金融行业

12月报
2020 年

安全月报

政策解读 | 行业研究 | 漏洞聚焦 | 安全态势

绿盟科技金融事业部出品

政策解读

解读| GB/T39335-2020《信息安全技术 个人信息安全影响评估指南》

行业研究

透过隐私合规，看数据安全技术发展趋势

自动化入侵响应的理想与现实

特朗普竞选网站遭加密货币骗子黑客攻击

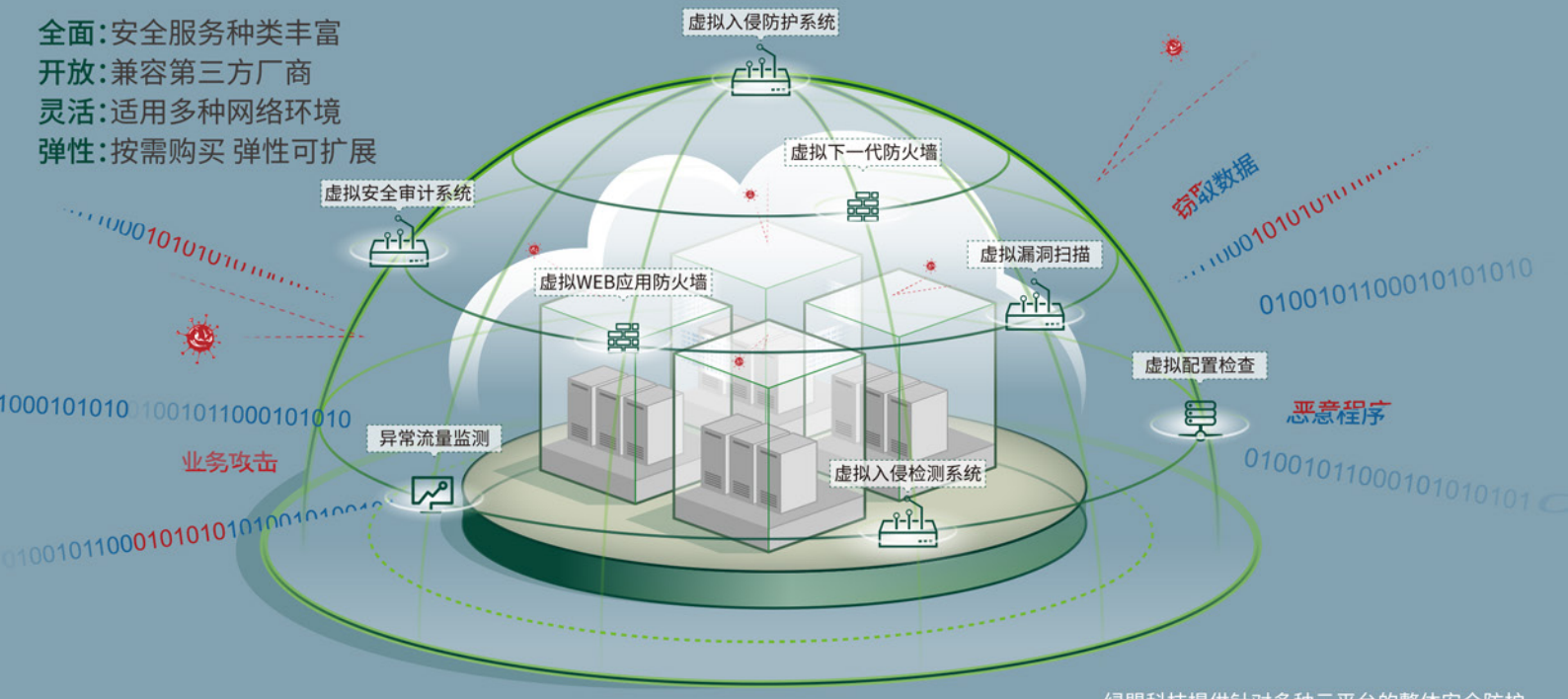
QBot 银行木马利用美国大选相关主题为诱饵，开展垃圾邮件活动

Akropolis 遭到闪电贷攻击损失 200 万美元 DAI 代币

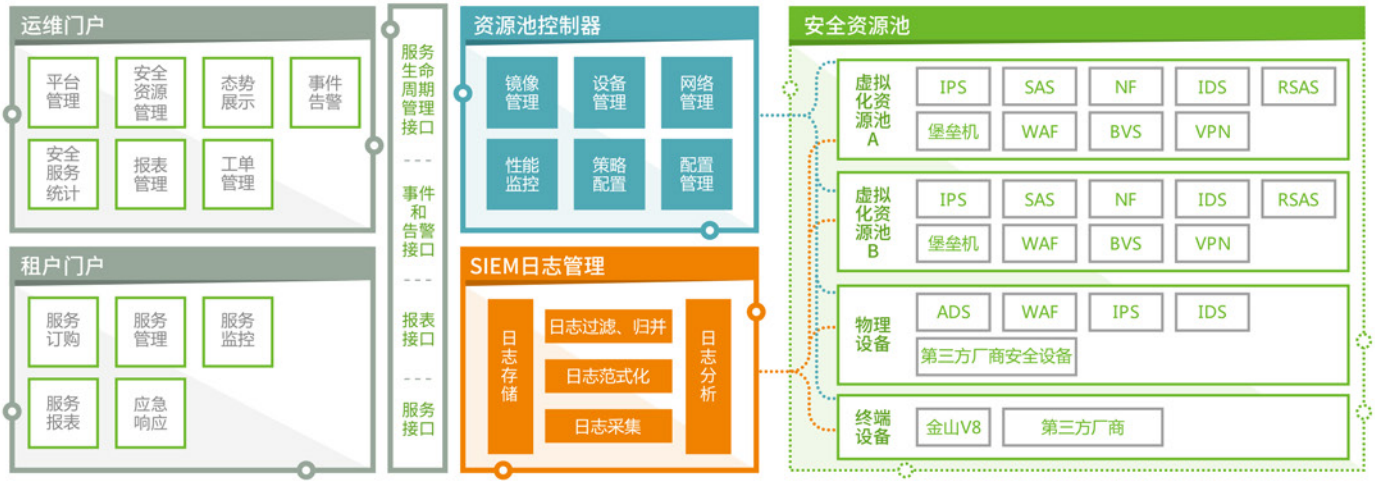
NSFOCUS

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。

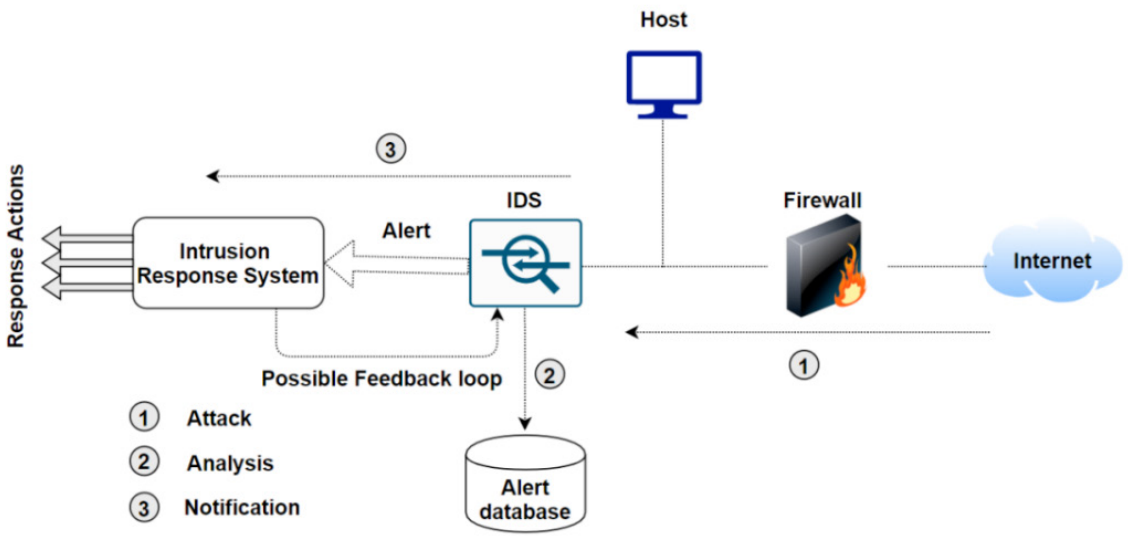
客户支持热线：400-818-6868

NSFOCUS绿盟科技

本|期|看|点

P4 解读 |GB/T39335-2020《信息安全技术 个人信息安全影响评估指南》

P23 自动化入侵响应的理想与现实



安全月报

2020年第12期

绿盟科技金融事业部

安全月报在线阅读

绿盟科技官方微信

目录 CONTENTS

政策解读

P04 解读 | GB/T39335-2020《信息安全技术 个人信息安全影响评估指南》

行业研究

P14 透过隐私合规，看数据安全技术发展趋势

P23 自动化入侵响应的理想与现实

P33 特朗普竞选网站遭加密货币骗子黑客攻击

P35 QBot 银行木马利用美国大选相关主题为诱饵，开展垃圾邮件活动

P37 警告！新的 Android 银行木马从 112 个金融 APP 中窃取数据

P39 Akropolis 遭到闪电贷攻击损失 200 万美元 DAI 代币

P41 加密货币交易所 Liquid 确认遭遇黑客攻击

漏洞聚焦

P44 Citrix SD-WAN 安全漏洞安全通告

P46 Drupal 任意 PHP 代码执行漏洞（CVE-2020-28949、28948）安全通告

P47 Drupal 远程代码执行漏洞 CVE-2020-13671 安全通告

P48 SaltStack 多个安全漏洞 CVE-2020-16846, CVE-2020-17490, CVE-2020-25592 安全通告

P50 【二次更新】Weblogic Console CVE-2020-14882 补丁绕过防护方案

P58 Windows Kernel cng.sys 权限提升 0-day 漏洞 CVE-2020-17087 安全通告

P59 Windows 网络文件系统漏洞（CVE-2020-17051、CVE-2020-17056）安全通告

P63 XStream 远程代码执行漏洞 CVE-2020-26217 安全通告

安全态势

P66 互联网安全威胁态势

NSFOCUS

政策解读

解读 | GB/T39335-2020《信息安全技术 个人信息安全影响评估指南》

绿盟科技　欧阳周婷

2020年11月19日，国家市场监督管理总局、国家标准化管理委员会发布的中华人民共和国国家标准公告（2020年第26号），GB/T39335-2020《信息安全技术 个人信息安全影响评估指南》国家标准正式发布，并将于2021年6月1日正式实施。本则指南历时3年终于发布，为公民个人信息再添一张保护伞。

1 背景介绍

1.1. 发布背景

随着大数据时代的到来，数据成为新的生产要素，是国家的基础性资源和战略性资源。美国，欧盟，日本等国家前后出台了有关数据保护与个人信息保护的法律法规标准，来保护本国的数据及个人信息安全。

在2016年4月19日召开的网络安全和信息化工作座谈会上，习近平总书记提出了“以人民为中心”的网信发展思想，并做出了“网络安全为人民、网络安全靠人民”的重要指示。2016年，《信息安全技术 个人信息安全规范》标准制定项目在全国信息安全标准化技术委员会立项，被列为重点标准项目，《个人信息安全规范》标准强调展开个人信息安全影响影响评估工作，旨在发现、处置和持续监控个人信息处理过程中的安全风险。个人信息安全影响评估与传统信息安全风险评估不同，其评估的风险是指对个人权益造成的损害，评估对象、评估方法均有所不同，国际上针对个人信息安全风险评估有大量专门的标准和指南，而我国尚无对个人信息主体权益影响进行评估的指导文件，制定该指南标准，将是推动个人信息保护工作深入落地，提升保护水平的有效途径。

1.2. 标准定位

2018年6月13日，全国信息安全标准化技术委员会发布国家标准《信息安全技术 个人信息安全影响评估指南》征求意见稿征求意见的通知。

2020年11月19日，国家市场监督管理总局、国家标准化管理委员会发布的中华人民共和国国家标准公告（2020年第26号）上，GB/T39335-2020《信息安全技术个人信息安全影响评估指南》国家标准正式发布。

《个人信息安全影响评估指南》（以下简称“《指南》”）是《个人信息保护法（草案）》和《个人信息保护规范》标准落地的重要抓手，是我国个人信息安全保护标准体系的关键环节。它规定了个人信息安全影响评估的基本概念、框架、方法和流程，并提出了特定场景下进行评估的具体方法。适用于各类组织自行开展个人信息安全影响评估工作。同时为国家主管部门、第三方测评机构等开展个人信息安全监管、检查、评估等工作提供的指导和依据。

1.3. 发展历程

个人信息安全政策及标准的发展历程如下所示：

1.4. 标准参考

《指南》参考了传统信息安全风险评估的方法，从资产、威胁、脆弱性三个角度进行分析，并结合个人信息处理行为对用户权益产生的影响，判断其对个人信息主体合法权益造成损害的各种风险，评估用于保护个人信息主体的各项措施有效性。同时，该标准还参考《ISO/IEC29134:2017隐私影响评估准则》中的隐私影响评估（PIA）的流程，通过借鉴国外立法和标准的研究，结合国内应用实践和标准编制组的科研成果，提出与国际标准接轨、适合我国国情，并具有一定创新性的“PIA”标准。为组织、监管部门、第三方测评机构等开展评估工作提供的指导和依据。

因此，《指南》既能够有效支撑我国《个人信息保护法（草案）》中的第五十四条要求，同时也能支撑实施《通用数据保护条例（GDPR）》下的数据保护影响评估（DPIA）要求。

2 内容解读

2.1 标准概述

《指南》由五个章节以及四份附录组成。其中第四章节“评估原理”和第五章“评估实施流程”作为主要章节，配合附录参考性材料，以“先原理后细节”的整体逻辑，明确指出了个人信息安全影响评估的基本原理、实施流程、评估细节，更加具象且专注于具体实操，对个人信息安全影响评估的工作落地起到了重要的指导意义。

2.2 内容简介

2.2.1评估原理

《指南》中第四章节“评估原理”，介绍了开展评估的价值、评估报告的用途、评估责任主体、评估基本原理和评估实施考虑的要素。

开展评估的价值主要从组织和组织第三方合作伙伴两个维度进行阐述。

- 针对组织，在个人信息处理前，协助组织识别风险，辅助其采取对应的安全控制措施，并基于评估工作，帮助企业员工熟悉个人信息安全风险，增强处置风险的能力；在开展个人信息处理过程中，持续修正安全控制措施有效性，确保风险可控，同时可作为证明组织个人信息保护与数据安全方面的合规证明；当发生个人安全事件时，可作为组

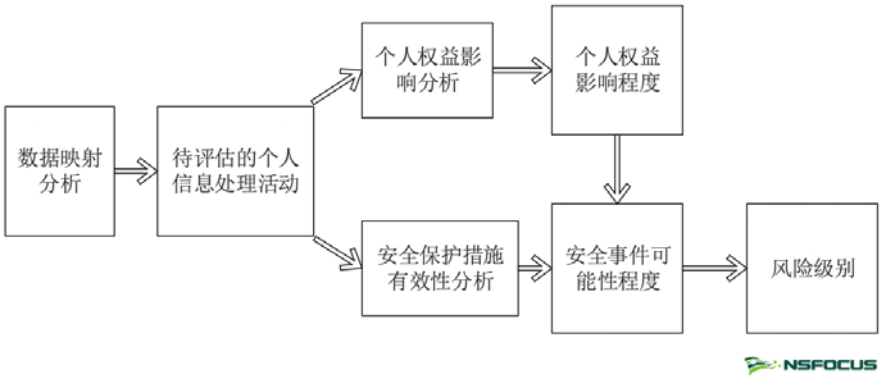
织已主动评估风险和采用保护措施的有效证明，减轻或免除组织相关责任和名誉损失。

- 针对组织第三方合作伙伴，在证明组织个人信息安全保护能力的同时，也可引导其采取适当安全管控措施。

在评估报告用途上，主要从个人信息主体、开展影响评估的组织、主管监管部门和组织第三方合作伙伴四个层面进行的阐述，具体如下图所示：

在评估责任主体上，由组织指定责任部门或责任人员（可选择自行开展或外聘独立第三方），但需要注意，该责任部门或人员需要具有独立性，不受被评估方影响。

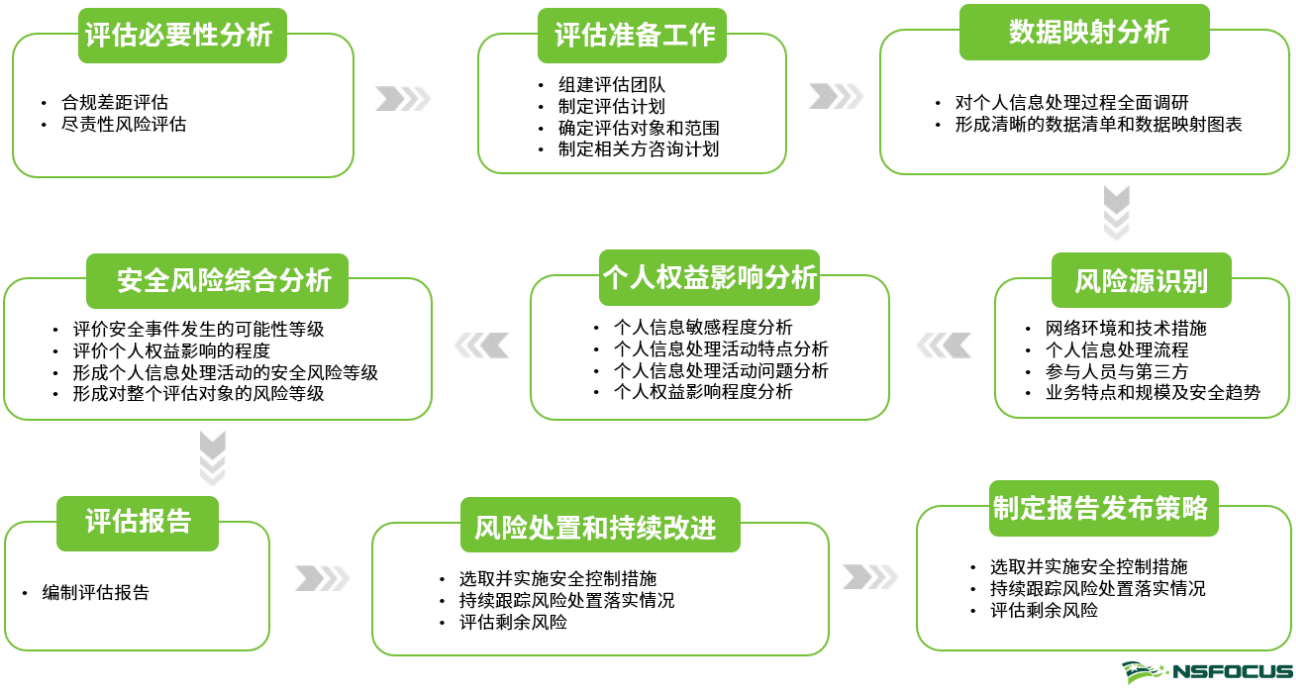
在评估原理上，从两方面对个人信息处理活动进行评估，一是个人权益影响，另一个是安全保护措施有效性，最终确定风险级别。



在评估实施考虑要素上，主要包含三方面：评估规模，取决于受到影响的个人信息主体范围、数量和受影响的程度；评估方法，提供了访谈、检查、测试三中基本评估方法；评估工作形式，可分为自评估和检查评估两种。

2.2.2评估实施流程

《指南》中第五章节“评估实施流程”，详细提供了组织进行个人信息安全影响评估的流程指引。评估实施流程可分为九步，具体如下图所示：



其中，主要内容如下：

- 评估必要性分析，可从合规差距分析（整体合规分析、局部合规分析、评估性合规要求分析）和尽责性风险评估两个维度开展。
- 开展评估准备工作，包括组建评估团队、制定评估计划、确定评估对象和范围（系统基本信息、系统设计信息、处理流程和程序信息）、制定相关方咨询计划。
- 数据映射分析，需要结合个人信息处理的具体场景，开展方式可参考附录C中表C.1《基于处理活动/场景/特性或组件的个人信息映射表》和C.2《个人信息生命周期安全管理》
- 风险源识别，针对个人信息安全事件，对要素进行了简化，归纳为网络环境和技术措施、个人信息处理流程、参与人员与第三方、业务特点和规模及安全趋势四个方面。具体评估可参考附录D.1《评估安全事件发生的可能性》
- 个人权益影响分析，是分析特定的个人信息处理活动是否会对个人信息

主体合法权益产生影响，以及可能产生何种影响，主要包括四个维度：限制个人自主决定权、引发差别性待遇、个人名誉受损或遭受精神压力、人身财产受损。具体评估可参考附录D.2《评估个人信息主体权益影响程度》

- 安全风险综合分析，具体过程和风险等级的判定可参考附录D中D.3《个人信息安全风险综合评估》。

2.3 关注重点

《指南》的发布为个人信息控制者提供了行之有效的方法去判断其个人信息处理活动的合法合规性，以及是否会对个人信息主体合法权益造成不利影响。对于一般企业来说，在个人信息安全保护工作的过程中，应当关注到以下内容：

2.3.1需开展个人信息安全影响评估的情况

《中华人民共和国个人信息保护法（草案）》第五十四条中指出：个人信息处理者应当对下列个人信息处理活动在事前进行风险评估，并对处理情况进行记录：

- 处理敏感个人信息；
- 利用个人信息进行自动化决策；
- 委托处理个人信息、向第三方提供个人信息、公开个人信息；
- 向境外提供个人信息；
- 其他对个人有重大影响的个人信息处理活动；

《GB/T 35273-2020 信息安全技术 个人信息安全规范》中对开展个人信息安全影响评估的场景进行了补充：

- 在产品或服务发布前，或业务功能发生重大变化时，应进行个人信息安全影响评估；
- 在法律法规有新的要求时，或在业务模式、信息系统、运行环境发生重大变更时，或者发生重大个人信息安全事件时，应进行个人信息安全影响评估。

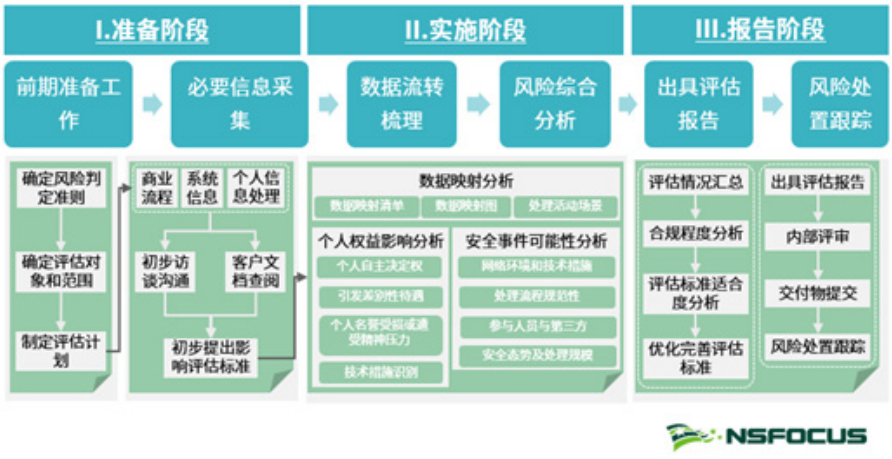
2.3.2可能对个人信息产生高风险的情况

为了让企业更好的发现个人信息安全风险，《指南》提供了常见的高风险个人信息处理活动与场景，企业存在下述个人信息处理活动时，应当对其特别关注。

3 绿盟科技个人信息安全影响评估服务方案

作为将 “巨人背后的专家，保障客户业务顺畅运行”列为使命的公司，为了有效保障客户的业务运行以及用户的个人信息安全，绿盟科技向全行业的客户提供专业高效的个人信息安全影响评估服务，全力保障企业个人信息处理业务的合法合规，规避对用户合法权益的损害，并保障用于个人信息保护的各项措施有效落实，帮助企业规避因侵害用户权益带来的合规风险、财务风险以及舆论风险。

3.1 服务方案实施流程



3.2 评估收益

个人信息安全影响评估可有效加强企业对个人信息主体权益的保护，能够对外展示企业在个人信息保护领域的努力，提升透明度，增进个人信息主体对企业的信任。

具体收益如下：

4 个人信息安全影响评估实践案例

基于对《指南》以及国际标准和最佳实践的深入理解，结合长久以来积累的风险评估经验，绿盟科技已为多家企业提供了成熟完善的个人信息安全影响评估服务，为帮助读者更好地理解个人信息安全影响评估的实施方法，下面是对某省烟草企业个人信息安全影响评估项目作为案例进行的分析。

- **企业特征：**业务设计明确、信息系统繁多、用户信息数量庞大、用户信息类别明确、可能导致重大个人权益影响。
- **评估对象：**出于对上述因素的考虑和对重点业务的分析，本次评估确定了多个信息系统作为评估对象，涉及个人信息的全生命周期行为，且覆盖了个人信息种类与数量最多的几个系统。
- **实践过程：**本次评估基于《指南》中的评估方法，结合企业架构特征与

项目团队经验，通过如下方法完成了个人信息安全影响评估工作，并出具了综合企业整体个人信息保护状况的个人信息安全影响评估报告。

◆ **评估结果：**本次评估发现安全保护措施落实不到位容易造成个人信息被泄露，以及引发零售户财产受损、歧视性待遇。下面选取两个典型的风险问题进行分析：

风险项	风险概述	风险处置建议
缺失数据安全管理细则，数据分类分级、数据权限管理、数据使用等流程管理混乱。	• 企业虽然遵照国家相关法律法规进行执行，已对数据资产进行核查形成了清单，但缺少制度化、规范化的管理细则，各层级在实际业务开展过程中，对数据的管理方式存在不统一，数据定义混乱、敏感程度认知存在分歧，导致数据分类分级存在遗漏和风险。且第三方人员可使用管理员权限进行系统维护、数据访问等操作。 • 数据安全管理细则未制定，易引发企业员工在数据收集、传输、存储、使用、交换、销毁等流程中的不合规操作，造成部分数据损失。且数据使用等权限未严格控制，易引发数据泄露风险，对零售户的个人权益造、对企业权益于声誉造成严重损失。	• 从企业整体考虑，并结合企业具体的业务活动，建立企业数据分类分级管理制度和具体细则，形成可落地执行的指导手册。 • 从管理和技术两个层面对不同类别和敏感程度的个人信息，实施相应的安全策略和保障措施，做到事前防御、事中防护、事后处置。 • 遵循PDCA原则，持续对数据保护策略进行动态维护，确保对应数据以适当的投入保持合适的控制水平。
数据全生命周期落地管控缺失安全管控要求。	• 企业对数据全生命周期的管控执行过程中，缺乏安全管控要求，大部分还停留在以业务为主导因素，如未经安全审核的临时敏感信息操作、缺失临时操作后的安全审计工作、未对服务到期的个人信息进行删除或去标识化处理（仅将用户状态从有效标记为无效）等。 • 缺失安全管控的数据管理，易造成数据管理过程中的数据损失与信息泄露风险，对零售户的个人权益造成较大影响，也会对企业名誉造成严重损失和经济损失。	• 严格落实数据全生命周期各项管控要求，做到数据行为可见、可控、可管。 • 定期开展数据风险评估，及时发现风险，并及时进行整改。 • 建立动态管控机制，发生安全事件后立即响应，及时上报，迅速处理，降低损失。 • 开展安全教育培训工作，提高企业员工的安全意识和正确的工作观念，有效减少安全事件的发生。

NSFOCUS

行业研究

透过隐私合规，看数据安全技术发展趋势

天枢实验室　陈磊

摘要

近年来，全球掀起个人信息与隐私的立法热潮。欧盟2018实施GDPR，美国2020年实施CCPA，两部法规均对企业处理用户的数据提出更严、更具体的约束和要求；最近十月份，我国对外公布《个人信息保护法（草案）》，它全面和具体地规定了企业保护个人信息安全的各项义务,同时指出违反法规最高可面临5000万或一年度营业额5%的巨额罚款。

据Gartner预测，到2023年年底，全球超过80%的企业将面临至少一项隐私数据保护的法规（跨国企业面临多个国家或地区的多项隐私法规）。在法规监管不断强化的背景下，企业不得不重新审视数据安全与合规性的重要性与急迫性。与此同时，数据安全技术近年来发展十分迅速，创新技术不断涌现。本文将从国内外隐私合规视角切入，对数据安全技术进行梳理和总结，并对国内外数据安全技术发展趋势进行洞察和分析。

第一章　监管不断强化的国内外隐私法规

2018年 5月25日，欧盟正式实施《通用数据保护条例》（General Data Protection Regulation，GDPR）[1]，取代了1995年起施行的《数据保护指令》。GDPR不仅保护欧盟境内的个人数据，以及境外的欧盟公民的个人数据（域外管辖权）。GDPR赋予数据主体（用户）更多的数据控制权：不仅包括原有法规的知情权、访问权、修改权等，同时增加“被遗忘权”和“可携带权”两项“特权”。被遗忘权，在一些注销账户、或者超过时间期限等场景中，用户可以行使该项权利——数据控制者（企业）收到权利请求后，允许删除与自己相关的个人

数据，同时需要通知合作的第三方也删除相关的个人数据；可携带权，用户可以便携地将其个人数据从一个数据控制者处转移至另一个数据控制者处，数据控制者需要配合完成该过程。同时，GDPR规定企业保护数据需采取假名化、加密以及其他技术措施，数据泄露采取快速响应机制等等。此外，违法的代价是高昂的——最高罚款额度在2000万欧元或公司全球营业额的4%。从2018年执法到现在，多数成员国已经陆续开出多张的罚单。非常具代表性的一家大型国际互联网公司——Google在隐私保护方面已经做了不少工作，然而Google却陆续被欧盟的两个国家罚款：2019年1月份被法国处罚5000万欧元，原因是执法方认为Google产品的隐私条款未充分体现GDPR公开透明和清晰原则；2020年3月被瑞典处罚700万欧元，原因是Google未能充分履行GDPR赋予用户的数据“遗忘权”。

受GDPR立法的影响，全球其他国家也陆续推出了相关的隐私法规。具有代表性的是美国2018年6月通过的《加州消费者隐私法案》（California ConsumerPrivacy Act，CCPA），由于影响涉及大部分知名IT科技公司，如惠普、Oracle、Apple、Google和Facebook等，该方案从立法到颁布备受各界人士的关注。该法规同样赋予了消费者多种数据权利，同时对企业提出更严的标准与要求。另外，巴西于2019年7月通过《通用数据保护法》（LGPD）的最终版本；印度在2018年12月公布修改后的《2019年个人数据保护法（草案）》（Personal DataProtection Bill, 2019）；泰国于2020年5月正式实施《个人数据保护法》（Personal Data ProtectionAct）等。

2020年10月21日，我国《个人信息保护法（草案）》在人大网正式对外公布[2]。作为一部全面保护个人信息安全的综合性法律，具有重要的意义。该法律保护我国境内公民的各项个人信息权益，同时赋予个人信息主体各项数据权利，包括知情权、决定权、查询权、更正权、删除权等；同时明确了个人信息处理者（企业）的合规管理和保障个人信息安全等义务，并指出保障个人信息安全采取分级分类、加密、去标识化等措施。此外，对违法的行为提出更高的处罚力度，违反法规最高面临5000万元人民币或一年度营业额5%的巨额罚款，同时可以责令暂停相关业务、停业整顿、吊销营业许可或营业执照等严厉的行政处罚。这些处罚给企业的个人信息违规违法行为形成强大的威慑力。值得关注的是，在该草案公布临近几天，金融领域执法重拳出击：央行对3家银行的6家分支机构由于侵害消费者个人信息等违规行为开出百万、千万级大额罚单，并对相关责任人予以警告并处以罚款[3]。可见，企业应足够重视个人信息安全与数据隐私合规性问题，并落实相关举措。

从对企业的影响来看，对欧盟GDPR和国内的《个人信息保护法（草案）》以下的一些合规性热点进行解读：

◆ 个人数据/个人信息的识别与分类

GDPR保护的数据对象是“个人数据”。其定义是“关于一个已识别或者可能识别的自然人（即数据主体）的任何信息”，“个人数据”范畴边界十分宽泛，涵盖信息十分丰富，不仅包括传统意义的姓名、年龄、性别这些基本的个人信息，还包括一些特殊的数据也被归并为“个人数据”，比如生物识别数据——指纹、虹膜、DNA数据等；再比如IP地址码, MAC地址码，Cookie信息等，这些信息以往被认为是网络设备信息或网络行为信息，GDPR将其归类到“个人数据”。《个人信息保护法（草案）》的“个人信息”，虽然与GDPR的“个人数据”叫法不同，但实际上概念趋向一致，界定标准也几乎完全类似——“个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息”，同样采取“识别说”为基础，拓宽了个人信息的范畴。企业为了满足合规，必须拥有强大的敏感数据识别能力，能发现各种个人相关的信息以及敏感数据子类别，同样具有分类能力，比如对个人信息主体按照国家归属地进行分类，按照不同儿童和成年人的年龄范围进行分类，以及敏感度分类等。

◆ 个人数据/个人信息保护的技术措施

GDPR明确指出保护过程可采取加密或假名化两种措施：加密可保障数据存储和传输过程的安全性，降低数据被非法窃取和泄露的风险；而假名化是GDPR推荐一种“无损的”数据脱敏方式，它对个人数据的标识符信息（比如姓名、身份证号）通过哈希等手段重新命名，同时将真实的标识符-“重命名”映射表与假名化后的个人数据分开存储，以降低隐私泄露风险，同时保证个人数据的完整性。《个人信息保护法（草案）》明确指出可应用加密或去标识化安全技术措施，其中去标识化相比GDPR假名化更为宽泛，去标识化在企业通常称为“数据脱敏”，不仅包括假名化、还包括数据屏蔽、数据泛化、量化、置换等处理方式。这些意味着企业在存储、处理这些个人数据，需采取数据层面的保护措施进行安全防护。

◆ 数据权利请求与响应机制

GDPR赋予用户个人数据的知情权、访问权、修改权、遗忘权等各项数据权利，相应地，企业必须响应用户的数据权利请求，比如用户行使“遗忘权”时，企业必须提供删除数据的界面与入口，并执行相关处理操作与流程，以及对用户输出响应报告。且GDPR明确规定企业处理一般请求的响应时间是一个月，复杂

请求的响应时间可延长至两个月。《个人信息保护法（草案）》首次全面赋予个人信息主体各项数据权利，包括知情权、决定权、查询权、更正权、删除权等，同时明确指出企业应当建立个人行使权力的申请受理和处理机制。对于响应时间，该草案未明确指出，但《个人信息安全规范》（GB/T 35273-2020）提出响应的时间是30天内（差不多是1个月）。这些促使企业必须建立个人信息请求运营机制，并需要使用流程自动化处理方式。

第二章 合规驱动下的数据安全技术盘点

Gartner今年7月份将数据安全（Data Security）与隐私（Privacy）作为安全的两个细分领域，分别发布了2020年数据安全成熟度曲线[5]、2020年隐私成熟度曲线[6]，后者与隐私合规性紧密相关。实际上，隐私包含数据安全领域大部分的技术栈，同时也包含新型技术，比如主体权利请求（Subject RightsRequest, SRR）、同意与偏好管理（Consent andPreference Management, CPM）等（一般地，国内习惯将隐私并入到数据安全的范畴，将相关技术都统称数据安全技术，本文沿用这种叫法）。

Gartner发布的2020年隐私成熟度曲线，涵盖了35种数据安全相关技术，种类丰富且繁杂，分别处在创新触发期、期望顶峰期、幻想破灭期、稳步爬升期和生产成熟期五个阶段。其中超过70%技术处在稳步爬升期，说明该领域创新技术活跃，有巨大的发展空间，具体如表1所示。

从作用和应用场景角度看，笔者认为35种数据安全技术可分为五大类：

◆ 数据安全治理相关

包含多种数据技术组合，以及融合非技术的组织管理措施。比如数据安全治理（Data SecurityGovernance，DSG）、隐私影响评估（Privacy Impact Assessment, PIA）、数据泄露响应、数字道德、隐私设计（Privacy by design, PbD）和IT风险管理方案。

◆ 敏感数据全生命周期的安全防护

包括数据分类、文件分析（针对非结构化敏感数据的识别）、动态脱敏（DDM）、保留格式加密（FPE）和数据销毁（Data sanitization）。

◆ 用户隐私权响应与评估合规

包括主体权利请求（SRR）、同意与偏好管理（CPM），可以自动化处理

和响应用户提出的数据访问权和删除权等各项权利，以及隐私设计（Privacy by design, PbD），用于在产品设计时考虑隐私合规与可用性问题等。

◆ 隐私增强计算类技术

包括差分隐私（DP）、安全多方计算（SMPC）、同态加密（HE）、零知识证明和机密计算（包括TEE）等技术。

◆ 其他

包括重点领域的数据安全技术，比如移动终端威胁防御、云环境、5G、区块链的敏感数据保护。

表1 Gartner 2020年隐私成熟度曲线涵盖的相关技术

技术成熟度	数据安全相关技术
创新触发期 (Innovation Trigger)	机密计算、数据安全治理（DSG）、同态加密（HE）、差分隐私（DP）、主体权利请求（SRR）、零知识证明（ZKP）、5G安全、合成数据、区块链的数据安全
期望顶峰期 (Peak of Inflated Expectations)	数据泄露响应、安全多方计算（SMPC）、同意与偏好管理（CPM）、去中心化实体、数字道德、文件分析、隐私影响评估（PIA）、数据分类
幻想破灭期 (Trough of Disillusionment)	保留格式加密（FPE）、人格化、隐私设计（PbD）、PHI个人医疗隐私同意管理、移动终端威胁防御、云数据保护网关、隐私管理工具
稳步爬升期 (Slope of Enlightenment)	数据销毁（Data sanitization）、安全即时通讯、电子取证软件、IT风险管理方案、云访问安全代理（CASB）、动态脱敏（DDM）、云应用程序发现
生产成熟期 (Plateau of Productivity)	数据库审计与防护（DAP）、云安全评估、数据库加密

第三章 合规视角下的数据安全发展趋势观察

在隐私法规的强有力推动下，国内外数据安全相关技术和产品得到快速发展，逐步形成以“合规遵循”为主的安全细分领域。据2019年11月Gartner的一份预测报告指出，预测在2023年之前全球80%以上的企业将面临至少一项以隐私

为重点的数据安全保护规定，并且在合规上的投入将突破80亿美元。由此可见，数据安全合规未来仍然有广阔的市场应用前景。下面对前文提到的数据技术的发展趋势分别进行分析。

观察1：欧美GDPR /CCPA驱动，用户数据权利响应自动化等相关技术发展迅速

全球一些隐私法规赋予数据主体（用户）自由访问、修改和删除个人数据等权利，相应地，要求企业必须在规定的时间内对用户提出的请求进行处理和响应，比如GDPR要求的时间一般为1个月，而CCPA是45天。快速响应数据主体权利请求（Subject RightsRequest, SRR）对多数企业是一项极大的挑战。据调查，约有三分之二组织人工处理单个SRR需要两周以上的时间，且平均消耗成本高达1400美元。那么，在合法时间内响应高并发的SRR，传统手工操作是一项困难任务。RSAC 2020创新沙盒比赛中，Securiti.ai一举夺得冠军，它主推自动化的SRR、CPM等用户数据权利响应类产品；另外RSAC2018的创新沙盒的冠军——BigID，它同样聚焦在该类隐私合规产品中；另一家非常著名的创业公司OneTrust有一块很大的业务也是隐私合规性产品，与Securiti.ai几乎重合。这三家初创安全公司融资累计规模超过6000万美元。可以侧面可以反映出，用户数据权利响应产品在国外十分火热，已经发展成为一块稳定的安全市场。

这些产品主要使用了流程自动化以及多种人工智能技术：其中流程自动化可帮助企业的数据安全运营团队从繁琐重复的手工处理“请求-响应”升级为程序的自动化处理，一方面可降低运营成本，另一方面降低由于响应时间延误带来的违规风险；而人工智能技术方面，使用自然语言处理技术（NLP）识别非结构化的敏感数据，使用知识图谱技术关联数据主体所有相关信息，同时使用对话机器人技术方便自动化处理一些提问需求。具体参考《Securiti.ai—解决隐私合规痛点的一站式自动化方案》。

我国《个人信息保护法（草案）》赋予个人包括知情权、决定权、查询权、更正权、删除权等，同时指出“个人信息处理者应当建立个人行使权利的申请受理和处理机制”，但尚未规定具体的时间，而在国标《个人信息安全规范》（GB/T 35273-2020）提出响应的时间是30天内。随着法规的完善，可预计国内SRR、CPM隐私合规技术与市场正逐步形成。

代表公司：Securiti.ai、BigID、OneTrust

观察2：合规基础产品——敏感数据识别、数据脱敏市场日趋成熟

无论是欧盟GDPR、美国CCPA，还是我国的《个人信息保护法（草案）》，均明确表示保护的数据对象是个人数据（或称为个人信息），企业必须履行该类数据的安全保

护义务。为了遵循合规，企业第一步是需要识别出存储和流动的各类敏感数据，不仅包括个人基本信息，包括用户姓名、身份证号、手机号等信息，还包括一些个人敏感数据，比如医疗隐私、金融隐私和网络行为的隐私（比如Cookie信息）等。这些敏感数据第一步需要识别。目前已经发展多种敏感数据识别方法：①基于正则的识别；②基于关键词库的识别；③基于数据相似度的识别；④基于机器学习的识别。目前前两种方式在工业界发展较为成熟，一般建立相对全面的规则库或字典。后两种方式通常应用前两种无法解决的敏感数据场景，比如很难直接定义规则或关键词。第③方法首先从参考数据提取一些特征，然后将其他数据使用同样处理方法后，进行相似度比较，超过一定阈值当作同一类数据；第④方法利用机器学习的强大学习与预测能力，收集足够的样本并进行类别标注，进行模型训练，完成后部署模型自动化识别新数据的类别。识别完成后，为降低敏感数据在二次使用和流通过程（非生产环境，比如数据分析、测试等）的法规风险，大量的数据脱敏需求应运而生。数据脱敏按处理结果是否可还原可分为可逆脱敏和不可逆脱敏技术。可逆脱敏可以理解为企业通过建立一些敏感词的映射表替换为其他非敏感数据，通过反向映射表可将脱敏数据恢复为原始数据。不可逆脱敏技术包含的策略丰富灵活，包括取整、量化、泛化、屏蔽、截断、散列和加噪等。按照使用场景，可将脱敏分为静态脱敏 (StaticData Masking, SDM)、动态脱敏 (Dynamic Data Masking, DDM)。静态脱敏一般用于非生产环境中（测试、统计分析等），动态脱敏一般用于生产环境中。目前静态脱敏技术已经发展较为成熟，而动态脱敏近年来也相关产品落地。

作为两类基础性的合规产品——敏感数据识别和数据脱敏，国内外市场日趋成熟。国内外多家安全厂商在此有所布局，如大型IT公司Microsoft、IBM推出了敏感数据识别和数据脱敏产品，初创公司Securiti.ai、BigID推出了大规模敏感数据的识别产品，并通过AI驱动实现半自动化或自动化扫描和发现。国内绿盟科技推出了IDR产品，可应用在传统数据库和大数据平台的敏感数据发现与分类分级场景中，安华金和推出数据库脱敏相关产品，可应用结构化数据的脱敏应用中。

代表公司：Microsoft、IBM、Securiti.ai、BigID、安华金和、绿盟科技

观察3：合规与数据利用业务场景紧密结合，隐私增强计算技术与应用不断涌现

大数据时代，敏感数据的高频使用和流通，数据既要安全也要求业务利用，这给传统以加密为核心的数据安全技术带来了巨大的挑战。为了满足合规

和数据利用的双重需求，促进一批与业务场景紧密结合的新型数据安全技术的产生和发展，包括同态加密、安全多方计算、联邦学习、差分隐私等。由于这些技术不仅可保证原始数据不被泄露（不可见），而且在具体某些业务场景（如聚合、集合运算以及AI建模）保证数据的可用性，工业界习惯将它们形象称为“可用不可见”技术。Gartner将这些技术统称为隐私增强计算（Privacy EnhancedComputation）技术，并将其与随处运营、人工智能工程化等作为2021年六大重要战略科技趋势。国内外均在此领域有布局：Google的联邦学习及在Android端应用；Apple在iPhone手机的数据采集中使用了本地化差分隐私技术；RSAC 2018创新沙盒亚军——Duality公司，在定制服务器实现商业化的同态加密方案；阿里主打安全多方计算技术以及平台；百度、腾讯和微众银行等分别推出联邦学习框架并应用在了隐私数据联合建模场景。

代表公司：Google、Apple、Duality、阿里、腾讯、百度、微众银行

观察4：数据安全治理框架与技术方案百家争鸣

传统一两种数据安全技术和措施，无法解决应对内部和外部数据安全威胁，以及合规性和业务带来的挑战。为了应对挑战，Gartner在2017数据安全与风险管理峰会上提出安全治理（DSG）的概念与方法论。数据安全治理——以“数据安全”为核心的综合治理体系，它涉及法规、场景、技术、产品、组织管理以及各类标准流程、策略配置等。微软也提出了针对隐私、保密和合规性的数据治理框架 (Data Governance for Privacy Confidentiality and Compliance, DGPC)，分别从人员、流程和技术这三个角度出发。IBM提出的数据安全和隐私解决方案采用敏感数据发现与分类、评估漏洞、监控与审计等分层方法实现数据安全性。在国内，多家企业提出各自的数据安全治理方法论或数据安全解决方案。比如，阿里提出了DSMM模型，它以数据为中心，数据生命周期为主线，针对数据生命周期各阶段建立全面的数据保护，并对能力成熟度进行定级；安华金和提出了数据安全治理通用框架，框架从数据安全治理机制、数据安全生命周期管理、数据安全技术部署开展数据安全治理与建设；绿盟在Gartner数据治理框架基础上，结合客户的数据安全防护需求，对实际情况进行研究和实践，也建立一套完整科学的方法体系——数据安全解决方案。该体系分为五个基本治理步骤——“知”、“识”、“控”、“察”、“行”，五个步骤分别采用不同的数据安全技术与管理措施具体参考《拨开云雾见天日——数据安全治理体系》

代表公司：Microsoft、IBM、阿里、安华金和、绿盟科技

第四章 小结

在全球相关法规的推动下，如欧盟GDPR，美国CCPA，以及我国最近发布的《个人信息保护法（草案）》，隐私合规逐步成为企业数据安全建设与治理重要驱动力。在法规监管不断强化的背景下，企业必须主动进行合规性建设，结合自身业务场景与风险，实施体系化的数据治理与建设，在数据的全生命周期结合安全需求实施一项或者多项技术与措施以应对数据安全风险。在一些新的数据安全场景，尤其是数敏感数据的安全共享计算，该领域创新技术不断，包括安全多方计算、联邦学习、差分隐私，唯有通过跟踪和探索这些新技术的发展，才能更好应对新场景中带来的新的数据安全问题、新的安全风险以及合规性挑战。

参考资料：

1.General DataProtection Regulation (GDPR), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC.

2. 《个人信息保护法（草案）》，http://www.npc.gov.cn/

3. 金融信息安全成监管重点央行开千万元级罚单护航，https://finance.sina.com.cn/stock/jhzx/2020-10-30/doc-iiznezxr8873053.shtml

4. 绿盟科技，《数据安全白皮书2.0》

5. Gartner, HypeCycle for Privacy, 2020

6. Gartner, HypeCycle for Data Security, 2020

关于天枢实验室

天枢实验室聚焦安全数据、AI攻防等方面研究，以期在“数据智能”领域获得突破。

自动化入侵响应的理想与现实

天枢实验室　童明凯

引言

面对各种各样的网络攻击，在防御上实现自动化入侵响应是企业安全自始至终的诉求，实际上，各种防护类、日志审计类等安全产品，最终目标还是为了对网络攻击做出合理的响应。在当今大数据、人工智能等概念的驱动下，网络安全有了新的机遇，这些智能化技术能否解决安全运营中最后一公里的问题呢？本文总结自动化入侵响应的需求和现实，给出见解。

第一章 背景

对于网络攻击，从防御角度来看可以大体分为检测和响应两大步，对应的系统称之为入侵检测系统（IDS，intrusion detection system）和入侵响应系统（IRS，intrusion response system），IDS负责检测网络中的恶意活动，IRS负责选择合适的应对措施处置恶意活动从而保护目标网络，不过由于IRS至今为止并没有一个成熟的商业化工具，该概念和相关研究仍然停留在学术圈内。早期的网络中，入侵事件并不频繁，防御系统的设计中心偏向系统的监测和分析模块，而把响应的任务留给用户，这种设计在现代复杂的网络环境中已逐渐凸显其弊端。

现代企业在部署核心安全产品后便对网络环境的安全性有了基本的感知能力，此后便会进入持续的安全运营阶段，安全分析人员会分析设备产生的告警，对告警进行研判，根据先验知识判断当前攻击的状态，并且结合企业实际的业务对攻击采取一定的缓解措施，如：封堵攻击IP，关闭对应端口，对主机打补丁等等，如果是高级攻击、复杂攻击，往往还需要部署蜜罐，捕获并分析此类攻击行为。

为了处理海量设备告警，现代企业往往会成立安全运营中心（SOC），运营人员会根据经验选择自认为可疑的告警进行研判，而该安全运营过程往往会遇到两方面压力：一方面，分析人员依靠人工处理，只能处理海量告警中的少量告警，引发“告警疲劳”问题，会遗失大量关键告警，另一方面，由于分析人员在安全知识、业务理解等方面的差异，做出的决策可能会出现失误。实际上，一个合理决策行为的制定往往需要考虑大量因素，如：攻击严重程度、攻击影响范围、网络拓扑、业务压力，甚至还需要对攻击做出一定预测等等，做出合理的决策往往不大容易，该目标不仅要求安全分析人员

对安全有比较深入的了解，还要对企业的需求和抗风险能力有一定的认知。总结来说，一方面，人力面对大量制约条件往往难以做出合理决策，另一方面，企业每天有大量的安全事件需要决策，需要大量人力投入，这种情况下，自动化或半自动化的入侵响应技术便成了企业共同的呼声。需要指出的是，这里的自动化入侵响应技术应该是从输入到输出的全流程自动化，不仅仅包括设备最后执行时的自动化，更重要的是核心决策部分，根据各种输入和限制条件给出合理动作的一种方法。

实际上，入侵响应系统在网络安全发展的早期就被提出，由于诸多原因，研究进展和工业实际部署都比较缓慢，本文将深入分析自动化入侵响应技术的本质，探索其技术发展方向。本文第二部分会对IRS系统做简单介绍，第三部分介绍IRS系统中核心的策略选择算法，第四部分对该方向做整体分析，第五部分进行总结。

第二章 入侵响应系统

IDS能够识别攻击，产生告警，但是缺乏对入侵的响应机制，IRS基于IDS的告警对入侵行为做出响应，两者的关系如图1所示，IDS、IRS均旁路部署于企业内网中，IDS会对链路上的流量进行分析，产生告警，IRS需要根据这些告警和一些其他因素，对攻击做出响应，执行的结果可能还会有一个反馈过程，以便对整体系统进行优化。

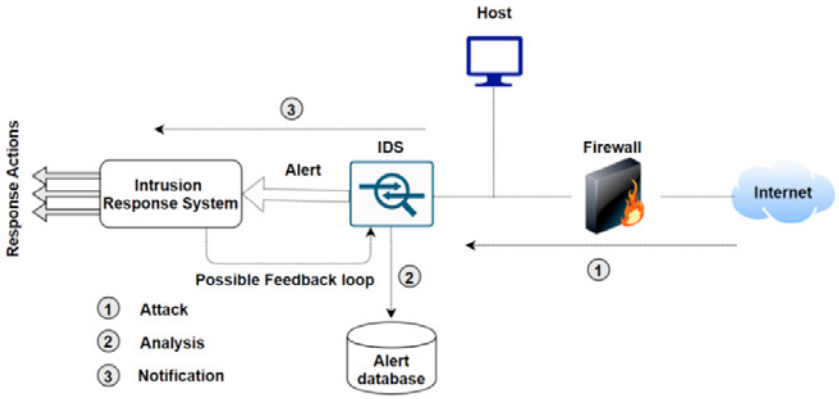


图1 IRS网络拓扑图

本部分总结IRS的体系结构、目标、分类、输入输出和核心问题。

2.1 入侵响应系统体系结构

入侵响应系统的总体结构如图2所示，当检测设备检测到入侵事件并触发告警给响应决策模块后，响应决策模块根据告警信息和响应决策知识库进行响应决策，最终决策出针对当前入侵行为的响应措施和响应时间策略发送给响应执行模块，响应执行模块从相应工具库中调用响应工具进行具体措施的执行。显然，在整个过程中，响应决策模块是最核心的部分，响应的正确性、及时性与之密切相关。

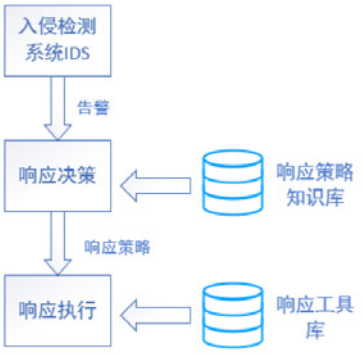


图2 入侵响应系统体系结构

2.2 入侵响应系统的目标

理想情况下，自动化入侵响应系统应该满足如下目标[4]：1. 快速找到止损/减轻方案（或者是临时应对措施）将事件影响尽可能控制在最小范围内；2. 修复感染设备；3. 配置相关策略防止未来相似的攻击。

在具体实施上，自动化入侵响应系统的响应策略应该满足以下要求：

- 合理性。响应决策不仅需要评估安全事件及相关影响因素，还要考虑代价、资源约束、技术可行性、响应效果等各种因素，力求以最小的代价达到尽可能高的安全级别保护，能够有效阻止入侵行为，降低系统损失。
- 自适应性。由于入侵行为的不断变化以及系统环境的不确定因素，仅仅通过简单的静态决策表来响应是不够的，应该根据响应的效果评估，动态调整响应策略。
- 及时性。现代黑客逐渐使用自动化攻击的手段，对响应的速度提出了挑战。
- 安全性。入侵响应系统应保证自身的安全性，不被攻击者控制。

2.3 入侵响应系统的分类

如图3所示，入侵响应系统从大类上分为3种：基于通知、基于人工响应、基于自动化响应。其中，基于通知的入侵响应系统就是提供各种形式的入侵信息给相应的人员，基本上就是目前IDS产品的功能；基于人工响应的入侵响应系统允许运维人员对从一些预定义的响应操作中选择特定动作对入侵事件做响应；基于自动化响应的入侵响应系统是安全运维人员的终极追求，即对入侵事件提供及时的响应能力。

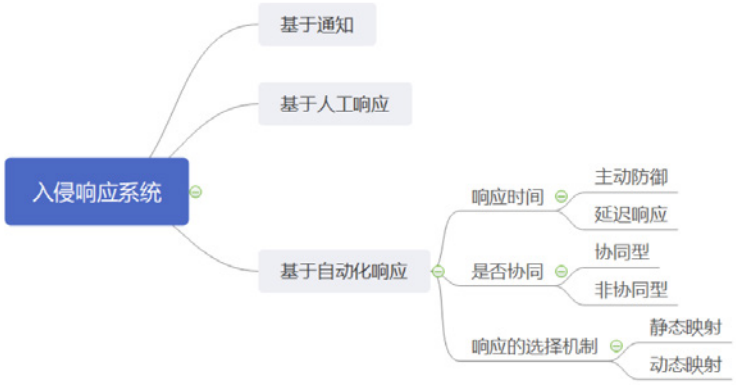


图3 入侵响应系统分类[2]

在基于自动化响应的IRS系统中，响应的选择机制是研究的重点内容，具体来说：

静态策略型IRS系统。该类型的IRS系统建立告警与响应之间的一一映射关系，通过枚举各种可能的告警种类，安全专家人工制定响应策略库，当告警发生时，IRS系统通过查表可以得到相应的响应策略。目前绝大多数的IRS为静态映射型，2001年，Carver调研了当时存在的56种入侵检测系统，其中有18种系统具有自动入侵响应机制，14种系统采用了静态映射模型进行响应措施的决策[7]。静态策略模型只考虑攻击类型采取动作，并没有对IDS的误报率和漏报率、攻击的严重程度、目标系统的脆弱性等因素做考量，因此该模型缺乏可行性和准确性。

动态策略型IRS系统。该类型的IRS系统要根据观察到的告警对正在发生的攻击活动进行推理，从而采取合适的响应，核心问题在于其动态决策能力。第一步需要考虑网络的拓扑、检测器的部署位置判定被攻击的目标，第二步需要根据发生攻击可能性、攻击的严重性、被攻击机器的实际情况等因素进行响应，最后需要评估响应的有效性以确定是否需要采取后续操作。实际上，大量因素会影响到该决策过程，如动作的执行成本、动作带来的负面作用等等。该方向也是目前IRS系统研究的主流方向，也是最有可能实现前一小节所说的目标和要求的方向。

2.4 入侵响应系统的输入输出

IRS的输出很好理解，就是针对各种攻击对应的处置动作，这些动作不仅仅是传统WAF、IPS等网络设备的IP封堵功能，还有针对资产的行为、不同设备之间的联动行为等等，如：检测到恶意域名访问时，需要通过与DNS系统对接进行封堵；当遇到网络入侵事件时，可以通过修改路由器的路由策略进行封堵、也可以联动防火墙、交换机配置ACL策略进行封堵、甚至可以通过TCP RST、SDN流表等方式实现精准阻断；对于某些失陷的主机需要进行隔离操作等等。我们依据NIST中对应急响应生命周期的定义[8]（图4），将各种处置动作分为隔离/清除类和加固类，分别对应NIST应急响应框架中的缓解模块和根除模块，缓解和根除是依次进行的。

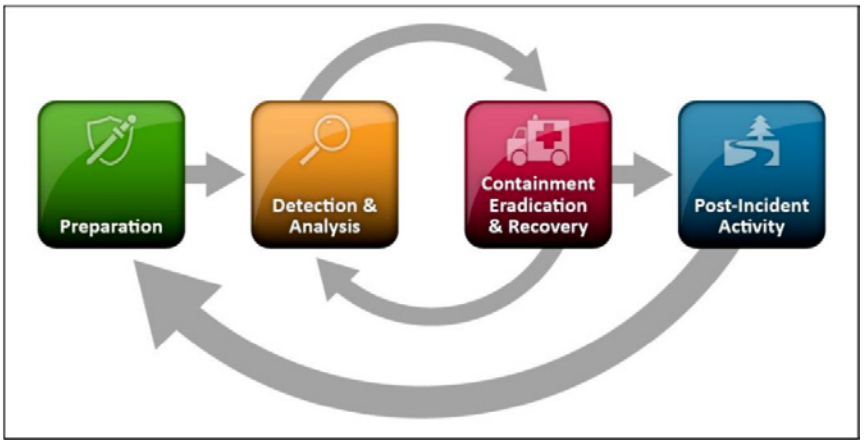


图4 应急响应生命周期

本部分我们尽可能多的收集整理安全设备的可以执行的防护动作，如表1所示，我们将IRS系统可以执行的动作分为加固类和隔离/清除类两大类，其中加固类的动作分为边界加固、Web加固、终端加固3种，需要指出的是，该分类是根据实际经验来得出的，我们仅采用在实际运营过程中会使用到的、便于部署实施的动作，很多类型的动作没有归入其中，如MITRE Shield中涉及到的各种针对ATT&CK的响应动作，Carver所提出基于追踪攻击、分析攻击、屏蔽攻击、最大化系统机密性、最大化数据完整性、最小化资源成本、恢复系统和维持服务等8个响应目的动作[7]，显然目前这些动作的都只是被动防御，

只涉及到事故缓解、系统加固类型的操作，但目前仅考虑这些动作的选择就需要大量的人力投入，有限集合内做到合理动作选择已属不易。

边界加固	Web加固	终端加固	事故隔离/清除
访问控制	字段过滤	补丁升级，病毒查杀	账户封禁
URL封堵 会话封堵 IP封堵 域名封堵 ACL规则	禁用未授权对象访问 禁止重定向	密码加固 注册表加固 安全配置加固	主机隔离/关闭 端口隔离/关闭 文件隔离/关闭 进程关闭 服务关闭
物理阻断/隔离	加密敏感信息	服务组件启停	TCP重置
流量牵引	组件升级		IP阻断
部署蜜罐			网段封禁

表1 IRS系统动作执行集合

IRS的输入往往很难界定，不仅仅需要告警，还需要很多额外的信息，额外信息的选取与响应策略息息相关。一般来说，想要做出合理的响应动作，需要考虑如下因素：攻击影响评估，响应操作损失评估，响应操作收益评估。

攻击影响评估，指的是安全设备告警所指示的攻击倘若真实发生，对目标系统造成的影响。首先必须明确的是，想要明确量化特定攻击造成的影响几乎是不现实的，常用方法是对损失做一个近似估计，该估计在实际运维过程中是有必要的，通常涉及到两个主体，一个是攻击，一个是目标系统，若目标系统为非重要资产，往往不会受到过多关注，若攻击本身并无高危险性，实际运维过程中也往往将之忽略。若要将该过程进行量化评估，则涉及到三种输入：一是资产信息，用以判断资产的严重性，二是资产的漏洞信息，用以判断告警中的攻击是否会对目标系统产生影响，三是攻击严重程度，不同漏洞造成危害程度是不一样的，CVSS评分可以作为一种参考。

响应操作损失评估，指的是操作对正常业务造成的影响，如关闭一台Web主机造成的影响，如：用户影响、业务影响等等，对于重要业务系统，响应策略往往需要非常保守，响应的前提条件也要以不影响正常业务也前提条件。

响应操作收益评估，指的是操作带来的收益，如是否能根除或者缓解攻击。

由于响应策略的选择过程涉及到过多的因素，因此IRS的输入绝不仅仅是设备告警这一个信息维度，往往还需要包含：攻击知识库，资产信息，网络拓扑结构等一系列辅助信息。

2.5 入侵响应系统的核心

入侵响应系统的核心是响应动作的选择策略问题，需要考虑大量的输入因素做出最终决策，放在现实运维场景中，分析人员需要根据攻击的严重程度、网络拓扑、操作的可能造成的后果等因素在面对攻击的时候做出及时的、风险承受范围内的操作，因此，本质上，该问题是一个多目标决策问题，限制条件为时间和成本。在众多研究当中，研究者们发明出攻击图、攻击树、防御树等分析方法对上一小节所述的各种维度进行量化评估，由于这些方法通常需要满足大量的前置条件，也没有一个成型的算法在实际工业生产中投入使用。

第三章 策略选择算法

策略选择算法是IRS系统的核心所在，在学术界有比较多的研究，其中很大一部分都是构造攻击图、攻击树、防御树等数据结构来对攻击成本和防御成本做分析，但是这些方法往往需要对内网资产、漏洞、网络拓扑等信息有比较全面的了解，这对于现代企业尤其是大型企业来说并不现实，因此本部分仅对种类型的方法做简单介绍，重点介绍一种基于部分信息对各种因素做评估的方法。

3.1 攻击树、攻击图

为了对攻击影响进行评估，通常会构建攻击图或者攻击树的数据结构，这种结构用于描述资产之间的联通性和依赖性。具体来说，攻击树用于描述系统的安全状态，能够直观地描述可以通过哪些路径对该目标系统进行攻击，如图5所示，攻击图把网络拓扑、可能的漏洞联系起来，描述了攻击者可能通过哪些路径接触到特定的目标系统。

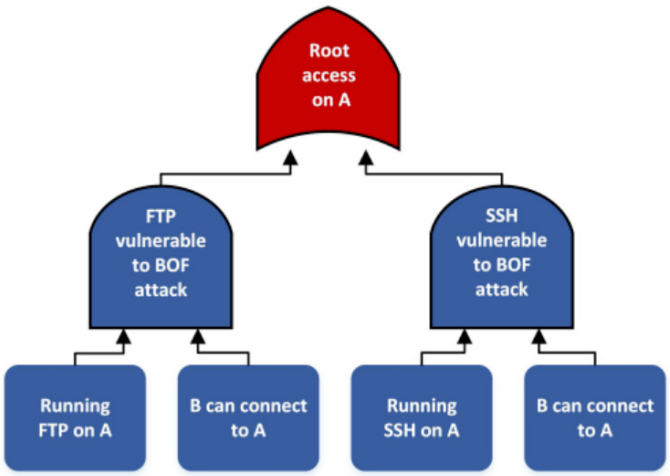


图5 攻击树样例

3.2 一种策略选择算法介绍

利用攻击树、攻击图等模型对各种因素进行评估在现实中会受到很大制约，系统之间的调用关系，存在的漏洞等信息错综复杂，很难完全梳理清楚，在这里我们介绍另一种方法[1]。

该方法按照如图5的步骤进行，可以看到策略选择的过程主要在于对各种因素进行评估，核心步骤主要分为4步：1.评估系统资产，该步骤旨在对系统资源做评估，了解各种资源的服务的重要性，2.设定评估入侵损害，根据攻击的严重程度、置信度、攻击目标等因素判定损失程度，3.评估响应成本，响应成本包括响应执行的收益，响应执行的负面作用和响应执行的操作成本，4.策略选择，该步骤需要对各种因素做有机结合，从而选择最优的动作。

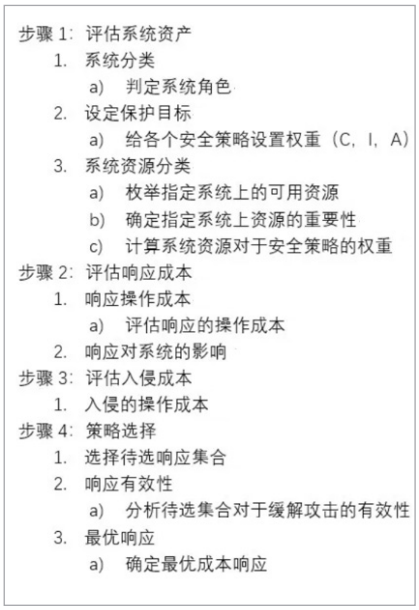


图6 一种无须全局信息的策略选择方法

◆ 评估系统资产

一个主机上有时候会运行多个服务，将这些服务表示为集合SR = (sr1, sr2, . . . , srz)，将一个服务的重要性表示为Wsrj ，该重要性由该资源在（C,I,A）上影响性和对应的权重组成，以一台Web服务器为例，网络接口的重要性可以按照如下方式计算：网络接口在的可用性要求最高，评分为1，机密性和完整性次之，评分为0.1，而CIA对于整个Web服务来说，权重分别问0,1和0.7，因此网络接口的重要性评分为1.07.

Policy Category	Weight (w)	Importance of Network Access (F)
confidentiality	0	0.1
availability	1.0	1.0
integrity	0.7	0.1
$W_{NetworkAccess} = 0 \times 0.1 + 1.0 \times 1.0 + 0.7 \times 0.1 = 1.07$		

◆ 评估响应成本

将响应定义为集合R = (r1,. . . , rn)，响应成本为rg，响应成本由两方面组成：操作成本和对系统的影响性，其中不同操作成本（如增加防火墙规则，给系统打补丁）之间存在较大差异，表示为OC(rg)，这个需要人工设定具体数值；对系统的影响性按照如下方式确定：1.确定会被操作影响的系统服务，2.把每个响应对服务的影响性按序排列，3.按照如下公式计算：

$$\mathrm{Impact}_{r_g,sr_j} = 1 - \frac{g}{h}$$

其中h为总响应数，g为当前响应的服务的影响性排名，我们以如下5种动作对网络接口的影响性为例，隔离整个网络的影响性最高，部署分析工具的影响性最小。

Rank g	Responses for sr_j	$\mathrm{Impact}_{r_g,sr_j}$
0.	Complete network isolation	1 - 0/5 = 1.0
1.	Network isolation: block subnet	0.8
2.	Terminate process	0.6
3.	Delay suspicious process	0.4
4.	Deploy intrusion analysis tools	0.2

那么，响应的影响成本可以表示为：

$$\mathrm{RC}(r_g) = \mathrm{OC}(r_g) + \sum_{sr_j \in SR} Impact_{r_g,sr_j} * W_{sr_j}$$

由于篇幅限制，对于入侵成本评估和策略选择方法本文在此不做过多介绍，感兴趣的读者可以参考[1].

第四章 整体分析

其实IRS与IDS的研究最早都可以追溯到上世纪90年代，可是由于IRS自身的复杂性、自动化响应实施困难等因素，不管工业界还是学术界，IDS一直是研究的主流方向，IRS的功能最多也只是以简单的响应组件的方式嵌套在IDS产品中，如IPS系统对流经的数据包做简单的放行/丢弃操作。面对日益复杂的网络攻击，SOC团队每天遇到海量的告警待处理，IPS已经完全不能满足现代企业的安全需求，安全编排自动化与响应（SOAR）的概念这个时候被业界广泛认同并寄予厚望。那么同样是一种自动化响应的方式，SOAR与学术界IRS的概念之间有何关系呢?

SOAR是Gartner 2015年提出的概念，组织收集来自不同数据源的安全威胁和警报数据,进行事故分析和分类，利用人类和机器的结合力量来帮助定义、划分优先级并推动标准化事件反应活动并形成一个标准的工作流程。其中，SOAR的核心就是Playbook，Playbook制定针对特定攻击的一整套处置流程，一旦配置完之后，便可做到对攻击的自动化响应。

实际上，通过图2我们不难发现，IRS中包含响应执行模块，而SOAR便是将响应执行模块做到极致的一种工业实践，并且前文所说的IRS的核心，响应决策模块，实际上对应的就是SOAR中内置的各种playbook，在实际生产环境当中，SOAR的playbook往往由有经验的工程师人为编排，因此这种方式往往受主观因素影响较大。

总结而言，学术界和工业界，自动化入侵响应的核心问题都是响应决策模块，因此我们可以清楚的明白SOAR未来的研究方向，即策略选择算法的研究。而通过对学术界主流的策略选择算法的介绍，读者不难发现，攻击图和攻击树的建模方式要求IRS对于系统之间的网络拓扑、系统漏洞情况有非常明确的认知，这很难满足实际情况，而不需要对全局信息有充分了解的方法，其评估方法也存在一定合理性问题，并且同样需要很多人工因素的参与，如人工设置各种系统和服务的重要性等等，这些不足导致学术界的方法很难适应现实中的入侵响应系统。

整体流程上，SOAR可以参照前文所述的评估系统资产、评估响应成本、评估攻击成本、策略选择的4步走策略，但是由于众多的因素会影响到响应动作的评估过程，这些因素也往往不好量化，究其原因，是我们在实际安全运维过程中往往会受到各种限制，我们将这些限制总结为IRS系统面临的4大挑战供读者参考：

1. 安全设备缺乏对内网环境的可见性。可见性分由多个方面组成，如：资产的可见性、漏洞的可见性、网络拓扑的可见性等等，现代企业的SOC一般被动地收集大量信息，但是缺乏对这些信息的进一步认知，例如，不清楚资产的重要性就无法进行针对性保护，缺乏对漏洞的可见性就会不清晰自身的薄弱环节，更容易陷入到告警疲劳之中，缺乏对网络拓扑的可见性就会丧失对攻击者的攻击路径和防御路径的判断，根据一项调查表明，网络环境的可见性是全球SOC的通病，也是分析人员公认的痛点之一[6]。更近一步，内网环境可见性的缺失会影响到各种防御措施的量化评估工作。

2. 缺乏动作影响因素的清晰的认知和量化。如，很多研究类论文称IRS系统需要考虑攻击代价与防御代价，但是动作的防御代价按常理来说应该由人工参与度、攻击的严重性、误操作严重性等等一系列因素构成，至今为止该因素的构成因素并未达成共识，并且没有一个合理的评估方法对这些因素进行量化；另一方面，动作的执行代价与保护的目标息息相关，信息系统的安全性往往有机密性、完整性、可用性（CIA）三方面构成，不同的保护目标对于动作的执行代价也存在一定差异。总之，由于无法量化，自动化响应往往也成为空中楼阁。

3. 误报的控制。基于大量误报的自动化工具对于安全运营来说无疑是一场灾难，虽然有一些模型会把告警的置信度进行评估，只对高置信度的告警进行处置，但是置信度如何计算，计算结果是否可靠等问题依然很具挑战性。

4. 动作采取的实时性。动作采取的延迟越大，内部网络所遭受的风险越大，具有关研究表明[5]，对于一个熟练的攻击者，响应延迟为10小时，入侵的成功率为80%，20小时，成功率为95%，30小时，攻击者几乎没有失败过，而目前业界在使用的SOAR，绝大多数场景还是在攻击成功，损失造成之后再进行响应，其动作的实时性还是有待提升。

第五章 总结

本文介绍了入侵响应系统的有关概念，通过比较工业界目前使用的入侵响应系统和理想中的入侵响应系统，读者可以清晰的了解到，虽然入侵响应系统有了20年左右的发展，但是目前来说仍然进展缓慢，笔者总结了造成这

种现象的主要挑战，并通过实际案例介绍一种学术界的入侵响应算法，读者可以清晰地看到这些方法无法落地的真正原因。

而如今虽然大数据、人工智能等技术蓬勃发展，但是这类技术的应用场景往往需要大量的标注、评估方法确定等比较确定的场景中，而就目前而言，IRS系统中的各个衡量指标往往存在争议，评估中的各种不确定性因素众多，执行结果的反馈往往不足，这些因素制约了高级算法在该领域的进一步应用。但是尽管如此，工业界对于响应自动化的需求是迫切的，SOAR仅仅根据专家知识构建出一套可以自动化运行的脚本便可在安全市场内大放异彩，可以预见策略选择方法的进一步研究会推动该方向的发展！

参考文献：

[1] Stakhanova, Natalia, et al. "Towards cost-sensitiveassessment of intrusion response selection." Journal of computersecurity 20.2-3 (2012): 169-198.

[2] Inayat, Zakira, et al. "Intrusionresponse systems: Foundations, design, and challenges." Journal of Networkand Computer Applications 62 (2016): 53-74.

[3] Nespoli, Pantaleone, et al. "Optimal countermeasuresselection against cyber attacks: A comprehensive survey on reactionframeworks." IEEE Communications Surveys & Tutorials 20.2(2017): 1361-1396.

[4] Foo, Bingrui, et al. "Intrusionresponse systems: a survey." Information assurance: dependability andsecurity in networked systems (2008): 377-412.

[5] Cohen, Fred. "Simulating cyber attacks, defences, andconsequences." Computers & Security 18.6 (1999):479-518

[6] Kokulu, Faris Bugra, et al."Matched and Mismatched SOCs: A Qualitative Study on Security OperationsCenter Issues." Proceedings of the 2019 ACM SIGSAC Conference on Computerand Communications Security. 2019.

[7] Carver, Curtis A. "Adaptive-basedintrusion response." College Station: Texas A&M University (2001).

[8] https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

关于天枢实验室

天枢实验室聚焦安全数据、AI攻防等方面研究，以期在“数据智能”领域获得突破。

特朗普竞选网站遭加密货币骗子黑客攻击

摘要：外媒 TechCrunch 报道，美国总统特朗普的竞选网站周二下午部分遭到黑 客攻击，因为未知的对手接管了 “关于”页面，并将其替换为似乎是一个收集加密 货币的骗局。尽管黑客声称，没有迹象表明实现了“对特朗普和其亲属的完全访 问”，或者 “大多数内部和秘密对话严格保密的信息 ”被曝光。

关键词：标签(特朗普、竞选网站、加密货币)，技术问题(安全事件)。

内容：据外媒 TechCrunch 报道，美国总统特朗普的竞选网站周二下午部分遭到 黑客攻击，因为未知的对手接管了 “关于”页面，并将其替换为似乎是一个收集加 密货币的骗局。尽管黑客声称，没有迹象表明实现了“对特朗普和其亲属的完全访 问”，或者 “大多数内部和秘密对话严格保密的信息 ”被曝光。

这次黑客攻击似乎发生在太平洋时间 10 月 27 日下午 4 点之后不久。黑客很可能 获得了对 donaldjtrump.com 网站服务器后台的访问权限，并将 “关于 “页面换成 了一段长长的经过混淆的 javascript，产生了一个模仿FBI“这个网站已经被查封” 的信息。

“世界已经受够了总统唐纳德·特朗普每天传播的假新闻，”新网站写道。“是时候让世界知道真相了。”

黑客声称自己掌握了“新冠病毒起源”的内部信息以及其他诋毁特朗普的信息， 他们提供了两个 Monero 地址。Monero 是一种容易发送但相当难以追踪的加密货币。一个地址是给那些希望“严格保密信息 ”被公布的人的，另一个地址是给那些希望保密的人的。在一个未指定的截止日期后，加密货币的总数将被比较，较高的总数将 决定如何处理这些数据。该页面用 PGP 公钥签署，对应一个不存在的域名 (planet.gov)的电子邮件地址。

在黑客攻击发生后几分钟内，网站就恢复了原来的内容。没有证据表明捐赠者信 息等任何敏感数据被访问，但在网站管理员彻底调查该事件之前，这是一个可能性。 让人们不可逆地将加密货币发送到一个神秘的地址是网上常见的诈骗形式，通常依靠 在名人 Twitter 账号等高知名度平台上短暂出现,这次也不例外。

没有任何迹象表明这次攻击是以任何方式由国家支持的。竞选和其他与选举相关的网站是黑客的高价值目标，它们并不像 whitehouse.gov 这样的官方网站那样安全。 虽然用词似乎不是以英语为母语的人，但没有其他正面证据表明黑客来自外国。

这不是特朗普最近第一次被黑客攻击。一个猜到密码(”Maga2020!”)的安全 研究人员称曾短暂接管特朗普的 Twitter 账号。特朗普最近表示，“没有人被黑客攻 击。黑客入侵需要一个智商 197 的人，而他需要你密码的 15%。”

信息来源: http://hackernews.cc/archives/32970

QBot 银行木马利用美国大选相关主题为诱饵，开展垃圾邮件活动

摘要：2020 年美国大选是大众关注的主题。随着选举之夜的结束以及对结果的不确定性开始蔓延，威胁行动者也决定加入进来。犯罪分子利用这些事件开展新的垃圾邮件活动，该活动传递了恶意附件。QBot 银行木马运营商使用相同的劫持电子 邮件线程技术，再次引发了垃圾邮件的浪潮。

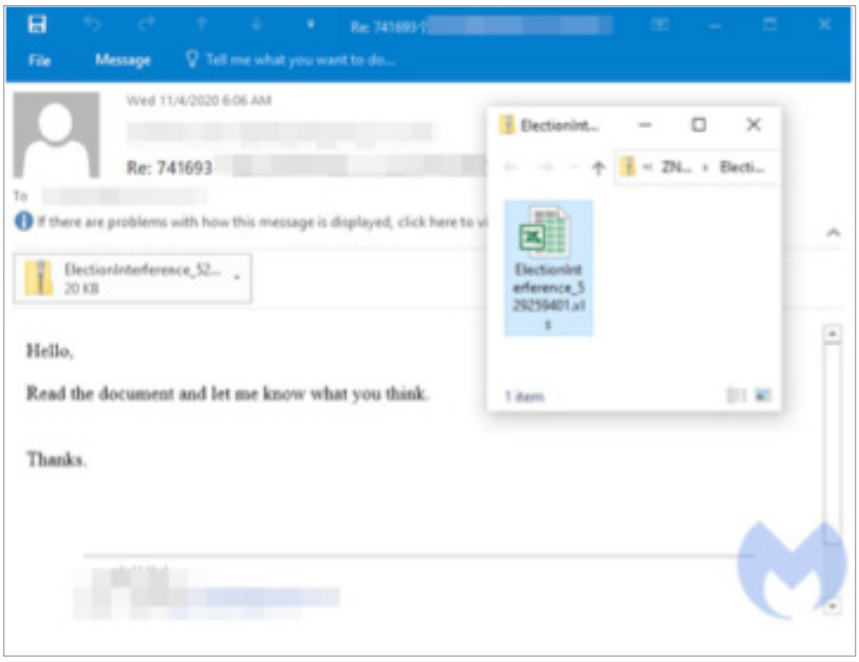
关键词：标签(QBot 银行木马、美国大选、垃圾邮件)，技术问题(安全事件)。

内容：2020 年美国大选是大众关注的主题。随着选举之夜的结束以及对结果的 不确定性开始蔓延，威胁行动者也决定加入进来。

犯罪分子利用这些事件开展新的垃圾邮件活动，该活动传递了恶意附件。QBot 银行木马运营商使用相同的劫持电子邮件线程技术，再次引发了垃圾邮件的浪潮。

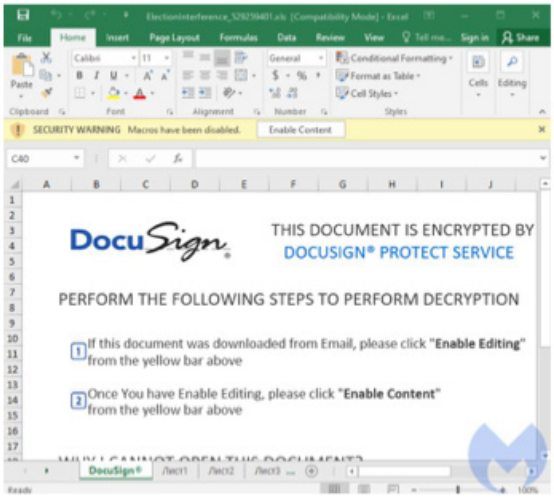
恶意电子邮件以回复的形式出现，类似于 Emotet 的操作，以增加合法性并增加 检测难度。它们包含适当地名为 ElectionInterference_ [8 至 9 位数字] .zip 的 zip 附件。

虽然选举结果仍在评估和辩论中，但受害者还是被诱使打开文档以阅读有关所谓的选举干预的信息:



带有 ElectionInterference 附件的恶意电子邮件

从附件中提取的文件是一个 Excel 电子表格，该电子表格经过精心处理，就像是安全的 DocuSign 文件一样。欺骗用户以允许宏来“解密”文档。



包含恶意宏的 Excel 文档

一旦执行，QBot 木马将联系其 C&C 服务器并请求指令。除了从受害者那里窃取和泄露数据外，QBot 还将开始抓取电子邮件，这些电子邮件将在以后的下一次恶意垃圾邮件活动中使用。

QBot 流程执行

ip 地址:

IP 地址	地理信息	ASN	情报标签
142.129.227.86	美国-California-Pomona	20001 (Time Warner Cable Internet LLC)	
95.77.144.238	罗马尼亚-Prahova-Dumbrava	6830 (Liberty Global Operations B.V.)	

信息来源: https://ti.dbappsecurity.com.cn/informationDetail/1331

警告！新的 Android 银行木马从 112 个金融 APP 中窃取数据

摘要：安全研究人员发现了针对巴西，拉丁美洲和欧洲金融机构的银行木马 “Tetrade”，四个月后，调查表明，攻击者扩大了策略，利用间谍软件感染移动设备。

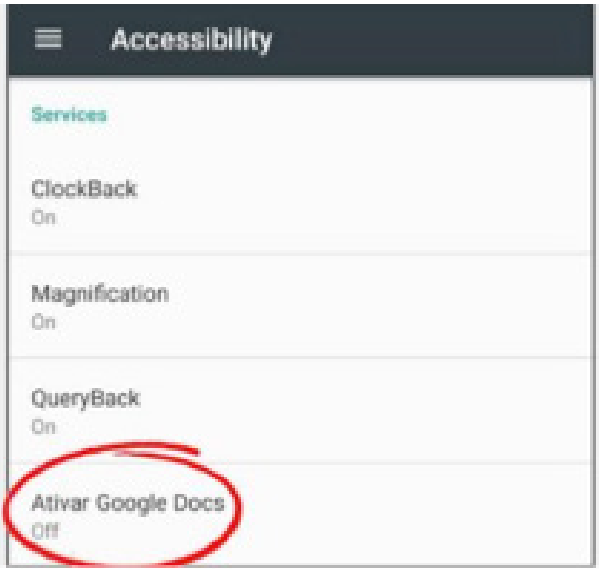
关键词：标签(Android 银行木马、窃取数据)，技术问题(安全事件)。

内容：安全研究人员发现了针对巴西，拉丁美洲和欧洲金融机构的银行木马 “Tetrade”，四个月后，调查表明，攻击者扩大了策略，利用间谍软件感染移动设 备。

根据卡巴斯基的全球研究和分析团队(GReAT)的说法，总部位于巴西的威胁集 团 Guildma 部署了“Ghimob”，这是一种 Android 银行木马，针对的是巴西、巴拉圭、 秘鲁、葡萄牙、德国、安哥拉和莫桑比克的银行、金融科技公司、交易所和加密货币 的金融应用程序。

网络安全公司在报告中表示，“Ghimob 是您一种成熟间谍:一旦感染完成，黑客就可以远程访问受感染的设备，用受害者的智能手机完成欺诈交易，从而避免被识别、金融机构采取的安全措施以及所有他们的反欺诈行为系统。”

除了共享与 Guildma 相同的基础结构外，Ghimob 继续使用网络钓鱼电子邮件作为分发恶意软件的机制，从而诱使毫无戒心的用户单击可下载 Ghimob APK 安装程序的恶意 URL。



该木马一旦安装在设备上，其功能与其他移动 RAT 十分相似，它通过隐藏应用程序中的图标来掩饰自己的存在，并滥用 Android 的辅助功能来获得持久性，禁用手动卸载并允许银行木马捕获击键信息，操纵屏幕内容并向攻击者提供完全的远程控制。

研究人员表示:“即使用户有适当的屏幕锁定模式，Ghimob 也能够记录下来， 然后再解锁设备。”

“当攻击者准备执行交易时，他们可以插入黑屏作为覆盖或以全屏方式打开某些网站，因此当用户查看该屏幕时，攻击者通过受害者运行的金融应用程序在后台执行 交易。”

此外，Ghimob 的目标多达 153 个移动应用程序，其中 112 个是巴西的金融机构， 其余的是德国，葡萄牙，秘鲁，巴拉圭，安哥拉和莫桑比克的加密货币和银行应用程序。

卡巴斯基研究人员总结说:“Ghimob 是巴西第一家准备扩展并瞄准居住在其他国家的金融机构及其客户的移动银行木马。”“该木马可以从许多国家/地区窃取 银行、金融科技、交易所、加密货币交易所和信用卡数据。”

信息来源: http://hackernews.cc/archives/33374

Akropolis 遭到闪电贷攻击 损失 200 万美元 DAI 代币

摘要：据外媒报道，近日，加密货币借贷服务 Akropolis 表示，一名黑客对其平台进行了“闪贷”攻击，偷走了价值约 200 万美元的 Dai 加密货币。

关键词：标签(Akropolis、黑客攻击、DAI)，技术问题(安全事件)。

内容：Akropolis 是 DeFi 借贷和存储服务提供商，用户可以从加密货币储蓄中获得贷款并产生收益。该服务的存储部分用的是 Curve 协议，在当天早些时候的攻击中被利用了。

攻击发生在 12 日下午(格林威治时间)，Akropolis 管理人员暂停了平台上的所有交易，以防止进一步的损失。

Akropolis 说，虽然它聘请了两家公司来调查这一事件，但两家公司都无法查明利用该攻击的攻击载体。尽管如此，此次入侵被认定为“闪贷”攻击。

闪发贷款攻击已经成为针对运行 DeFi(去中心化金融)平台的加密货币服务的常见攻击，该平台允许用户使用加密货币借入或贷款，投机价格变化，并从加密货币储蓄类账户赚取利息。

闪速贷款攻击发生在黑客从 DeFi 平台(如 Akropolis)借出资金，然后利用平台代码中的漏洞逃避贷款机制，并获得资金。

自今年 2 月初以来，此类攻击的数量一直在增加，其中最大的一次闪电贷款攻击发生在上个月，也就是 10 月份，黑客从 DeFi service Harvest Finance 窃取了价值 2400 万美元的加密货币资产。

好消息是，Akropolis 声称自己已经找到了攻击者的 Ethereum 账户，可以在资金在区块链上流动时进行追踪。

DeFi 平台表示，目前它已经通知了主要加密货币交易所关于黑客和攻击者的钱包，试图冻结资金，防止攻击者将资金洗钱到其他形式的加密货币，丢失调查人员的踪迹，并将资金套现。

Akropolis 表示，该公司目前正在探索补偿用户损失的方法。

信息来源:

https://mp.weixin.qq.com/s/vg101A4gJJQN_BVyQddzaA

加密货币交易所 Liquid 确认遭遇黑客攻击

摘要：加密货币交易所 Liquid 已确认遭到黑客攻击，它仍在调查受影响的范围有多大。Liquid 首席执行官 Mike Kayamori 在博客中表示，在这次攻击当中黑客获得了公司域名记录的访问权限，使得黑客控制员工的电子邮件账户，随后入侵了公司的网络。

关键词：标签(交易所、Liquid、黑客攻击)，技术问题(安全事件)。

内容：加密货币交易所 Liquid 已确认遭到黑客攻击，它仍在调查受影响的范围有多大。 Liquid 首席执行官 Mike Kayamori 在博客中表示，这次黑客攻击攻击发生在 11 月 13 日，在攻击当中黑客获得了公司域名记录的访问权限，使得黑客控制员工的电子邮件账户，随后入侵了公司的网络。

Kayamori 表示，虽然加密货币资金已经 "入账"，但黑客可能已经访问了公司的文件存储。Liquid 认为，黑客有能力从用户数据库中获取个人信息，如客户的电子

邮件、姓名、地址和加密密码等数据。加密货币交易所 Liquid 表示，它正在继续调查，如果黑客获得了用户向交易所提交的用于验证身份的文件，如政府颁发的身份证、 自拍照或地址证明，这可能会使用户面临身份被盗风险，或进行有针对性的攻击。

Liquid 在一封电子邮件中告诉用户，为了安全起见，他们应该更改密码。通常，针对公司网络基础设施的攻击会利用弱小或重复使用的密码，这些密码被用来注册公司的域名。通过闯入并更改这些网络设置，攻击者可以在无形中控制网络，并获得对电子邮件账户和系统的访问权，而通过其他攻击途径则要困难得多。

鉴于入侵可能带来巨大经济回报，加密货币初创公司和交易所是黑客的高价值目标。2018 年，Nano 在一次黑客事件中被盗走 1.7 亿美元 Binance 和 Coincheck 在黑客入侵后分别损失了 4 亿美元的巨额资金，Coinrail 在一次黑客攻击后损失了 4000 万美元，Bithumb 损失了 3000 万美元。

加密货币交易所 Liquid 成立于 2014 年，并声称在过去的一年里促成了 500 亿美元的加密货币交易。

信息来源: https://new.qq.com/omn/20201119/20201119A04Z5X00.html

NSFOCUS

漏洞聚焦

Citrix SD-WAN 安全漏洞安全通告

发布时间：2020 年 11 月 18 日

综述

近日，Citrix SD-WAN发布安全通告称修复了SD-WAN中的3个安全漏洞:CVE-2020-8271,CVE-2020-8272,CVE-2020-8273。在可以访问SD-WAN Center网络的情况下，未授权的攻击者可以利用这些漏洞以root权限执行任意代码。

目前已有相关漏洞的细节分析内容与CVE-2020-8271的POC。

漏洞概况

CVE	漏洞影响	利用条件
CVE-2020-8271	未授权的远程代码执行。	攻击者必须能够访问 SD-WAN Center's Management IP/FQDN
CVE-2020-8272	验证绕过，从而暴露 SD-WAN 的相关功能	
CVE-2020-8273	权限提升：普通认证用户提权成为 root 权限用户	攻击者必须是 SD-WAN Center 认证过的用户

受影响产品版本

- ☐ Citrix SD-WAN 版本 < 11.2.2
- ☐ Citrix SD-WAN 版本 < 11.1.2b

- ☐ Citrix SD-WAN 版本 < 10.2.8

不受影响的版本

- ☐ Citrix SD-WAN 版本 >= 11.2.2
- ☐ Citrix SD-WAN 版本 >= 11.1.2b
- ☐ Citrix SD-WAN 版本 >= 10.2.8

解决方案

Citrix官方已经发布了新版本修复了上述漏洞，受影响的用户请尽快升级进行防护。

新版本下载地址：

https://www.citrix.com/en-gb/downloads/citrix-sd-wan/

参考链接：

https://support.citrix.com/article/CTX285061

https://medium.com/realmodelabs/sd-pwn-part-2-citrix-sd-wan-center-another-network-takeover-a9c950a1a27c

Drupal 任意 PHP 代码执行漏洞（CVE-2020-28949、28948）安全通告

发布时间：2020 年 11 月 26 日

综述

北京时间11月26日，Drupal官方发布安全通告称修复了2个Critical级别的任意PHP代码执行漏洞CVE-2020-28949和CVE-2020-28948。

漏洞是由Drupal 使用的PEAR Archive_Tar库引入，后者用于在PHP中对tar文件进行处理。Archive_Tar中存在PHAR反序列化漏洞以及本地文件覆盖漏洞。

当Drupal配置为允许.tar、.tar.gz、.bz2或.tlz等类型文件上传，并对上传文件进行处理时，远程攻击者可能利用漏洞实现任意代码执行。

受影响产品版本

- ☐ Drupal 9.0.x
- ☐ Drupal 8.9.x
- ☐ Drupal 8.8.x
- ☐ Drupal 7.x

不受影响版本

- ☐ Drupal 9.0.9
- ☐ Drupal 8.9.10
- ☐ Drupal 8.8.12
- ☐ Drupal 7.75

解决方案

目前Drupal官方已经发布新版本修复了上述漏洞，建议受影响用户应尽快升级进行防护。

新版本下载地址如下:

Drupal 9.0: https://www.drupal.org/project/drupal/releases/9.0.9

Drupal 8.9: https://www.drupal.org/project/drupal/releases/8.9.10

Drupal 8.8: https://www.drupal.org/project/drupal/releases/8.8.12

Drupal 7 : https://www.drupal.org/project/drupal/releases/7.75

在不能马上升级的情况下，可禁止用户上传 .tar、.tar.gz、.bz2及.tlz等类型的压缩包作为缓解。

官方通告：

https://www.drupal.org/sa-core-2020-013

Drupal 远程代码执行漏洞 CVE-2020-13671 安全通告

发布时间：2020 年 11 月 19 日

综述

北京时间11月19日，Drupal官方发布安全通告称修复了一个远程代码执行漏洞CVE-2020-13671。该漏洞源于Drupal Core没有正确的处理上传文件的文件名，导致后续处理中文件会被错误地解析为其他MIME类型，在特定的配置下，文件可能会被当做PHP解析，从而导致远程代码执行。

受影响产品版本

- ☐ Drupal 9.0.x
- ☐ Drupal 8.9.x
- ☐ Drupal 8.8.x
- ☐ Drupal 7.x

不受影响版本

- ☐ Drupal 9.0.8
- ☐ Drupal 8.9.9
- ☐ Drupal 8.8.11
- ☐ Drupal 7.74

解决方案

目前Drupal官方已经发布了新版本修复了上述漏洞，受影响的用户应尽快升级进行防护。

新版本下载地址如下:

Drupal 9.0: https://www.drupal.org/project/drupal/releases/9.0.8

Drupal 8.9: https://www.drupal.org/project/drupal/releases/8.9.9

Drupal 8.8: https://www.drupal.org/project/drupal/releases/8.8.11

Drupal 7 :

https://www.drupal.org/project/drupal/releases/7.74

同时，用户可以检查已上传的文件中是否存在可疑的文件名，尤其是多个后缀的文件，具体建议可参考官方通告：

https://www.drupal.org/sa-core-2020-012

SaltStack 多个安全漏洞 CVE-2020-16846, CVE-2020-17490, CVE-2020-25592 安全通告

发布时间：2020 年 11 月 4 日

综述

近日，SaltStack官方发布安全通告称修复了多个安全漏洞，CVE-2020-16846,CVE-2020-17490,CVE-2020-25592。这些漏洞可造成认证绕过和命令执行，SaltStack建议用户尽快升级进行防护。

Salt是用Python编写的开源IT基础架构管理解决方案，已被全世界的数据中心广泛使用。

参考链接：

https://www.saltstack.com/blog/on-november-3-2020-saltstack-publicly-disclosed-three-new-cves/

漏洞概述

☐ CVE-2020-16846

攻击者在连接到Salt API时，可以利用Shell注入(shell injection)获取SSH连接，从而执行Salt-API命令。

☐ CVE-2020-17490

攻击者可以利用一个低权限的用户登录Salt主机端并读取秘钥内容，造成信息泄露。

☐ CVE-2020-25592

由于Salt中eauth和ACL功能存在认证绕过漏洞，攻击者可以通过salt-api绕过身份验证，从而利用salt ssh连接目标主机，并执行命令。

受影响产品版本

☐ 2015
☐ 2016
☐ 2017
☐ 2018
☐ 2019
☐ 3000
☐ 3001
☐ 3002

解决方案

SaltStack官方已经发布更新修复了上述漏洞，建议用户尽快升级进行防护。

新版本下载地址：

https://repo.saltstack.com/

相关修复版本下载地址：

https://gitlab.com/saltstack/open/salt-patches

【二次更新】Weblogic Console CVE-2020-14882 补丁绕过防护方案

发布时间：2020 年 11 月 2 日

一、综述

【更新说明】：

本次更新主要新增以下两部分信息：

1. Oracle 官方为 CVE-2020-14882补丁绕过发布解决方案,并分配编号 CVE-2020-14750，详见3.2 官方修复方案。

2. WAF 自定义规则更新，之前已经添加过自定义规则和升级规则包的用户仍建议添加，详见 4.5 WAF自定义规则配置。

Oracle官方为 Weblogic Console CVE-2020-14882发布的补丁并不完善，存在被绕过的情况，且官方暂未发布针对该补丁绕过的解决方案。

在 Weblogic 安装了 10月最新补丁的情况下，攻击者通过绕过CVE-2020-14882的补丁，依然可以绕过 Console 控制台的权限校验，直接访问原本需要登录才能访问的各种资源和接口功能。

建议相关用户在官方解决方案发布前尽快采取防护措施！

Oracle官方CPU链接：

https://www.oracle.com/security-alerts/cpuoct2020.html

二、漏洞影响范围

- ☐ Oracle Weblogic Server 10.3.6.0.0
- ☐ Oracle Weblogic Server 12.1.3.0.0
- ☐ Oracle Weblogic Server 12.2.1.3.0
- ☐ Oracle Weblogic Server 12.2.1.4.0
- ☐ Oracle Weblogic Server 14.1.1.0.0

三、技术防护方案

3.1 临时缓解措施

在不影响正常业务的情况下，建议暂时对外关闭后台 /console/console.portal 的访问权限 ，或者对 Console 访问路径进行重命名（将默认的请求路径 console 更改为一个不易猜解的请求路径）。

3.2 官方修复方案

当地时间11月1日，Oracle 官方发布安全通告，为CVE-2020-14882补丁绕过漏洞分配编号 CVE-2020-14750，同时也发布了CVE-2020-14750的补丁。

请用户参考官方通告及时下载受影响产品更新补丁，并参照补丁安装包中的readme文件进行安装，以保证长期有效的防护。

注：Oracle官方补丁需要用户持有正版软件的许可账号，使用该账号登陆https://support.oracle.com后，可以下载最新补丁。

官方安全通告链接：

https://www.oracle.com/security-alerts/alert-cve-2020-14750.html

3.3 绿盟科技检测防护建议

3.3.1 绿盟科技检测类产品与服务

内网资产可以使用绿盟科技的远程安全评估系统（RSAS V6）、Web应用漏洞扫描系统（WVSS）、入侵检测系统(IDS)、统一威胁探针（UTS）进行检测。

- 远程安全评估系统（RSAS V6）

  http://update.nsfocus.com/update/listRsas
- Web应用漏洞扫描系统（WVSS）

  http://update.nsfocus.com/update/listWvss
- 入侵检测系统(IDS)

  http://update.nsfocus.com/update/listIds
- 统一威胁探针（UTS）

  http://update.nsfocus.com/update/bsaUtsIndex

3.3.1.1 检测产品升级包/规则版本号

检测产品	升级包 / 规则版本号
RSAS V6 系统插件	V6.0R02F01.2006
RSAS V6 Web 插件	V6.0R02F00.1904
WVSS V6 插件	V6.0R03F00.187
IDS	5.6.10.23834、5.6.9.23834
UTS	5.6.10.23834

- RSAS V6 系统插件包下载链接：

  http://update.nsfocus.com/update/downloads/id/109796
- RSAS V6 Web插件包下载链接：

  http://update.nsfocus.com/update/downloads/id/109793
- WVSS V6插件包下载链接：

  http://update.nsfocus.com/update/downloads/id/109792
- IDS 升级包下载链接：

  5.6.10.23834

  http://update.nsfocus.com/update/downloads/id/109743

  5.6.9.23834

  http://update.nsfocus.com/update/downloads/id/109742

- UTS升级包下载链接：

  http://update.nsfocus.com/update/downloads/id/109765

3.3.2 绿盟科技防护类产品

使用绿盟科技防护类产品，入侵防护系统（IPS）、Web应用防护系统（WAF）、下一代防火墙系统（NF）来进行防护。

- 入侵防护系统（IPS）

  http://update.nsfocus.com/update/listIps

- Web应用防护系统（WAF）

  http://update.nsfocus.com/update/wafIndex

- 下一代防火墙系统（NF）

  http://update.nsfocus.com/update/listNf

3.3.2.1 防护产品升级包/规则版本号

防护产品	升级包 / 规则版本号	规则编号
IPS	5.6.10.23834、5.6.9.23834	25079
WAF	添加自定义规则 uri_path * rco /console/appmanager/.*?\.\.	——
NF	6.0.2.833、6.0.1.833	25079

- IPS 升级包下载链接：

  5.6.10.23834

  http://update.nsfocus.com/update/downloads/id/109743

  5.6.9.23834

  http://update.nsfocus.com/update/downloads/id/109742

- NF 升级包下载链接：

  6.0.2.833

  http://update.nsfocus.com/update/downloads/id/109759

  6.0.1.833

  http://update.nsfocus.com/update/downloads/id/109760

3.3.3 安全平台

平台	升级包 / 规则版本号
TAM（绿盟全流量威胁分析平台）	2.0.7.232258
ESP-H（绿盟企业安全平台）	ESP-EVENTRULE-019-20201030.dat

四、附录A 产品使用指南

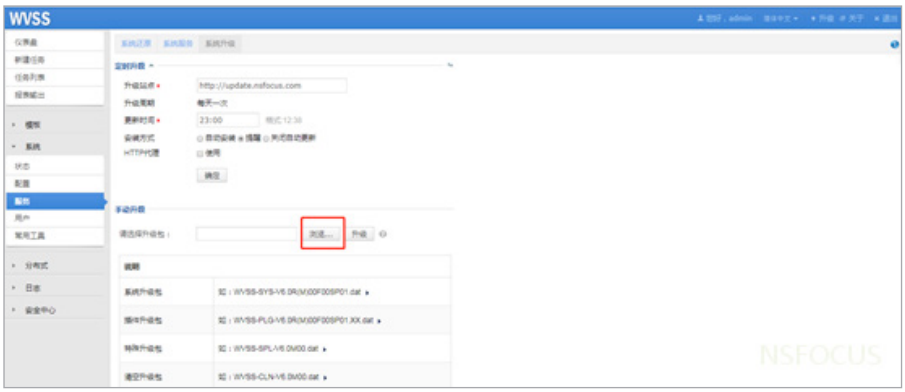
4.1 RSAS扫描配置

在系统升级中，点击下图红框位置选择文件。

选择下载好的相应升级包，点击升级按钮进行手动升级。等待升级完成后，可通过定制扫描模板，针对此次漏洞进行扫描。

4.2 WVSS扫描配置

在WVSS的系统升级界面，点击下图红框位置选择文件，进行升级：



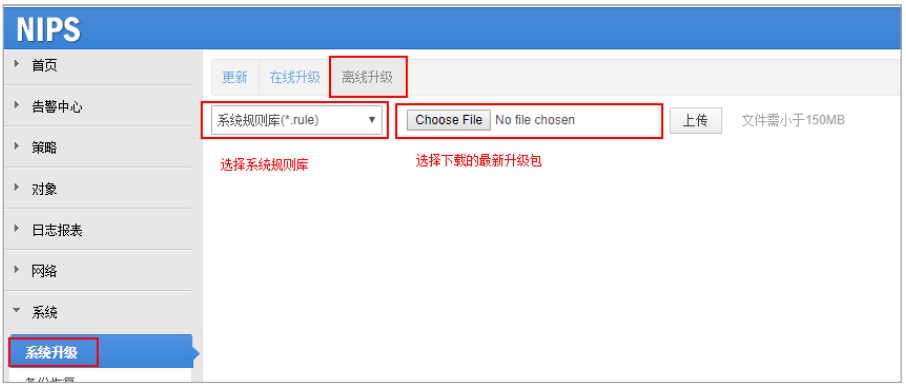
选择下载好的相应升级包，点击升级按钮进行手动升级。等待升级完成后，可通过定制扫描模板，针对此次漏洞进行扫描。

4.3 UTS检测配置

在系统升级中点击离线升级，选择规则升级文件，选择对应的升级包文件，点击上传，等待升级成功即可。

4.4 IPS防护配置

在系统升级中点击离线升级，选择系统规则库，选择对应的文件，点击上传。



更新成功后，在系统默认规则库中查找规则编号，即可查询到对应的规则详情。

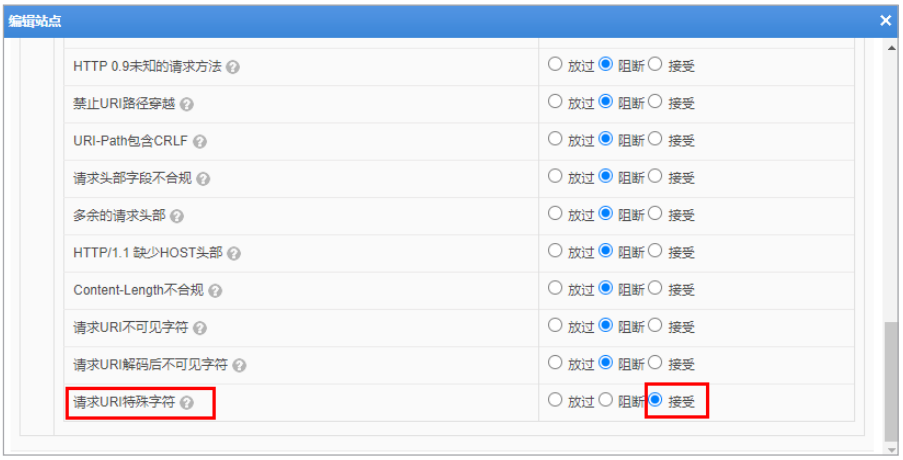
注意：该升级包升级后引擎自动重启生效，不会造成会话中断，但ping包会丢3~5个，请选择合适的时间升级。

4.5 WAF自定义规则配置

在系统中新建自定义规则，依次点击“安全管理”-“规则库管理”-“自定义”-“新建”

【更新规则】：

内置协议校验选项：“请求URI特殊字符”使用“接受”动作：



之前已经添加过自定义规则和升级规则包的用户仍建议添加以下自定义规则：

- 针对CVE-2020-14882

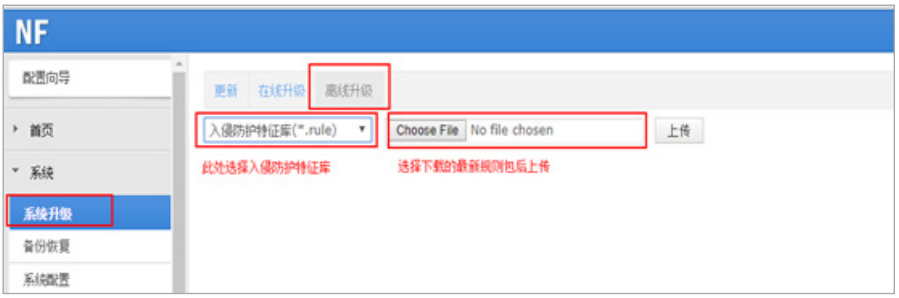

```
(uri_path * rco (images|common|css|js|bea-helpsets)/\S+(%2e|\.)/\S*console(jndi)?\.portal)
```

- 针对CVE-2020-14883


```
(parameter handle rco (com.tangosol.coherence.mvel2.sh.ShellSession|com.bea.core.repackaged.springframework.context.support.(ClassPath|FileSystem)XmlApplicationContext)\(".*?"\))
```

4.6 NF防护配置

在 NF 的规则升级界面进行升级：



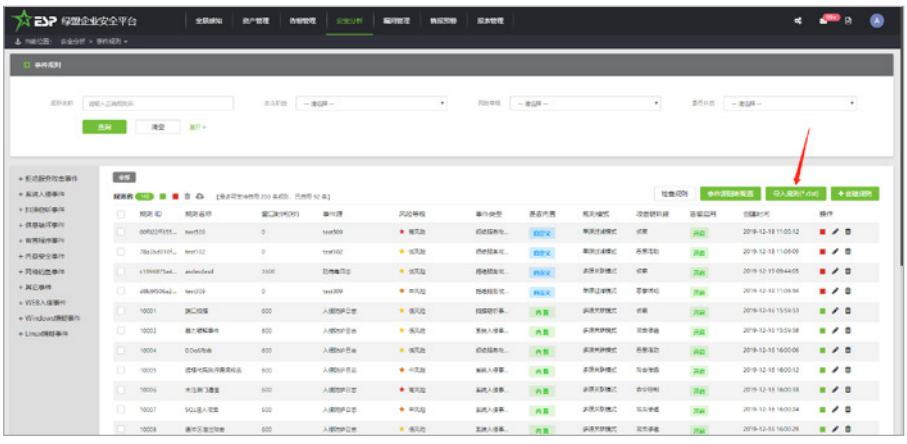
手动选择规则包，提交即可完成更新。

4.7 ESP-H（绿盟企业安全平台）

第一步：登录ESP/ESP-H平台

第二步：进入安全分析-事件规则

第三部：如下图，点击导入规则。



声明

Windows Kernel cng.sys 权限提升 0-day 漏洞 CVE-2020-17087 安全通告

发布时间：2020 年 11 月 2 日

综述

近日，Google Project Zero团队发布了一篇关于Windowscng.sys提权漏洞（CVE-2020-17087）的文章。该漏洞允许攻击者在未授权的情况下，通过诱使用户运行精心制作的恶意程序，从而达到权限提升的效果。

目前该漏洞已经有在野利用的行为出现，并且微软官方暂时没有发布相关补丁进行修复。建议用户保持关注，同时避免运行来历不明的程序。

参考链接：

https://bugs.chromium.org/p/project-zero/issues/detail?id=2104

受影响产品版本

- ☐ Windows 10
- ☐ Windows 7

解决方案

目前该漏洞已经被在野利用，微软官方尚未发布相关补丁进行修复，建议用户保持关注，同时避免运行来历不明的程序，等待官方补丁发布后，及时更新进行防护。

Windows 网络文件系统漏洞（CVE-2020-17051、CVE-2020-17056）安全通告

发布时间：2020 年 11 月 11 日

综述

当地时间11月10日，微软最新的月度补丁更新中修复了两枚存在于Windows网络文件系统（Network File System，NFS）中的漏洞，分别是 CVE-2020-17051和 CVE-2020-17056。

CVE-2020-17051 是存在于nfssvr.sys驱动中的远程代码执行漏洞，据称复现时可导致蓝屏死机（BSOD）[3]。

CVE-2020-17056是一个存在于nfssvr.sys驱动中的远程越界读取漏洞，可导致ASLR（地址空间布局随机化）被绕过。

当这两个漏洞被组合利用时，攻击者在Windows服务器上绕过漏洞缓解措施并实现远程利用的可能性将大大增加。

官方已为受影响系统提供了补丁，建议用户尽快安装更新进行防护。

NFS是个分布式的客户机/服务器文件系统。通过Windows NFS,用户可以在运行 Windows 的计算机上，像访问本地文件一样访问其他非 Windows 操作系统（如 Linux 或 UNIX）上的文件。

参考链接：

[1]https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-17051

[2]https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-17056

[3]https://www.mcafee.com/blogs/other-blogs/mcafee-labs/cve-2020-17051-remote-kernel-heap-overflow-in-nfsv3-windows-server/

受影响产品版本

CVE-2020-17051

- ☐ Windows 10 Version 20H2 for 32-bit Systems
- ☐ Windows 10 Version 20H2 for ARM64-based Systems
- ☐ Windows 10 Version 20H2 for x64-based Systems
- ☐ Windows Server, version 20H2 (Server Core Installation)
- ☐ Windows 10 Version 1809 for 32-bit Systems
- ☐ Windows 10 Version 1809 for x64-based Systems
- ☐ Windows 10 Version 1809 for ARM64-based Systems
- ☐ Windows Server 2019
- ☐ Windows Server 2019 (Server Core installation)
- ☐ Windows 10 Version 1909 for 32-bit Systems
- ☐ Windows 10 Version 1909 for x64-based Systems
- ☐ Windows 10 Version 1909 for ARM64-based Systems
- ☐ Windows Server, version 1909 (Server Core installation)
- ☐ Windows 10 Version 1903 for 32-bit Systems
- ☐ Windows 10 Version 1903 for x64-based Systems
- ☐ Windows 10 Version 1903 for ARM64-based Systems
- ☐ Windows Server, version 1903 (Server Core installation)
- ☐ Windows 10 Version 2004 for 32-bit Systems
- ☐ Windows 10 Version 2004 for ARM64-based Systems
- ☐ Windows 10 Version 2004 for x64-based Systems
- ☐ Windows Server, version 2004 (Server Core installation)
- ☐ Windows 10 Version 1607 for 32-bit Systems
- ☐ Windows 10 Version 1607 for x64-based Systems
- ☐ Windows Server 2016
- ☐ Windows Server 2016 (Server Core installation)
- ☐ Windows 7 for 32-bit Systems Service Pack 1
- ☐ Windows 7 for x64-based Systems Service Pack 1
- ☐ Windows 8.1 for 32-bit systems
- ☐ Windows 8.1 for x64-based systems

- ☐ Windows RT 8.1
- ☐ Windows Server 2008 for 32-bit Systems Service Pack 2
- ☐ Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
- ☐ Windows Server 2008 for x64-based Systems Service Pack 2
- ☐ Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
- ☐ Windows Server 2008 R2 for x64-based Systems Service Pack 1
- ☐ Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
- ☐ Windows Server 2012
- ☐ Windows Server 2012 (Server Core installation)
- ☐ Windows Server 2012 R2
- ☐ Windows Server 2012 R2 (Server Core installation)

CVE-2020-17056

- ☐ Windows 10 Version 1803 for 32-bit Systems
- ☐ Windows 10 Version 1803 for x64-based Systems
- ☐ Windows 10 Version 1803 for ARM64-based Systems
- ☐ Windows 10 Version 1809 for 32-bit Systems
- ☐ Windows 10 Version 1809 for x64-based Systems
- ☐ Windows 10 Version 1809 for ARM64-based Systems
- ☐ Windows Server 2019
- ☐ Windows Server 2019 (Server Core installation)
- ☐ Windows 10 Version 1909 for 32-bit Systems
- ☐ Windows 10 Version 1909 for x64-based Systems
- ☐ Windows 10 Version 1909 for ARM64-based Systems
- ☐ Windows Server, version 1909 (Server Core installation)
- ☐ Windows 10 Version 1903 for 32-bit Systems
- ☐ Windows 10 Version 1903 for x64-based Systems
- ☐ Windows 10 Version 1903 for ARM64-based Systems
- ☐ Windows Server, version 1903 (Server Core installation)
- ☐ Windows 10 Version 2004 for 32-bit Systems
- ☐ Windows 10 Version 2004 for ARM64-based Systems
- ☐ Windows 10 Version 2004 for x64-based Systems

- ☐ Windows Server, version 2004 (Server Core installation)
- ☐ Windows 10 for 32-bit Systems
- ☐ Windows 10 for x64-based Systems
- ☐ Windows 10 Version 1607 for 32-bit Systems
- ☐ Windows 10 Version 1607 for x64-based Systems
- ☐ Windows Server 2016
- ☐ Windows Server 2016 (Server Core installation)
- ☐ Windows 8.1 for 32-bit systems
- ☐ Windows 8.1 for x64-based systems
- ☐ Windows RT 8.1
- ☐ Windows Server 2012
- ☐ Windows Server 2012 (Server Core installation)
- ☐ Windows Server 2012 R2
- ☐ Windows Server 2012 R2 (Server Core installation)
- ☐ Windows 10 Version 20H2 for ARM64-based Systems
- ☐ Windows Server, version 20H2 (Server Core Installation)
- ☐ Windows 10 Version 20H2 for x64-based Systems
- ☐ Windows 10 Version 20H2 for 32-bit Systems

解决方案

微软官方已针对受影响系统发布安全补丁，强烈建议相关用户尽快更新。补丁升级，参考链接:

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-17051

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-17056

XStream 远程代码执行漏洞 CVE-2020-26217 安全通告

发布时间：2020 年 11 月 16 日

综述

近日，XStream官方发布安全通告，修复了一个远程代码执行漏洞CVE-2020-26217，远程攻击者在未授权的情况下，通过向使用 XStream 的web应用发送特制的请求，导致远程代码执行，进而取得目标服务器控制权限。XStream是一个常用的Java对象和XML相互转换的工具。

该漏洞是CVE-2013-7285的一种变体，利用了新的类对象在反序列化流程中绕过黑名单限制，从而导致远程代码执行。

参考链接：

http://x-stream.github.io/CVE-2020-26217.html

受影响产品版本

☐ xstream:xstream 版本 <= 1.4.13

不受影响的版本

☐ xstream:xstream 版本 1.4.14

解决方案

官方已经发布了新版本修复了上述漏洞，受影响的用户请尽快升级进行防护。

新版本下载地址：https://github.com/x-stream/xstream/releases

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. 华为向谷歌发起惊人的新一击，击败安卓

【概述】

华为Mate 40终于上市了。在美国限制为华为设备供电的芯片组设置限制的背景下，由于Google仍然缺失，中国领先的智能手机制造商发布了另一款出色的设备，该设备将根据其无法控制的因素在中国以外地区停售。尽管美国黑名单是真正存在的问题，但谷歌的损失再次成为新闻头条。

【参考链接】

https://www.forbes.com/sites/zakdoffman/2020/10/25/huawei-premium-smartphone-search-replaces-google-apple-iphone-and-samsung-galaxy-alternative/?ss=cybersecurity

2. 微软团队凭借出色的新功能与Zoom展开战斗

【概述】

在过去的几个月中，Microsoft Teams不断 涌现新功能，以击败最大的竞争对手Zoom。这些功能包括添加自定义背景和共同模式的能力，以使视频会议体验尽可能接近真实生活。

【参考链接】

https://www.forbes.com/sites/kateoflahertyuk/2020/10/25/microsoft-teams-battles-zoom-with-superb-new-features/

3. Vastaamo突破：黑客勒索心理治疗患者

【概述】

据报道，网络犯罪分子已经发布了300名Vastaamo患者的详细信息-并威胁要公开其他人的数据，除非支付赎金。

【参考链接】

https://threatpost.com/vastaamo-hackers-blackmailing-therapy-patients/160536/

4. 美国财政部禁止企业支付勒索软件赎金

【概述】

本月初，美国财政部外国资产控制办公室（OFAC）发布咨文警告组织不要向勒索软件支付赎金，并声称此举存在违反政府对网络犯罪集团或国家黑客施加的经济制裁的法律风险。

【参考链接】

https://www.aqniu.com/industry/70827.html

5. 出售美国庞大的选民数据库

【概述】

根据Trustwave的一份报告，在一个在线论坛上出售了多达1.86亿美国人的选民信息。Trustwave的SpiderLabs部门表示，这些信息显然来自公共资源以及数据泄漏。

【参考链接】

https://www.inforisktoday.com/massive-us-voter-database-offered-for-sale-a-15239

6. 进口开源软件纷纷中招，国产创新路在何方？

【概述】

8 月 13 日，Docker 更新了《服务条款》并于当日生效，禁止所有美国禁运国家和被列入【美国财政部指定国民清单】、【美国商务部实体清单】【被拒绝人清单】、【未核实清单】和【美国州界防扩散制裁清单】（统称为【指定国民清单】）的个人或实体使用带有该服务协议链接的 Docker 网站以及所有相关网站。

【参考链接】

https://www.aqniu.com/vendor/70873.html

7. 1.6亿小目标：黑客从Harvest Finance窃取价值1.6亿的数字货币

【概述】

10月26日，黑客从DeFi 挖矿项目 Harvest.finance窃取了价值2400万美元的数字货币，随后公司管理层在公司官方推特和Discord 确认了被黑的事实。根据官方发布的消息，黑客在Harvest.finance 项目中投入了大量的数字货币资产，然后利用数字货币漏洞利用讲平台资金非法转移到其钱包中。黑客总共窃取了价值2400万美元的数字货币，其中包括价值1300万美元的USD Coin (USDC)和价值1100万美元的Tether (USDT)。

【参考链接】

https://www.4hou.com/posts/wZWz

8. 问道新基建，大咖指点2021云安全趋势新动向

【概述】

10月26日，腾讯安全联合InfoQ共同举办的云安全趋势研讨会，汇聚中国信息通信研究院云大所云计算部副主任陈屹力、腾讯云安全总经理董志强、

腾讯云安全副总经理李滨、普华永道中国区信息安全与隐私保护合伙人万彬、数世咨询创始人李少鹏等来自科研院所、评测机构和一线厂商的专家，围绕“新基建快速发展，将面临哪些新的安全挑战”为主题，共话云上安全未来趋势。

【参考链接】

https://www.freebuf.com/articles/neopoints/253411.html

9. 威胁评估：Ryuk Ransomware和Trickbot针对美国医疗保健和公共卫生领域

【概述】

2020年10月28日，网络安全和基础设施安全局（CISA），联邦调查局（FBI）和卫生与公共服务部（HHS）发布了联合网络安全警报，内容涉及对美国日益严重的网络安全威胁。威胁运营商对以医疗保健和公共卫生部门为目标的兴趣日益浓厚，有可能破坏医疗保健服务和运营。观察到的活动包括使用Trickbot恶意软件，这是一种众所周知的信息窃取者，可能导致安装其他恶意文件，包括Ryuk勒索软件。

【参考链接】

https://unit42.paloaltonetworks.com/ryuk-ransomware/

10. 选举后的日子：美国警惕黑客攻击，错误信息

【概述】

在焦虑持续了数周之后，大选日在美国进行，没有公开迹象表明有人干预。但是专家说，错误的信息运动仍然可能发生，并且随着计票的进行，有大量的时间进行恶意活动。

【参考链接】

https://www.inforisktoday.com/post-election-day-us-on-guard-for-hacking-misinformation-a-15300

11. 美国公布俄罗斯黑客用于攻击议会、大使馆的恶意软件信息

【概述】

当地时间29日，美国网络司令部分享了俄罗斯黑客组织在针对外交部，国民议会和使馆多个部门的攻击中使用的恶意软件信息。该恶意软件样本由美国

网络司令部的网络国家任务部队（CNMF）以及网络安全和基础设施安全局（CISA）识别，并于昨日上传至Virus Total在线病毒扫描平台。

【参考链接】

https://www.freebuf.com/articles/253572.html

12. 芬兰的赎金黑客正在使用心理治疗病历作为弹药

【概述】

“除非您在48小时内向我支付了500欧元的加密货币，否则您的心理治疗患者记录将被公布”。在过去两周内，只有不到1%的芬兰人口收到了这一需求。多个潜在无关的人已经进入“ Vastaamo”心理治疗中心，该中心主要在奥卢和坦佩雷治疗了约40.000名患者。黑客利用了2018年和2019年初的安全漏洞，似乎尚未向当局或公众广泛报道。

【参考链接】

https://www.forbes.com/sites/michalgromek/2020/10/31/ransom-hackers-in-finland-are-using-psychotherapy-medical-records-as-ammunition/

13. Code42 Incydr系列：为什么大多数公司无法停止离职员工数据盗窃

【概述】

根据Code42的数据暴露报告，有63%的员工表示他们将数据从以前的雇主带到了当前的雇主。这是内部人风险的最明显的迹象：员工的辞职信。根据《信息安全杂志》（Infosecurity Magazine）的一项2019年研究发现，有72%的员工在离职时会使用公司数据。

【参考链接】

https://threatpost.com/code42-incydr-series-why-most-companies-cant-stop-departing-employee-data-theft/160879/

14. 新的APT使用DLL侧载到“ KilllSomeOne”

【概述】

最近，我们观察到了几种情况，其中DLL侧加载用于执行恶意代码。旁加载是利用恶意DLL欺骗合法的DLL，依靠合法的Windows可执行文件加载和执行恶意代码。

【参考链接】

https://news.sophos.com/en-us/2020/11/04/a-new-apt-uses-dll-side-loads-to-killlsomeone/

15. 利用美国大选不确定性通过malspam活动交付的QBot特洛伊木马程序

【概述】

2020年美国大选是在全球大流行中进行的同时，受到严格审查和情感关注的主题。随着选举之夜的结束以及对结果的不确定性开始蔓延，威胁行动者也决定加入进来。那些追踪威胁态势的人都非常清楚，重大世界事件并没有被犯罪分子所忽视。在这种情况下，我们开始观察到一个新的垃圾邮件活动，该活动传递了恶意附件，这些附件利用了对选举过程的怀疑。QBot银行木马运营商使用相同的劫持电子邮件线程技术，再次引发了主题为垃圾邮件的浪潮，诱使受害者受到恶意选举干扰附件的攻击。

【参考链接】

https://blog.malwarebytes.com/cybercrime/2020/11/qbot-delivered-via-malspam-campaign-exploiting-us-election-uncertainties/

16. 俄罗斯网络犯罪分子Aleksandr Brovko被判入狱8年

【概述】

俄罗斯网络犯罪分子亚历山大·布罗夫科（Aleksandr Brovko）因其在僵尸网络计划中的作用而被判入狱八年，该计划造成至少1亿美元的经济损失。

【参考链接】

https://securityaffairs.co/wordpress/110358/cyber-crime/aleksandr-brovko-sentenced-jail.html

17. 美国大选如火如荼，网络安全战局即将重塑?

【概述】

特朗普政府的国家网络战略呼吁利用经济的力量推动整个行业的网络安全改善，并在新兴领域制定和实施标准，比如抗量子公钥密码术。拜登说，网络威胁对美国的国家安全、选举廉洁和国家民主的健康构成越来越大的挑战。与此同时，他认为政府应该向科技公司施压，改革他们在隐私、监视和仇恨言论方面的做法。

【参考链接】

https://www.freebuf.com/articles/neopoints/254098.html

18. 前微软工程师被判9年监禁

【概述】

据司法部称，在今年早些时候因涉嫌18项刑事指控而被判有罪后，一名前微软软件工程师被判处有期徒刑9年。

【参考链接】

https://www.inforisktoday.com/former-microsoft-engineer-sentenced-to-9-years-in-prison-a-15340

19. 黑客可以通过观察你的肩膀移动来获取密码

【概述】

安全研究人员永远想出新的方法，并且常常用令人惊讶的方式来入侵您的数据和系统。我最近报道说，这样的研究人员如何通过将连接到望远镜的电光传感器对准灯泡来监视大约80英尺（25米）远的对话。如果您认为这是非同寻常的，请做好准备：研究人员认为他们可以通过在Zoom通话期间观察您的上臂动作来获取您的密码。

【参考链接】

https://www.forbes.com/sites/daveywinder/2020/11/07/surprising-new-zoom-hacking-threat-revealed-what-users-need-to-know/

20. 谷歌开发了一个应用程序，如果用户拖欠付款，可以锁定设备

【概述】

银行和信贷放贷机构一直以来都有相当一部分不良的公共覆盖，这要归功于如果人们拖欠贷款会发生什么。Google不会通过其最新的应用程序来寻求帮助，该应用程序旨在锁定那些无法使用智能手机融资付款的用户的设备。

【参考链接】

https://www.hackread.com/google-app-lock-devices-users-default-payment/

21. 勒索软件集团转向Facebook广告

【概述】

这已经很糟糕了，许多勒索软件帮派现在拥有博客，他们在其中发布从拒绝勒索款项的公司那里窃取的

数据。现在，一个犯罪集团已开始使用被黑客入侵的Facebook帐户公开运行广告，迫使其勒索软件受害者付款。

【参考链接】

https://krebsonsecurity.com/2020/11/ransomware-group-turns-to-facebook-ads/

22. 中国黑客集团利用新鲜DLL进行侧载攻击

【概述】

安全公司Sophos的一份报告指出，最近发现的一个中国黑客组织正在使用多种动态链接库攻击技术来针对东南亚的非政府组织，尤其是缅甸。

【参考链接】

https://www.inforisktoday.com/chinese-hacking-group-using-fresh-dll-side-loading-attack-a-15320

23. 美国司法部扣押了10亿美元与丝绸之路市场相关的比特币

【概述】

美国司法部（DoJ）宣布没收了10亿美元的比特币和其他加密货币。美国司法部声称，这些资金与如今运转不良的暗网市场丝绸之路有关。

【参考链接】

https://www.hackread.com/1-billion-silk-road-marketplace-bitcoin-seized/

24. 拜登的网络安全使命：重振势头

【概述】

网络安全有望成为较高白宫优先级时任总统当选人拜登上任。预计他将与打击网络攻击续约所需的关键国际关系。

【参考链接】

https://www.inforisktoday.com/blogs/bidens-cybersecurity-mission-regain-momentum-p-2966

25. Game Over？Capcom被勒索1100万美元

【概述】

老牌视频游戏发行商Capcom成立于1979年，是世界上生存最悠久的视频游戏制造商之一。Capcom在美国，欧洲和东亚都有业务，最著名的游戏包括《生化危机》、《街头霸王》、《鬼泣》、《怪物猎人》、《王牌律师》和《洛克人》。在11月4日的一份新闻稿中Capcom透露遭遇勒索软件攻击，被迫停止了部分运营，该事件影响了其电子邮件和文件服务器以及其他系统。Capcom声称没有发现证据表明客户信息受到了损害。

【参考链接】

https://www.aqniu.com/threat-alert/71121.html

26. 特朗普的竞选诉讼证据收集网站发生数据泄露

【概述】

特朗普竞选团队刚刚启动的DontTouchTheGreenButton.com网站发生了选民数据泄露事件。遭泄露的数据包括选民姓名，地址和唯一标识符。有报道称该网站存在SQL注入漏洞，所以黑客可以收集选民的SSN和出生日期。

【参考链接】

https://www.freebuf.com/news/254290.html

27. Microsoft Store游戏提权漏洞分析（CVE-2020-16877）

【概述】

本文描述了Windows特权提升漏洞（CVE-2020-16877），我在6月向微软报告了这一问题，该问题在10月进行了修复。通过这一漏洞，攻击者可以直接利用Windows处理Microsoft Store游戏过程中的缺陷实现攻击，最终在Windows 10系统上从普通用户提升到Local System权限。

【参考链接】

https://www.anquanke.com/post/id/221818

28. 针对Linux的勒索软件木马现身，属于RansomEXX变种

【概述】

近日卡巴斯基（Kaspersky）发现某已知勒索软件帮派部署了一种针对Linux

的文件加密木马。卡巴斯基安全研究员指出：“这是一个全新的文件加密木马，属于ELF可执行文件，能够对Linux电脑上的数据进行加密。该木马类似于现有的RansomEXX木马，后者在上周刚刚被用于攻击巴西法院以及美国和其他地区的目标。

【参考链接】

https://www.aqniu.com/threat-alert/71148.html

29. CVE-2020-14882：Weblogic Console 权限绕过深入解析

【概述】

2020年10月29日，360CERT监测发现 Weblogic ConSole HTTP协议代码执行漏洞 相关 POC已经公开，相关漏洞编号为 CVE-2020-14882,CVE-2020-14883，漏洞等级：严重，漏洞评分：9.8。远程攻击者可以构造特殊的HTTP请求，在未经身份验证的情况下接管 WebLogic Server Console，并执行任意代码。对此，360CERT建议广大用户及时将Weblogic 升级到最新版本。与此同时，请做好资产自查以及预防工作，以免遭受黑客攻击。

【参考链接】

https://www.anquanke.com/post/id/221752

30. 报告：CISA负责人期望白宫解雇他

【概述】

美国第一任和现任网络安全总监克里斯·克雷布斯（Chris Krebs）表示，特朗普政府对他对选举程序的保护感到愤怒。特朗普总统一直坚持认为，尽管缺乏证据，但选举期间普遍发生选民欺诈行为，并在许多州提起诉讼以质疑选举结果。路透社报道说，由于 CISA支持公正的选举程序，预计白宫将要求克雷布斯辞职。

【参考链接】

https://threatpost.com/report-cisa-chief-expects-white-house-to-fire-him/161185/

31. 打码平台背后，血汗工厂下的打码工人

【概述】

验证码就像互联网世界的守卫，拦截黑产恶意攻击，守护46亿网民安危，可是有一天，城内网民骗过守卫，开了后门，黑产大军涌入城内，各路牛鬼蛇神，各种坑蒙拐骗偷。打码平台，又被称作CAPTCHA farms，指在进行验证码人机测试时，将该请求发送到打码平台，由真实的人来完成。从而通过人肉众包的形式，帮助黑产团伙绕过验证码。

【参考链接】

https://www.freebuf.com/news/254659.html

32. 亚马逊起诉Instagram，TikTok影响者

【概述】

购此商品，获取此商品”：社交媒体影响者是亚马逊合法的十字准线，用于宣传亚马逊的一般商品，并承诺将获得禁止的假冒奢侈品。在亚马逊提起的诉讼中， Instagram和TikTok社交媒体影响者Kelly Fitzpatrick和Sabrina Kelly-Krejci是13名被告，他们声称他们参与了一个在线骗局，销售假冒奢侈品。

【参考链接】

https://threatpost.com/amazon-sues-instagram-tiktok-knockoff-scam/161233/

33. 网络犯罪转移到云中以加速数据混乱

【概述】

一份关于地下经济的报告发现，恶意行为者正在提供基于云的大量窃取数据，可通过方便的工具进行访问以对所提供的内容进行切片和切块。

【参考链接】

https://threatpost.com/cybercrime-cloud-accelerate-attacks-data-glut/161243/

34. 分析师警告：DDoS攻击可能激增

【概述】

分布式拒绝服务攻击今年没有引起太多关注。但是分析人士说，此类攻击可能在未来几个月内激增，并且有可能与勒索软件和其他类型的网络威胁一样造成破坏。

【参考链接】

https://www.inforisktoday.com/analysts-warn-ddos-attacks-likely-to-surge-a-15365

35. 即使在危机时期，我们也必须保护我们的隐私

【概述】

在COVID-19之后，减少自由可能是我们为提高安全性所必须付出的代价。随着各国放宽针对冠状病毒而施加的锁定限制，自由的权衡取舍可能是增加了民用数据的可访问性。在至少二十三个国家中，数十个“数字联系人跟踪”应用程序已被下载超过五千万次。

【参考链接】

https://www.forbes.com/sites/nikitamalik/2020/11/16/we-must--protect-our-privacy-even-during-times-of-crisis/

36. 攻击者针对“ Malmoke” Zloader攻击中的色情网站观众

【概述】

在各种色情网站上发现的虚假Java更新实际上下载了著名的Zloader恶意软件。网络罪犯欺骗成人网站访问者，包括bravoporn.com和xhamster.com等网

站，进行恶意攻击，将受害者重定向到提供恶意软件的恶意网站。

【参考链接】

https://threatpost.com/attackers-porn-malsmoke-zloader-attack/161277/

37. Capcom勒索软件攻击：游戏详细信息泄漏；没有支付赎金

【概述】

日本知名视频游戏公司Capcom在新闻稿中证实，它已成为11月初勒索软件攻击的受害者。怀疑是Ragnar Locker Gang负责了这次袭击。 该公司还确认，由于攻击者可以访问9名现任和前雇员的个人数据，机密销售报告以及其客户的财务信息，因此目前可能有35万个个人信息受到威胁。

【参考链接】

https://www.hackread.com/capcom-ransomware-attack-no-ransom-paid/

38. 赛门铁克2021年网络安全预测–展望未来

【概述】

有一个词描述了2020年的威胁态势。那个词：勒索软件。对于企业或组织而言，没有更大的威胁，或者对于2020年的网络罪犯而言，任何可赚钱的都没有。这是有一个简单的原因。勒索是有利可图的。网络犯罪分子正在努力使这些利润最大化。该博客着眼于未来以及对未来的预测。过去在这些预测中发挥了重要作用也就不足为奇了。尽管我们并非所有的预测都专门针对勒索软件，但它们都受到勒索软件驱动威胁态势的方向的严重影响。

【参考链接】

https://symantec-enterprise-blogs.security.com/blogs/feature-stories/symantec-2021-cyber-security-predictions-looking-toward-future

39. Android端Firefox引擎中的漏洞分析

【概述】

正好恰逢新版本安卓端火狐浏览器的问世，GitLabs的安全红队研究人员克里斯·莫伯利（Chris Moberly）报告了以下几个旧版本浏览器中存在的安全漏洞。

【参考链接】

https://www.anquanke.com/post/id/222389

40. 苹果被曝重大系统漏洞：root权限秒获取，新款MacBook、iPhone 12统统波及！

【概述】

11月18日消息，苹果换芯了，安全漏洞也来了。腾讯安全玄武实验室对外公布了他们近期发现的一个苹果的安全漏洞。据悉，这个漏洞不仅影响最新的基于M1芯片的 MacBook Air、MacBook Pro，也会影响今年新推出的 iPhone 12、iPhone 12 Pro 系列产品。同时这也是第一个公开的能影响苹果 Apple Silicon 芯片设备的安全漏洞。

【参考链接】

https://www.freebuf.com/vuls/255362.html

41. 我们渗透了一个IRC僵尸网络。这是我们发现的

【概述】

CyberNews.com调查小组针对IRC僵尸网络进行了渗透操作，并将其报告给CERT越南以帮助将其删除。为了收集有关IRC僵尸网络活动的有价值的信息，我们加入了其“指挥与控制”渠道，在那里我们遇到了负责运行受感染系统的整个网络的botmaster。我们还利用这次渗透机会来学习bot管理员的动机和IRC僵尸网络的可能目的。

【参考链接】

https://securityaffairs.co/wordpress/111170/malware/irc-botnet-hack.html

42. 英国电信安全法案将禁止华为

【概述】

英国政府提出的立法草案，将为该国电信提供商制定最低的、可执行的安全标准，并将对选择使用中国华为(Huawei)等高风险制造商设备的任何公司进行处罚。周二，英国首相鲍里斯·约翰逊(Boris Johnson)的政府推出了《电信安全法案》(Telecommunications Security Bill)。草案要求电信运营商对其网络和服务遵守具体的、最低的安全要求——这一要求将在未来通过二级立法加以详细说

明——政府表示，这将有助于“限制任何入侵造成的损害”。未达到安全标准的企业将面临高达10万英镑(13.4万美元)的罚款，继续不遵守安全标准的企业将面临高达年收入10%的罚款。目前，电信提供商制定了自己的安全标准。

【参考链接】

https://www.inforisktoday.com/uk-telecommunications-security-bill-would-ban-huawei-a-15445

43. 百度Android应用程序被捕获到收集用户详细信息

【概述】

中国科技巨头百度旗下的百度地图和百度搜索框，因被发现收集敏感用户信息，已于10月底从谷歌游戏商店下架。这两个应用程序是由帕洛阿尔托网络公司发现的，该公司使用一种基于机器学习(ML)的间谍软件检测系统对它们和其他泄露数据的应用程序进行识别。这两个应用程序在他们发现的时候总共有超过600万的下载量。数据采集代码是在百度推送SDK中找到的，用于显示两个应用内的实时通知。

【参考链接】

https://securityaffairs.co/wordpress/111402/mobile-2/baidu-android-removed-play-store.html

44. Instagram又泄露了未成年人的PII

【概述】

在至少一个月的时间里，在爱尔兰数据保护委员会调查Facebook是否未能保护儿童个人数据时，Instagram泄露了未成年人的电子邮件地址。Facebook已经解决了这个问题。这是Facebook第二次修复Instagram上的此类错误，这引发了人们对该公司保护个人数据的谨慎程度的质疑。施泰尔发现，Instagram将未成年人的电子邮件地址暴露在了通过网页浏览器而不是app浏览的Instagram个人资料的HTML源代码中。这些电子邮件地址属于那些将个人资料转换为商业资料的未成年人。斯蒂尔认为，这些电子邮件地址很容易就能被刮走。

【参考链接】

https://www.inforisktoday.com/instagram-leaked-minors-pii-again-but-now-its-fixed-a-15444

45. 索普拉·斯特里亚在勒索软件攻击后的巨大的经济损失

【概述】

据2020年10月的报道，法国著名IT服务提供商Sopra Steria证实，其系统在10月遭到勒索软件攻击，造成数千万美元的损失。这家总部位于巴黎的IT公司在最新的事件更新中承认，Ryuk恶意软件家族的一个新变种被用来攻击其系统。拉格纳的储物柜勒索团伙利用Facebook广告敲诈受害者该公司表示，它“迅速”阻止了勒索软件的攻击;这家it公司表示:“立即实施的措施使得将病毒控制在集团基础设施的有限部分，并保护其客户和合作伙伴成为可能。”该公司承认，勒索软件攻击对其营业利润率造成了负面影响，其营业利润率保持在4000万至5000万欧元之间，而网络攻击的保险覆盖额为3000万欧元。

【参考链接】

https://www.hackread.com/sopra-steria-financial-loss-ryuk-ransomware-attack/

46. 拜登的总统竞选活动网站遭到土耳其黑客入侵

【概述】

本周，因支持Biden-Harris总统竞选活动而建立的Vote Joe网站，遭到了土耳其黑客“RootAyyildiz”的入侵，黑客还在网站上挂出宣传信息页面。根据现有证据和该站点的存档快照显示，黑客的入侵时间已经持续超过24小时。2020年美国总统大选几天后，即11月9日左右，vote.joebiden.com网站重定向到iwillvote.com。但是，本周，Vote Joe网站遭到入侵并且网站被控制，并呈现了攻击者发布的土耳其语信息。

【参考链接】

https://www.inforisktoday.com/analysts-warn-ddos-attacks-likely-to-surge-a-15365

47. 黑客把小米扫地机器人变成窃听器

【概述】

一台被黑客入侵的智能扫地机器人能够监听主人的一言一行。黑客已经找到了办法，利用一种名为LidarPhone的技术，把智能扫地机器人中的导航

组件——激光雷达（LiDAR），变成激光麦克风。近日，马里兰大学和新加坡国立大学的学者用LidarPhone成功将小米公司热卖的“石头”（Roborock）扫地机器人变成了窃听器。LidarPhone攻击并不简单，需要满足某些条件。尽管存在诸多条件限制，研究人员表示，他们已经成功地从测试的小米扫地机器人的LiDAR激光雷达导航组件中记录和获取了音频数据。他们通过改变机器人与物体之间的距离以及声源与物体之间的距离，来测试LidarPhone技术对各种物体的攻击成效。

【参考链接】

https://www.aqniu.com/threat-alert/71301.html

48. 一次网络攻击使圣约翰市的IT基础设施瘫痪

【概述】

11月15日，加拿大圣约翰市遭到大规模网络攻击，整个IT市政基础设施遭到瘫痪。这次网络攻击导致整个城市网络关闭，包括城市网站、在线支付系统、电子邮件和客户服务应用程序。圣约翰市正在与联邦和省当局合作，从网络攻击中恢复过来。专家认为，此次袭击是由勒索软件团伙实施的，预计该市可能需要几周时间才能完全恢复运作。网络安全的‘最佳做法’，不公开提供可能进一步危及伦敦金融城地位的细节，包括攻击的有效性、受影响的系统以及遏制措施的成功等信息。”城市经理约翰·科林证实，没有证据表明黑客窃取了个人信息。截至今天，没有任何迹象表明个人信息被访问或转移。

【参考链接】

https://securityaffairs.co/wordpress/111259/cyber-crime/saint-john-cyber-attack.html

49. 亚太地区的选举网络威胁

【概述】

在民主社会中，选举是选拔国家元首和政策制定者的机制。有强烈的动机促使敌对国家了解人民和政党的意图和偏好，这些意图和偏好将塑造一个国家的未来之路，并减少可能获胜者的不确定性。Mandiant威胁情报部门定期观察网络间谍活动，认为这是在寻求与选举相关的信息，这些信息针对全球政府，民间社会，媒体和技术组织。我们还看到破坏性和破坏性的网络攻击以及旨在破坏目标政府并影响选举竞赛结果的宣传运动。2020年美国大选目前正引起人们对选举网络风险的关注，但2020年已经在全球举办了数十场大选，而且还会有更多选举。在亚太地区，这些选举包括台湾，印度，韩国和新加坡的选举。

【参考链接】

https://www.hackread.com/capcom-ransomware-attack-no-ransom-paid/

50. 直播平台里的“房间密码”的秘密

【概述】

近期，通过对虚假荐股平台的分析发现，此类诈骗存在一个共同的特征：均要求用户通过指定的直播间听课，而部分直播间需要输入房间密码才能进入。借助此类直播平台，诈骗团伙既可以营造出一种万人追捧直播间的假象，用户在直播间看到观众、点评、投票等数据都是伪造出来的。又可以将虚假的理财项目对接至直播间内，快速实施诈骗。研究还发现，此类直播平台不仅仅服务于荐股诈骗，在其他黑灰产业也有其踪影。

【参考链接】

https://www.anquanke.com/post/id/223225

51. 谷歌在2020年注册了创纪录的200万个钓鱼网站

【概述】

根据Atlas VPN分析的数据，自2020年初以来，谷歌已经注册了202万个钓鱼网站。根据谷歌的透明度报告，该科技巨头在2020年平均每周发现46000个新的钓鱼网站。数据还表明，这个问题在今年上半年尤为严重，在2月、4月、3月和5月的几周内，发现了超过50,000个新的钓鱼网站。

【参考链接】

https://www.forbes.com/sites/simonchandler/2020/11/25/google-registers-record-two-million-phishing-websites-in-2020/

52. 伪装成httpd的机器人瞄准Linux服务器

【概述】

来自Intezer的研究人员发现了一种广告软件和投币僵尸网络的新变种，自2012年起由Stantinko威胁者操作。2017年，ESET首次发现了Stantinko僵尸网络，当时它感染了全球约50万台电脑。根据Intezer发布的一项新的分析，Linux木马伪装成httpd，这是在Linux服务器上常用的Apache超文本传输协议服务器。

【参考链接】

https://securityaffairs.co/wordpress/111393/malware/stantinkos-linux-variant.html

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

安全月报

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

月报电子版下载/ http://www.nsfocus.com.cn/research/list_145_145.html