闭宏”。相应的，黑客在恶意代码中加入诱骗信息、**诱骗受害者“打开宏”**(②)，释放恶意代码。黑客还提出了**远程下载真正恶意代码**等检测绕过手段(④)。

相关工作

Attack Stage	Defense Solution	Information Used	ML†
①	Spam filtering	Email content	◐
②,③	Document analysis	Signature	◐
		File metadata	◐
		Macro code	●
		Deception information	○
④	Traffic analysis	Network traffic	◐
⑤,⑥	Runtime detection	Dynamic behavior	◐

- 防御者在利用宏恶意代码的攻击链中的**不同阶段**添加了防御措施。
- 包括基于机器学习的方案和非机器学习方案。然而重量级方案效率不足，轻量级方案精度不足。
- 针对**代码恶意性**的检测容易被绕过。

解决思路



基于图像和文本双模态学习的分类模型（MobileNetV3+TextCNN）

DitDetector的效果

MalDoc数据集

Model	Precision	Recall	Accuracy	F1-score
MLP	0.9906	0.9904	0.9904	0.9905
RFC	0.9910	0.9909	0.9909	0.9910
SVC	0.9896	0.9895	0.9895	0.9895
XGBoost	0.9805	0.9798	0.9798	0.9800
DitDetector	**0.9935**	**0.9935**	**0.9935**	**0.9934**

收集的样本数据集（From奇安信）

Dataset	MLP	RFC	SVC	XGBoost	*DitDetector*
MalDoc	0.9905	0.9910	0.9895	0.9800	**0.9934**
XL4 Macro	0.2358	0.6927	0.9405	0.9537	**0.9993**
RTInjection*	–	–	–	–	**0.9990**

*其他方案无法检测远程下载的样本

商用引擎对比

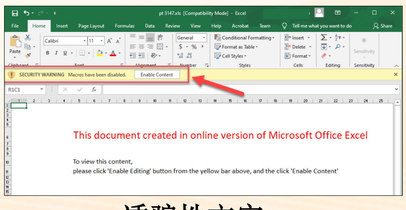
Dataset	Kaspersky	Symantec	Microsoft	McAfee	Sophos	*DitDetector*
Maldoc	0.9684	0.8988	0.9607	0.9620	0.8726	**0.9934**
XL4 Macro	0.9219	0.8435	0.9677	0.8990	0.6093	**0.9993**
RTInjection	0.9810	0.7972	0.7915	0.9206	0.4753	**0.9990**

消融实验

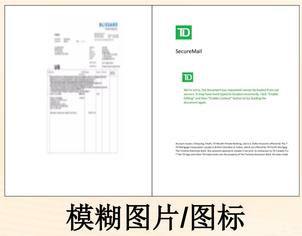
Model	Precision	Recall	Accuracy	F1-score
TextCNN	0.9791	0.9782	0.9782	0.9785
MobileNetV3	0.9473	0.9434	0.9434	0.9402
DitDetector	**0.9935**	**0.9935**	**0.9935**	**0.9934**

诱骗信息类型及示例

模拟官方提示



诱骗性文字



模糊图片/图标