## 以70%精度从安全博客中提取STIX网络威胁情报

摘要：威胁情报（CTI）共享的趋势稳步增长，开源情报（OSINT）提供定期更新的威胁信息。包括结构化的（STIX，OpenIOC）以及非结构化的（黑名单）。然后大部分情况下威胁情报精确程度不足以做出明智的安全决策。大多数指标内容多变，如ips 、hash等。缺乏攻击模式和攻击技术信息。

威胁信息存在大量的重复，需要大量人工来对信息进行筛选。我们用自然语言处理技术从非结构化文本中以70%精度提取有效信息。结果以STIX的标准威胁情报格式提供。

介绍：CTI威胁情报包括高级指标如活动、动机、战术、技术和程序，以及低级指标如ips、hash、。博客和文章提供了关于攻击的大量信息，包括妥协的指标，以及像攻击模式和杀伤链这样的高级信息。另一问题是处理CTI的实际实例和防止误报的指标、安全产品的广告以及可能与安全相关但不提供攻击信息的各种其他词语。此类文本还存在冗余和不一致的情况，如果不同信息源对一个攻击的信息不一致，很难确定哪个是更加可靠的信息。

使用命名实体识别技术Named Entity Recognition (Stanford NLP) 来提取信息。丰富并标准化为STIX格式便于存储和分享。为了提取CTI，我们使用了非监督学习方法并对来自二十多个不同来源的数据文档进行了注释。我们开发了一个RESTful web服务，用于执行注释和从文本内容中提取术语，其中不仅包括低级指标，还包括高级信息，尤其是TTPs和攻击模式。我们还创建了一个关联和聚合服务，该服务接收从众多来源提取的分阶段数据，并对它们进行关联和聚合，以消除冗余，并将与相同攻击相关的信息组合在一起。

指标：演员:归因于某次攻击的黑客团队，如卡巴纳克赛博帮、APT30等。

目标行业:攻击的目标行业，如金融机构、政府、军队等。

目标位置:攻击的具体地理目标，如南亚、土耳其、美国等。4

预期效果:攻击者的目标，如网络间谍、经济利益、窃取信息等。

技术(TTPs):攻击者采用的高级技术，例如鱼叉式网络钓鱼电子邮件、社交工程、水坑等。

使用的工具:攻击者使用的工具，如后门、反向shell、Mimikatz等。

目标应用程序:攻击者希望利用其漏洞的应用程序，例如MS Word、PowerShell等。

流程：先过滤掉所有unicode字符后，再对文本进行词性标注，必须能正确识别ip 和注册码。

Stanford nlp (使用线性crf 完成)

twiti: Social Listening for Threat Intelligence

从非结构化文本中提取威胁情报3：iocminer

数据集地址：<https://github.com/DissectMalware/IoCMiner/tree/master/dataset>

摘要：因为许多网络攻击者倾向于在多个攻击中重复使用或共享其网络基础设施、技术、战术和程序。因此，许多安全专业人员将他们的时间和精力用于搜寻网络威胁，并通过社交媒体和文本共享网站等公共数据共享平台与公众共享这些有价值的信息。

介绍：提出IoCMiner框架，用于自动提取在 ioc （indicators of Compromise） 中提取ioc。结合图论、机器学习和文本挖掘技术来实现目标。IoCMiner 根据声誉模型发现发布CTI的可信twiter用户，之后使用CTI分类器从观测流中进一步过滤出非CTI推特流。最后使用一组正则表达式从推文中提取CTI。由于数据共享平台上发布信息数量巨大，IoCMiner不去直接检查发布信息，而是鉴别信息源的可靠性。

IOC分为三组：原子IOC、计算IOC和行为IOC。原子IOC，如ip地址、域名、注册表项和进程名，表示网络攻击期间观察到的网络或系统工件。计算IOC是根据攻击期间观察到的数据（如恶意软件实例的哈希值）计算的IOC。行为IOC是其他IOC的组合，例如恶意docx文件，散列值为Ys托管在serverZ上，打开docx后，将在受攻击机器上执行恶意程序。

IOCMine收集了一批对追踪网络威胁和发布IOC感兴趣的用户发布的推文。大部分关于社交媒体的研究集中于那些有影响力的用户，而本研究的目的不在于此。

组件：1.识别IOC专家 2.使用词袋模型和随机森林算法来对含IOC内容进行分类 正确率97%

从非结构化威胁建议文本中半自动提取信息

摘要：使用自然语言处理技术和模式识别框架来提取信息。

介绍：各种软件或硬件组织（如Microsoft或Cisco）以及政府机构或监管机构发布的包含潜在漏洞或威胁信息的安全建议。我们使用自然语言处理、半监督模式识别和匹配技术，以半自动的方式从自然语言文档中提取这些安全公告中的关键信息。形成标准的结构化安全表达式（STIX）

数据集： M.S-ISAC. Multi-state information sharing centre.

<http://msisac.cisecurity.org/>.

F. Services. Information sharing and analysis center.

<https://www.fsisac.com/>.

USCERT. United states computer emergency

readiness team. https://www.us-cert.gov/.

模型：1.用半自动的匹配模板进行模式匹配，模板由basiilisk完成。 2 basiiilisk 用于对领域关键词的匹配模式的生成，匹配与否使用jaccorid等算法完成。

使用Opennlp3 完成句子检测， 使用clearNLP4完成句子语法等分析，使用ner识别通用命名实体帮助模板生成。

从非结构化文本中提取威胁情报1

摘要：本文提出了一种安全开源智能框架（OSIF），用于自动分析非结构化文本，生成基于事件的CTI。它使用自然语言处理、机器学习和数据挖掘等多种技术提取网络安全事件相关信息（设备、组织、位置等）和常见漏洞和暴露（CVE）以进行威胁行为人分析。最后，我们在从数十个网站收集的数据集上对关键威胁进行全面的结构和概念评估。在数据集上进行的实验表明，我们的方法具有相当高的性能。

介绍：使用nlp技术。识别文本中与安全相关的语义要素。使用ner事件模板和事件触发器来提取web文本中的语义要素。

相关工作：

Real-time discovery and geospatial visualization of mobility and industry events from large-scale, heterogeneous data streams

Extracting city traffic events from social streams

Toward automatic discovery and analysis of open-source cyber threat intelligence

本文工作：1.提出了框架OSIF来自动从非结构化文本中提取威胁信息

2.提出一种策略用于在开放数据源中查找安全相关信息

3.一种数据过滤和文本摘要方法，用于收集和选择安全相关信息

4.CTI模板

框架：1.爬虫和过滤器：爬取安全相关文章并过滤掉非安全相关 2.实体提取器和摘要生成器 实体提取器先用规则模板定义实体出现位置，再使用ner技术提取实体。摘要生成器使用textrank生成每篇文章的摘要，生成CTI。

过滤器：使用tf-idf统计，数据集131篇

Ner：类似 斯坦福 ner工具 44篇文章

Textrank：将句子视为顶点，边视为两个句子之间的相似性，连接一个顶点的句子越多，认为越重要。选取最重要的一些句子并按时间排序。

A Quantitative Evaluation of Trust in the Quality of Cyber Threat Intelligence Sources

摘要：本文提出一种根据定量参数来评估威胁信息来源可靠性的模型。

介绍：信息发布源每有一篇新的信息发布就会被评估，并同其他来源进行对比。两个指标质量和信任。能基于对威胁情报源提供的每条消息的参数的定量评估，得出每个消息源的信任值。

相关工作：

3：提出了一些指标

13：NLP工具自动识别威胁信息

15：类pagerank方法进行排名

方法：封闭世界假说：所有威胁情报都来自一组固定的源，通过比较源提供情报速度和original程度。

定量评价参数：extensiveness、maintenance、False Positives 等，给出定义以及定量计算方法。

信任参数：加权

更新：隔一段时间更新信任值：更新方式为由新的内容的计算结果加上过去的信任值进行加权

Twiti：social listening for threat intelligence

摘要：twiti：一种自动从twitter中提取各种形式恶意软件IOC的系统。Twiti不仅可以准确地提取恶意软件IOC，而且提取的IOC是唯一的和早期的。Twitter比其他公共威胁情报源更好捕获持续的恶意软件威胁。且只有小部分IOC来自商业供应商账户。其他均来自个人客户，有很高价值。

介绍：恶意软件ioc的示例包括恶意文件的MD5哈希，IP地址，僵尸网络的URL或域以及文件名。Twiti使用tweet分类器来识别可能包含恶意软件IOC的tweet，然后从tweet和其中的外部链接中提取IOC。通过twiti收集IOC并从数据源、文件类型、恶意软件类型等方面分析收集到的IOC特征。

贡献：1.高性能IOC提取系统，精度哈希0.93 URL0.92 唯一性高 延迟低

2.研究了twitter上IOC特征性质

Twiti组件:

收集器：根据关键字跟踪以及api用户跟踪和一些安全专家来寻找数据。

选择器：1.排除URL影响 2.具体的ip、url等被替换为【ip】，【url】。3使用bert训练的ner识别恶意软件名称

分类器：特征1.手工特征 2.n-grams特征 3.bag of words 用随机森林分类器进行

外部链接：筛选了与关键字同时出现的pastebin链接，安全博客，安全分析服务等

分析：ip、has、url、domain 从容量、效率、延迟、准确性四个方面评估twiti与其他源性能

[52]Shengping Zhou, Zi Long, Lianzhi Tan, and Hao Guo. 2018. Automatic identification of indi-cators of compromise using neural-based sequence labelling.arXiv preprint arXiv:1810.10156

(2018).

[38]Nuno Dionísio, Fernando Alves, Pedro M Ferreira, and Alysson Bessani. 2019. Cyberthreat

detection from twitter using deep neural networks. In2019 International Joint Conference on

Neural Networks (IJCNN). IEEE.

**IJCNN c会 2019**

**使用序列神经网络从非结构化安全文章内识别ioc**

13 参考文献 使用了双向lstm+crf 用于识别IOC

模型三层:

编码层 ：词向量+用bilstm训练的字符向量

序列层：bilstm+attention 两层attention+卷积层 人工特征向量

Crf层：crf

人工特征：1.拼写特征 通过拼写特征来确定是否有ioc存在，有就输出1

2.上下文特征 找到一组词，在ioc的上下文中出现频率较高且不说stopword和标点符号。利用这组词在任何一个词的上下文中出现的比例作为特征

用双语训练一次，效果比单语模型要好。-

没有数据集 ！！！！！

Apt原始数据：[https://github.com/CyberMonitor/APT\_CyberCriminal\_Campagin\_Collections](https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/tree/master/2021/2021.01.04.Dridex_Next_Strike)

**机器学习方法在快速筛选论坛威胁情报的潜力：**

C类 international conference on big data

摘要：黑客论坛里面有许多威胁情报存在，通过卷积网络和传统方法对比来进行判断是否包含信息，证明svm不必卷积差。

数据：

二分类数据：分为安全相关和安全不相关类。判断依据时是否包含关键字以及related work中。当这个标注并不全面，因此将未出现安全关键字且出现与运动、音乐等主题相关的标记为非安全相关。

多分类数据：在安全相关里面再根据关键字细分，这部分进行了人工审核。

没有数据！！！！

模型：svm 使用了 不同值的grams 和词级别以及字符级别的特征作为输入

Cnn使用了 glove/word2vec 来作为输入

实验结构 使用为word2vec效果较好，在训练数据训练出的词嵌入效果最好。但是使用random向量的效果也不错。

使用字符级3-grams的输入效果最好

**复杂网络时代下关于技术威胁情报的调查**

摘要：旨在给出什么是威胁情报，鉴别威胁情报的多种来源，收集方法、信息寿命以及使用情况。我们发现1.快速贡献不足以避免攻击 2.组织间的信任问题 3.通用标准格式能节约时间 4.不同组织目标不同，有的侧重标准化和自动分析需求，有的关注高速度

介绍：ioc 可分为三个类别

技术威胁情报限制：

1.数量大于质量 数量庞大 没有分类 及时性不够

2.

使用深度学习来在twitter中探测网络威胁

介绍：提出了一种智能威胁工具用于处理数据流来辨别相关安全信息并提取相关实体。

首先根据关键字过滤，然后使用cnn二分类是否与安全相关，再使用bilstm进行实体提取。

相关工作：【4】C. Sabottke, O. Suciu, and T. Dumitras, “Vulnerability Disclosure in

the Age of Social Media: Exploiting Twitter for Predicting Real-World

Exploits,” inProc. of the 24th USENIX Security Symposium (USENIX

Security 15). USENIX Association, 2015.

用svm分类器提取信息并从其他来源进行补充，进行了对抗性实验

【3】 X. Liao, K. Y uan, X. Wang, Z. Li, L. Xing, and R. Beyah, “Acing the

IOC Game: Toward Automatic Discovery and Analysis of Open-Source

Cyber Threat Intelligence,” inProc. of the 2016 ACM SIGSAC Confer-

ence on Computer and Communications Security (CCS). Association

for Computing Machinery, 2016.

iACE 使用语言规则来进行提取

【10】A. Severyn and A. Moschitti, “Twitter Sentiment Analysis with Deep

Convolutional Neural Networks,” inProc. of the 38th International

ACM SIGIR Conference on Research and Development in Information

Retrieval. Association for Computing Machinery, 2015.

推特情感分析挑战赛内容

数据：<https://github.com/ndionysus/twitter-cyberthreat-detection>

标记列表：org公司或组织 pro 产品或字长 ver 版本号可能与资产相关 vul 指代存在的威胁或漏洞 id漏洞标识符