
SPRING 春日版
CIS 2021
网络安全创新大会
Cyber Security Innovation Summit
AI for Attacker：攻击者画像
柳星 <root@4o4notfound.org>
网安江湖
谁主沉浮
REEBUF

## 柳星（404notfound）

- 白帽
- 专注安全智能化
- 蚂蚁集团 网商银行安全工程师
- 4o4notfound.org

# 目录

# 背景

# 背景

冰山一角

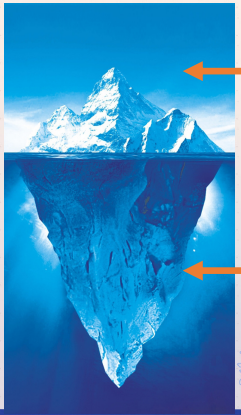
视野有限

知识有限

治标不治本

# 目的

看见攻击者



攻击表层

攻击者

# 目的 看清攻击者

基础属性：姓名、身份证、手机

高级属性：兴趣、爱好、性格

正常用户数字化

漏洞 身份

模式 资产

工具 等等

攻击者数字化

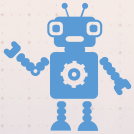
# 目的 管理Top风险

Top攻击者

Top风险

# 技术 全局技术

数据智能



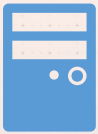
机器智能

知识图谱

# 技术

数据智能

主机层



网络层


关联计算

应用层

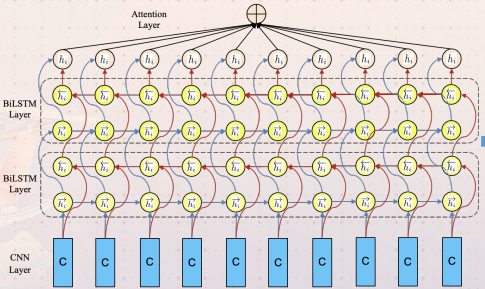
# 技术 机器智能

群体攻击

自动化攻击

- 攻击聚类：从大量攻击数据中找出共性
- 机器攻击分类：从大量原始数据中找出机器攻击

# 技术 机器智能



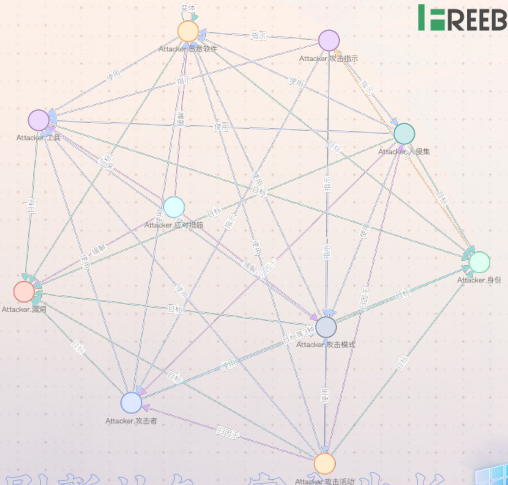

经典网络

## CVE漏洞命名实体识别

- WordEmbedding-BiLSTM-CRF
- Bert-NER
- Bert-BiLSTM-CRF-NER

# 技术 知识图谱

- 攻击者数字化
  - 身份
  - 工具
  - 漏洞
  - 模式
  - 资产
  - 恶意软件
  - ……
- 10个节点，39条边
- 利用图关联深度遍历和推理知识



# 结果

## 整体结果

攻击者数字化

- 定向攻击主体：数十个
- 真实身份：数百个
- 攻击组织：数十个
- 攻击者固定资产：数千个


数字化应用

- 落地应用场景6种
- 发现热点事件3起
- 支撑应急定位攻击者

# 结果

模型结果

机器智能

- 机器攻击分类模型
  - 误报率<0.3%
- 攻击同源聚类模型：
  - 1起热点事件
- 漏洞实体识别模型
  - 召回率提升50%+

知识图谱

- 10个节点，39条边
- 实体数数十万
- 关系数数百万

# 结果

## 应用场景

Top威胁发现

- 攻击活动：1起攻击者越权利用
- 热点攻击活动：1起聚集性通用漏洞利用

# 结果

## 应用场景

**安全产品新威胁对抗**

- 新型攻击模式挖掘
- 产品安全能力兜底

# 结果 应用场景

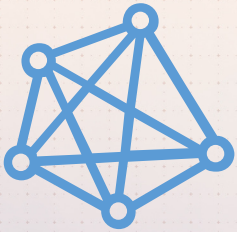

Log4j2 0day应急

- Log4j2 ioc：2k+个
- 失陷机器外连检测

# 展望

攻击者图谱

知识体对抗



防守方图谱


SPRING 春日版
CIS 2021
网络安全创新大会
Cyber Security Innovation Summit
THANKS
网安江湖
谁主沉浮
REEBUF