金融行业

6 月报
2021 年

安全月报

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

解读《数据安全法》，打开数据安全保护“新思路”

行业研究

如何评估安全运营能力转型成熟阶段？

什么是威胁狩猎的正确“姿势”？

新网银木马Bizarro 正在欧洲和南美地区肆虐

新型Smishing 钓鱼木马曝光：冒充Chrome 窃取用户信用卡信息

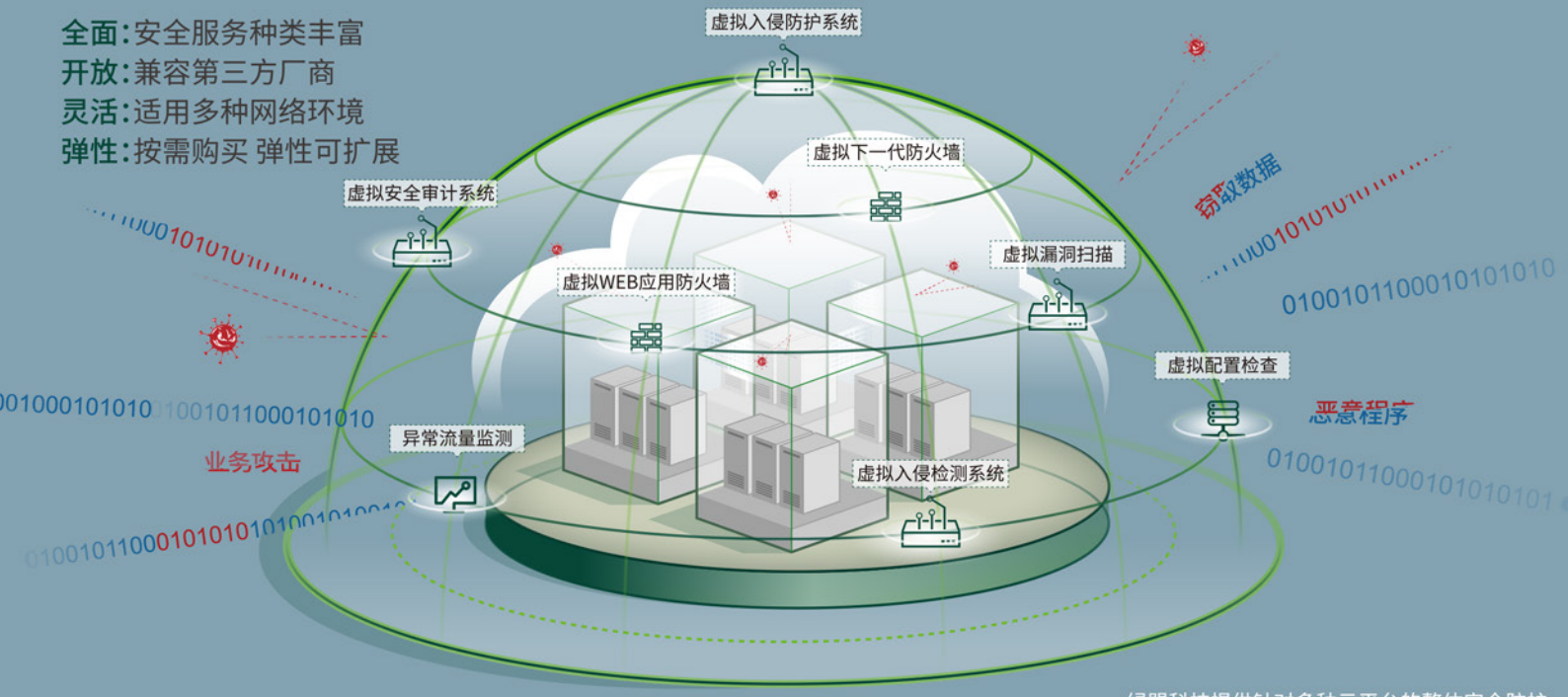
黑客团队搞瘫美国最大燃油管道后解散：已获得9000 万美元比特币

美国当局追回管道公司向黑客支付的230 万美元比特币赎金

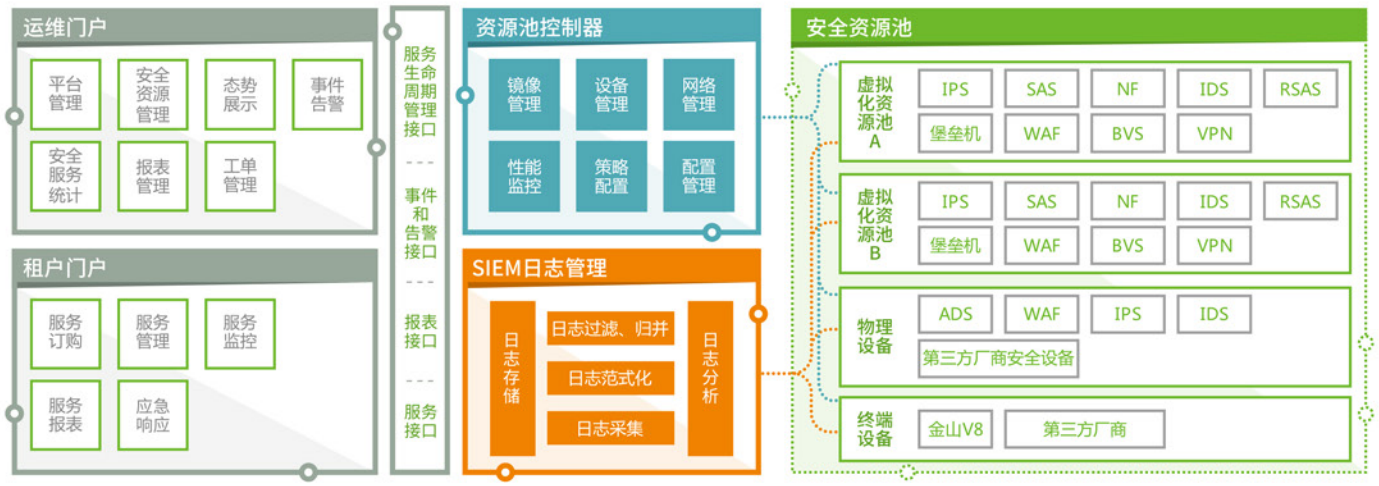
NSFOCUS

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《数据安全法》，打开数据安全保护“新思路”

2021年6月10日，十三届全国人民代表大会常务委员会第二十九次会议通过

2021年4月26日，十三届全国人大常委会第二十八次会议进行二审，完善数据分类分级和重要数据收集保护制度等内容

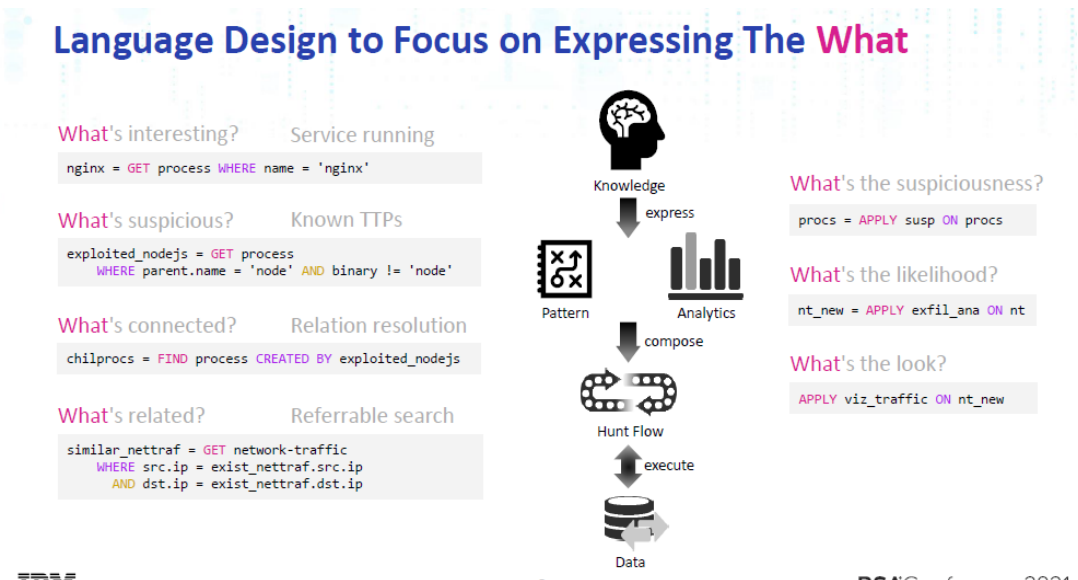
2018年9月7日，十三届全国人大常委会公布立法规划

2021年6月7日，十三届全国人大常委会第二十九次会议进行三审，增加了公共服务智能化、加大违法行为处罚力度等内容

2020年6月28日，第十三届全国人大常委会第二十次会议进行一审，面向社会公众征求意见

NSFOCUS

P18 什么是威胁狩猎的正确“姿势”？



安全月报

2021年第6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

NSFOCUS

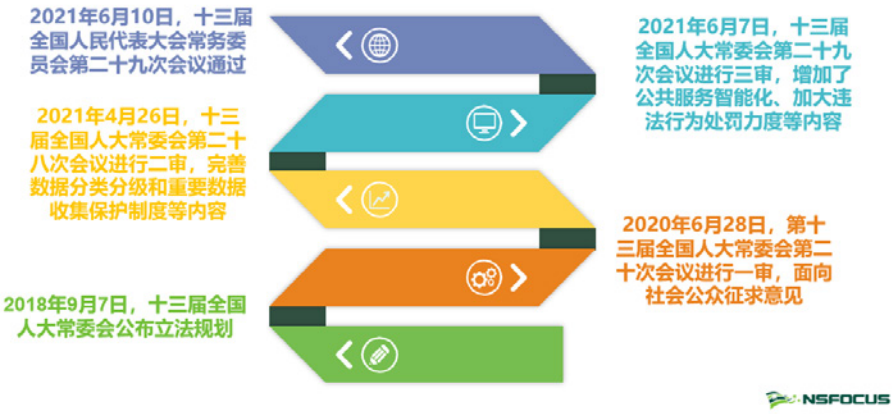
安全观点

解读《数据安全法》，打开数据安全保护“新思路”

绿盟解决方案中心 陈怀源

摘要：绿盟安全专家带你解读《数据安全法》

2021年6月10日，第十三届全国人民代表大会常务委员会第二十九次会议通过《中华人民共和国数据安全法》（简称《数据安全法》）。这部法律是数据领域的基础性法律，也是国家安全领域的一部重要法律，将于2021年9月1日起施行。



数据安全法的制定，是为了保障数据安全，促进数据开发利用，保护公民、组织的合法权益，维护国家主权、安全和发展利益。是维护国家安全的必然要求，是维护人民群众合法权益的客观需要，也是促进数字经济健康发展的重要举措。

为了能够更好的理解《数据安全法》条款，落地数据安全建设思路，绿盟科技对《数据安全法》作出更进一步解读，希望与广大安全从业者互相交流、共同探讨数据安全的最佳实践。

第一章　总则

本法对数据、数据处理、数据安全给出了明确的定义，从总体国家安全观的视角提出要求，规范数据处理活动，保障数据安全，促进数据开发利用，保护个人、组织的合法权益，维护国家主权、安全和发展利益。

1. 法律适用范围：

◆ 在中华人民共和国境内开展数据处理活动及其安全监管，适用本法。

◆ 在中华人民共和国境外开展数据处理活动，损害中华人民共和国国家安全、公共利益或者公民、组织合法权益的，依法追究法律责任。

2. 责任分工与权责：

◆ 一统领，三监管：中央国家安全领导机构负责国家数据安全工作的决策和议事协调，研究制定、指导实施国家数据安全战略和有关重大方针政策。工业、电信、交通、金融、自然资源、卫生健康、教育、科技等主管部门承担本行业、本领域数据安全监管职责；公安机关、国家安全机关负责各自职责范围内承担数据安全监管职责；国家网信部门负责统筹协调网络数据安全和相关监管工作。

◆ 各地区、各部门对本地区、本部门工作中收集和产生的数据及数据安全负责。

3. 数据安全开展：

◆ 建立健全数据安全治理体系，提高数据安全保障能力。鼓励开展数据处理活动，但不得危害国家安全、公共利益，不得损害个人、组织的合法权益。

◆ 相关行业组织按照章程，依法制定数据安全行为规范和团体标准。

◆ 任何个人、组织都有权对违反本法规定的行为向有关主管部门投诉、举报，同时对投诉、举报人的相关信息予以保密。

第二章　数据安全与发展

1. 总体原则：

国家统筹发展和安全，坚持以数据开发利用和产业发展促进数据安全，以数据安全保障数据开发利用和产业发展。

2. 战略要求：

◆ 国家实施大数据战略，推进数据的创新应用，省级以上人民政府制定数字经济发展规划。

◆ 国家支持开发利用数据提升公共服务的智能化水平，充分考虑老年人、残疾人的需求，避免对老年人、残疾人的日常生活造成障碍。

◆ 全面加强数据开发利用，鼓励产业发展。

◆ 推进数据开发利用技术和数据安全标准体系建设。

◆ 促进数据安全检测评估、认证等服务的发展。

◆ 建立健全数据交易管理制度。

◆ 数据开发利用和数据安全相关教育培训。

第十九条 国家建立健全数据交易管理制度，规范数据交易行为，培育数据交易市场。

解读

数据交易可以促进数据的流通，摆脱“数据孤岛”，发挥数据资源的经济价值。目前，在国内数据交易还面临着众多安全问题和挑战，需要规范数据资源交易行为，建立良好的数据交易秩序，促进数据交易服务参与者安全保障能力提升。

近年来，国内多地已开始率先探索大数据交易市场，如“贵阳大数据交易所”、“上海数据交易中心”、“北京国际大数据交易所”等。从交易市场化要素角度来看，其落地实施的相关配套细则并不完善，让数据发挥作用还需设计出配套制度。

相关标准的发布：

GB/T 37932《信息安全技术 数据交易服务安全要求》

GB/T 36343《信息安全技术 数据交易服务平台 交易数据描述》

GB/T 37728《信息技术 数据交易服务平台 通用功能要求》

第三章 数据安全制度

1. 数据分类分级与重点保护：

第二十一条

◆ 国家建立数据分类分级保护制度，依据危害程度，对数据实行分类分级保护。

◆ 各地区、各部门应当按照国家有关规定，确定本地区、本部门、本行业重要数据保护目录，对列入目录的数据进行重点保护。

解读

数据分类分级是数据安全防护的支撑与基础，有针对性的开展数据分级防护，从而减轻资金、人员、运维精力等综合投入成本。根据数据在经济社会发展中的重要程度和危害程度进行分类分级，前提是企业和组织要充分了解和掌握自身数据的类别、范围、业务系统、业务数据流转，才能更准确的形成重要数据保护目录，并做到针对性的重点保护。

相关标准的发布：

JR/T0158-2018《证券期货业数据分类分级指南》

JR/T0197-2020《金融数据安全数据安全分级指南》

GB/T39725-2020《信息安全技术 健康医疗数据安全指南》

YD/T3813-2021《基础电信企业数据分类分级方法》

2. 数据安全运营：

第二十二条

◆ 建立集中统一、高效权威的数据安全风险评估、报告、信息共享、监测预警机制。

解读

数据安全监督运营管理，以数据安全为中心，利用多种数据安全技术，从资产稽核、策略的优化、事件监测与处置等多维角度进行数据安全监督，7*24小时持续运营，保障数据活动的安全。

3. 数据安全审查与管制：

第二十三条、第二十四条、第二十五条、第二十六条

◆ 建立数据安全应急处置机制和数据安全审查制度。属于管制物项的数据依法实施出口管制。在与数据和数据开发利用技术等有关的投资贸易，对中国采取歧视性的禁止、限制或者其他类似措施的，中国可以根据实际情况对该国家或者地区对等采取措施。

解读

建立应急处置机制，旨在提升企业和组织的应急响应能力，提前发现安全隐患，及时解决问题，降低应急事件带来得不良影响。我们可以从应急准备、监测与预警、应急处置和总结改进四个阶段来建设。

数据安全审查制度，数据安全主管和监管部门，定期或不定期对各级企业和组织开展数据安全检查工作，从而协助各级企业和组织，了解自身的数据安全情况，找出潜在的数据安全隐患与不足，为以后的数据安全建设提供指导性意见。

对程序源代码、算法等技术资料做为出口管制的范围；针对国外敌对势力恶意或不公平对待我国合法的数据贸易投资，可依据本法予以反制。数据安全审计、出口管制与外交反制是国家对数据利益的保障，审计取证是必要的手段。

第四章　数据安全保护义务

1. 数据安全保障措施

第二十七条

◆开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务。重要数据的处理者应当明确数据安全负责人和管理机构，落实数据安全保护责任。

解读

依照国家法律法规及行业标准，结合企业自身的安全需求，从组织建设、人员能力、制度流程和技术工具四个维度，围绕数据生存周期（数据采集、数据传输、数据存储、数据处理、数据交换、数据销毁）及业务风险场景，按照资产梳理、分类分级、管理流程、技术能力及持续优化的步骤，建设数据安全治理体系。同时定期开展数据安全教育培训，加强全员数据安全防护意识，提升数据安全人员专业技能。

全面落实GB/T 22239《网络安全等级保护基本要求》中安全通用和安全扩展要求内容，做好物理环境、通信网络、区域边界、计算环境、管理中心等安全管理。

对相关业务系统、操作系统、数据库、大数据组件等进行漏洞扫描，及时升级补丁或采取补救措施；充分识别风险场景，对重大安全事件，采用技术手段及时发现及时处理上报。

2. 数据安全风险评估、数据出境、数据交易、取证调取

第三十条：

◆重要数据的处理者应定期开展风险评估，并向有关主管部门报送风险评估报告。

解读

数据安全风险评估在信息安全风险评估的基础上，更加重视数据资产本身的安全性，呈现出围绕数据资产、强调数据安全业务场景的特点。

通过数据资产梳理“摸清家底”，建立数据资产清单，是数据安全风险评估的基础，同时也是分类分级的基础。数据安全业务场景与数据生命周期相关联，不仅包括数据收集、传输、使用、存储、交换、销毁等过程，还包括数据的摘取、汇聚、共享外发等活动。每个数据类型都对应着多个业务场景，每个业务场景都存在着潜在的安全风险。

风险评估能够帮助企业/组织发现自身数据安全问题和短板，明确数据安全保护需求，为建设数据安全管理和技术手段指明方向，并给出解决方案。

第五章　政务数据安全与开放

1. 国家推进政务数据开放利用

第三十七条 第四十二条

◆ 提高政务数据的科学性，准确性，时效性

◆ 制定政务数据开放目录，构建统一规范，互联互通，安全可控的政务数据开放平台

解读

依照GB/T 39477《信息安全技术 政务信息共享 数据安全技术要求》，对政务信息共享安全框架、数据安全技术要求、基础设施安全技术要求三部分进行安全体系建设，增强政务信息共享交换的数据安全保障能力。

2. 对国家机关的要求

第三十八条至第四十一条

◆ 收集数据和使用数据应合法合规，对个人隐私、商密等信息依法保密。

◆ 建立健全数据安全管理制度，落实数据安全保护责任

◆ 委托他人建设、维护电子政务系统，存储、加工政务数据，受托方应当依照法律法规、合同约定履行数据安全保护义务，不得擅自留存、使用、泄露或者向他人提供政务数据。

◆ 依据公正、公平、便民的原则，及时、准确的公开政务数据。

解读

◆ 建立数据安全管理制度，落实数据责任制。

◆ 采用数据源鉴别、身份鉴别、访问控制、数据加密、数据防泄露等技术手段，对个人隐私、商密等数据进行安全防护。

◆ 国家机关应对受托方定期进行监督检查，包括但不限于受托方的数据安全管理制度、资质审核、签订服务合同、保密协议等内容。同时建立数据流转异常监测、用户行为管控、数据外发风险告警、数据追溯等防护能力，加强受托方在数据处理、数据存储等环节的审批。

◆ 受托方应定期开展安全自评估，满足国家机关的数据安全要求。对于未履行数据安全保护义务的，按照法律法规、合同中规定予以惩罚。

第六章　法律责任

本章主要对国家机关和国家工作人员，以及其他违反本法规定的，提出不同的处罚措施。

主体	违规行为	单位	负责人
组织、个人	未履行数据安全保护义务或未采取必要的安全措施	5-50万	1-10万
	拒不改正或造成大量数据泄露等严重后果的	50-200万	5-20万
	违反国家核心数据管理制度，危害国家主权、安全和发展利益的	200-1000万	
	违反本法第三十一条规定，向境外提供重要数据的	10-100万 情节严重的：100-1000万	1-10万 情节严重的：10-100万
	拒不配合数据调取的	5-50万	1-10万
	未经主管机关批准向外国司法或执法机构提供数据的	并处10-100万 造成严重后果的：100-500万	1-10万 造成严重后果的：5-50万
中介服务机构	进行非法来源数据交易	违法所得的1倍-10倍 10-100万	1-10万
国家安全机关 国家工作人员	未履行本法规定的数据安全保护义务的		依法处置

第七章　附则

国家秘密和军事数据不在此法范围内

◆ 国家秘密，适用《中华人民共和国保守国家秘密法》等。

◆ 军事数据，由中央军事委员会制定数据安全保护办法。

结语

《数据安全法》的出台发布，填补了我国在数据安全领域法律的空白，后续各行业主管和监管部门会陆续发布数据安全相关的标准、规范，完善和细化数据安全的实施办法与具体要求，指导企业和组织进行数据安全治理体系的建设，同时定期开展数据安全风险评估工作，排查安全隐患，及时采用数据安全技术措施保障数据安全，否则必将按照《数据安全法》依法严惩。

本文探讨了数据安全法的内容，对重要条款进行了解读，绿盟科技将致力于数据安全解决方案的落地，满足各行业客户的业务保障目标和政策合规要求，为客户在数据安全建设的道路上保驾护航。

NSFOCUS

行业研究

如何评估安全运营能力转型成熟阶段？
“多、准、快、稳”的提高网络安全弹性

摘要：“可度量”的安全运营能力

一、引言

度量是安全运营的重要部分，对安全过程的度量使运营工作有的放矢，对安全态势的度量使安全运营的成果可视化。

在2021 RSA大会中，《Building a Global Cyber Rating How to Objectively Rate Cyber Capabilities》列举了网络安全能力度量中常见的问题：缺少对网络安全风险的全局视角、缺少衡量风险的一致性方法、缺少不同组织间的比较基准、缺少业务角度的风险测量以及针对安全开支的判断能力等，导致评估结果无法充分发挥作用；此外，CRO、CISO、执行领导等多种角色在网络安全上有各自的关注点，单一维度的安全状态评估通常无法同时满足各相关方的需求；建议综合多个维度建立全局度量模型，形成可靠的评估结论。

《Building a Global Cyber Rating How to Objectively Rate Cyber Capabilities》

FireEye的议程《Your Metrics Suck! 5 SecOps Metrics That Are Better Than MTTR》则谈到传统的MTTR指标并不能有效地帮我们发现运营工作的缺陷，有意义的指标应为我们提供信心并推动变革。议程建议引入分析工作、健康度、过程偏差等指标，更有针对性地评估安全运营工作的有效性。

《Your Metrics Suck! 5 SecOps Metrics That Are Better Than MTTR》

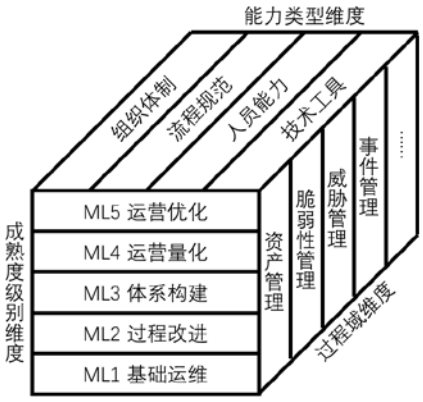
可见安全的模糊既是安全运营要解决的问题，也是安全运营本身存在的问题。同时，“智慧安全3.0”理念提出了全场景、可信任、实战化的特性，对安全运营提出更高的要求。

因此，我们提出网络安全运营能力成熟度模型，尝试客观地评估安全运营的能力，并能在运营能力建设和发展过程中作为参考。本文“网络安全”皆对应“Cybersecurity”，而不特指网络的安全。

二、模型概述

安全运营是为了实现组织的安全目标，提出安全解决构想、验证效果、分析问题、诊断问题、协调资源、解决问题并持续迭代优化的统筹管理过程，满足组织信息安全的动态性、持续性和整体性需求。对比“安全运营”与“安全”，我们认为安全运营是保持和提升安全状态与安全能力的过程。

国际上已经有多个比较完善的安全能力成熟度模型，例如CMMC、C2M2、NIST CSF、SSE-CMM。参考这些模型，我们在安全运营的语境下提出成熟度级别、过程域、能力类型三个维度，将安全运营能力划分为五个成熟度等级和多个过程域，各个过程域又从组织体制、流程规范、人员能力、技术工具四个方面拆分为基本实践，各自按照统一的方式评估过程成熟度。总体结构如下：



三、成熟度级别

参考CMM类模型，本模型包含的五个成熟度级别总体上按照基本执行、计划跟踪、充分定义、量化控制、持续改进的思路来划分，带入到安全运营的语境下。然而安全的持续改进本身就是安全运营的主要内容，因此级别的执行、定义、量化和改进也都是针对安全能力提升的过程，而不直接等同于安全（执行）过程。例如传统CMM的级别4要求实现过程的量化控制，而本模型在级别3要求实现安全执行过程的量化控制，因为这本就属于安全运营的核心能力，在级别4实现安全运营过程与结果的量化管理。各成熟度级别如下：

ML0 初始状态

无安全运营活动，安全能力不发展甚至可能随着威胁的发展而衰退。

一般特征：特事特例地执行安全工作，没有制度化。

注：这是没有开展安全运营工作的状态，不在五个成熟度等级内，为了明确区分也列在此处，基本对应SSE-CMM、CMMC等模型的一级。

ML1 基础运维

执行最基本的安全运营工作，由外部因素推动维持基础安全状态。

一般特征：

a. 被动、局部识别安全需求

b. 面向合规建设安全能力

c. 安全工作形成流程规范

d. 有计划地执行安全工作

e. 提供基本的资源保障

典型状态：根据合规要求部署了一些安全设备、设计了管理制度，定期巡检安全设备、处置发现的事件。

ML2 过程改进

有计划地执行部分安全运营工作，对安全提升有一定的主动投入，能确保基本的能力提升。

一般特征：

a. 识别主要网络安全威胁

b. 领导层牵头安全建设

c. 安全过程标准化

d. 安全过程包含改进环节

e. 为安全能力提升提供必要的资源

典型状态：安全设备和流程制度比较完备，有独立的安全团队，实现一些跨团队流程，能够识别执行过程的问题并尝试改进。

ML3 体系构建

全面建立安全运营体系，充分定义运营过程，管理和执行运营过程，有效提升安全状态。

一般特征：

a. 主动、全面地识别网络安全威胁

b. 系统地规划安全能力

c. 安全能力提升形成标准化过程

d. 对安全过程实现量化控制

e. 验证并保障安全机制的有效性

f. 安全工作成果可视化

g. 内外部相关方充分参与安全工作

h. 持续提升安全人员能力

典型状态：有一定规模的独立安全团队，建立了安全运营中心，有安全运营团队持续监控安全态势，根据数据定期评估、改进流程。

ML4 运营量化

对安全运营过程实现量化的认知和控制，可定量评估运营成果，实现安全与业务的同步发展。

一般特征：

a. 充分识别业务风险

b. 将业务目标转化为量化的安全目标

c. 形成系统的安全能力发展方法

d. 评估和控制安全能力提升过程有效性

e. 安全发展与业务发展保持同步

f. 体现安全对业务的支撑作用

典型状态：建立了较大规模的安全团队，岗位分工明确细致，实现了丰富的业务安全能力，积极引入安全运营的新技术新方法并有效应用，内外部安全数据被充分挖掘利用。

ML5 运营优化

持续有效改进运营过程。

一般特征：

a. 建立持续提升运营能力的机制

b. 在业务领域具备安全的开拓能力

c. 安全深度集成在组织的制度中

典型状态：建立了庞大的安全团队，安全能力长期保持在行业领先位置，能够按照业务发展方向准确识别和实现自身安全需求。

四、能力类型

模型从组织体制、流程规范、人员能力、技术工具四个能力类型出发量化过程能力。其中流程、人员、技术是业内普遍接受的安全运营组成部分，但在这三者组成的体系成立之前，还需要确定安全目标、资源调配、沟通协调等工作，因此模型增加了组织体制这一能力类型。

1. 组织体制：组织体制对于设计并实现安全运营体系的保障能力，如架构调整、资源保障、职责分配、业绩考核等。

2. 流程规范：安全运营过程相关的流程的规范性、完善性和有效性。

3. 人员能力：安全运营过程相关人员的专业能力和安全通识能力，以及相关的能力建设。

4. 技术工具：支撑安全运营中人员与流程运转以实现安全功能的技术或工具。

五、过程域

根据模型的关注点，由一般的安全运营工作总结梳理出15个过程域，每个过程域代表安全运营中的一类工作过程，各过程内容不重叠，但相互关联配合共同实现安全运营目标。

资产管理	脆弱性管理	威胁管理	事件管理	身份和访问管理
人员管理	数据与隐私保护	合规性管理	安全开发	安全数据与态势感知
信息共享与交流	供应链与外部依赖	安全制度与统筹	对抗能力管理	审计与追责

各过程域的内容在此暂不详细展开，仅以资产管理为例展示各成熟度级别下的实践内容。

PA01 资产管理

ML1 基础运维

组织体制

1. 安全策略包含资产管理

流程规范

2. 建立并维护资产清单

人员能力

3. 人员充分了解资产清单维护的过程

技术工具：无

ML2 过程改进

组织体制

1. 业务方配合资产管理流程

2. 建立事故处罚机制

流程规范

3. 建立资产基线并有计划地发现异常资产

4. 分析异常并调整资产管理策略

5. 建立资产上下线安全管理流程

6. 明确资产责任人

人员能力

7. 能够识别异常资产情况出现的原因

技术工具

8. 资产基线信息模板

9. 基于资产基线发现异常资产的技术

ML3 体系构建

组织体制

1. 设计覆盖资产管理的安全体系，并将资产管理纳入组织级制度

2. 资产管理纳入各相关方考评体系

3. 建立专职团队承担资产管理职责

流程规范

4. 基于业务情况建立资产分类分级管理规范和流程

5. 资产基线覆盖组件、版本、配置等详细信息并实施管理

6. 建立资产全生命周期管理流程

7. 建立资产管理过程的度量指标

8. 定期评估资产管理中各项措施的有效性

9. 资产管理流程标准化并覆盖全部相关方

10. 识别资产管理过程存在的问题并改进

人员能力

11. 建立覆盖资产管理的知识库

12. 能够基于流程和知识库评估资产级别

13. 能够评估资产变更可能产生的风险

14. 能够基于资产管理的记录结合业务情况发现制度存在的问题

技术工具

15. 识别资产组件、版本、配置等详细信息并与基线对比差异的技术

16. 支撑各相关方参与资产全生命周期管理流程的平台

ML4 运营量化

组织体制

1. 资产管理过程的改进效果纳入考评体系

2. 明确业务发展目标

流程规范

3. 将业务发展目标拆解为量化的资产管理优化目标

4. 评估知识库对资产管理的提升作用

5. 针对各项提升资产管理能力的过程建立度量指标

人员能力

6. 人员具备运营过程执行和管理能力

7. 人员具备针对运营过程建立度量模型的能力

技术工具

8. 准确、全面记录资产管理执行和改进过程数据的系统

9. 提供数据分析能力的系统

ML5 运营优化

组织体制

1. 设立长期安全目标

2. 设立运营优化岗位

流程规范

3. 持续分析业务演化对资产管理的需求

4. 持续评估资产管理提升机制的有效性

5. 基于业务和数据分析改进资产管理运营机制

人员能力

6. 运营体系优化设计能力

技术工具

7. 运营优化体制支撑技术与平台

总结

近年来网络安全环境快速变化，技术发展催生出云计算、大数据、工业物联网等安全新场景，威胁的演进导致勒索软件、供应链威胁等新形态，网络安全法、关基条例、数据安全法等法律法规相继出台，在国产化、新基建、数字化等浪潮中，客户需要能够灵活应对安全环境变化、快速响应、自适应的安全能力，而这正是安全运营要面对的问题。

围绕智慧安全3.0“全场景 可信任 实战化”的理念体系，我们也在重新审视和理解安全运营，本文的模型是一次初步的尝试，我们将在今后的运营工作中进一步探索、实践和完善。

什么是威胁狩猎的正确“姿势”？
——从 RSAC2021 看绿盟威胁狩猎（Threat Hunting）

绿盟科技威胁情报中心 孙建鹏、张宇娜

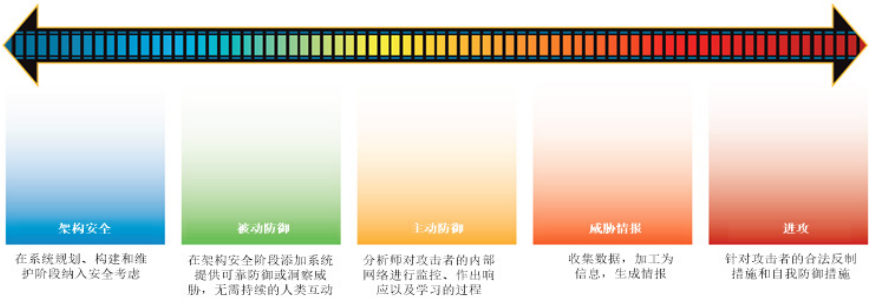
一、编者话

威胁狩猎依旧是2021RSA的热门话题，企业往往通过威胁狩猎发现已知遗漏威胁和未知威胁。本文结合2021RSA内容，总结了威胁狩猎的基础知识，并分享了绿盟科技的威胁狩猎体系。

二、概述

网络攻击技术和方法不断升级换代，攻击者从脚本小子、黑产犯罪团伙向国家级组织演进，攻击能力不断提高，攻击技术不断升级；威胁利用也从已知到未知不断发展变化。我们在NSA武器库泄漏事件中发现，AI技术的普及以及服务云化等技术让攻击门槛越来越低。随着攻击技术的演进，防守方也需要升级自身的防御方案。

SANS网络安全滑动标尺模型把整个安全建设划分为五个阶段：架构安全、被动防御、主动防御、威胁情报和反制。为了应对日益严峻的网络安全挑战，越来越需要防守方将自身安全建设从被动防御转换到主动防御、反制等主动安全的方向上来，而威胁狩猎技术就应运而生。

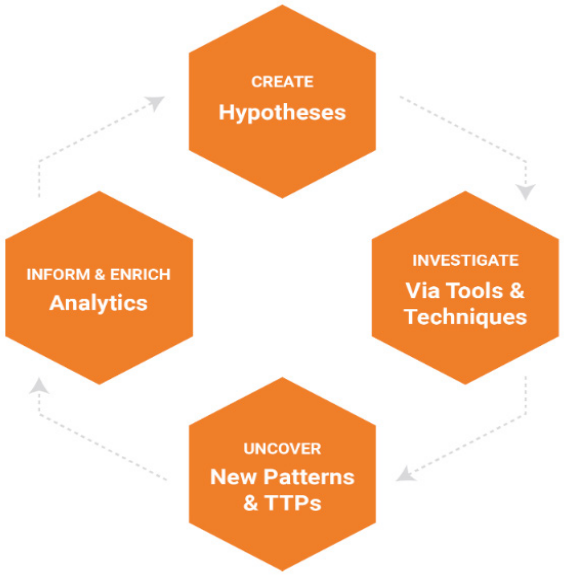


【图】SANS网络安全滑动标尺模型[1]

三、从RSAC2021看威胁狩猎

威胁狩猎是一种主动识别攻击痕迹的方法。有别于SOC、IDS、渗透测试和扫描，由威胁猎人利用威胁分析工具、威胁情报和大类实践经验来积极筛选、分析网络和端点数据，寻找可疑的异常或正在进行的攻击痕迹，去证明威胁假设。

从威胁狩猎的方法论来讲，威胁狩猎包含如下过程：



【图】威胁狩猎流程[2]

威胁假设：威胁猎人可以依赖于对自身资产的了解结合全网威胁情报对可能出现的高风险资产遭受的攻击进行假设；

攻击工具/技术调查取证：利用已收集的数据结合威胁情报，使用可视化、数据统计分析等方法对数据集进行挖掘与分析，获取攻击者的已知的或未知的攻击工具和攻击技术；

TTP发现与转换：狩猎的关键部分，结合威胁模型对已发现攻击者的攻击工具和攻击技术进一步挖掘，发现攻击者的TTP。

持续改进与自动化处置：上述步骤基本上都是由威胁猎人发起并参与的，发现已知或未知威胁的过程可以通过自动化处理，并改进狩猎过程。最终将整个狩猎过程标准化、程序化，形成完整的自动化TTP情报发现机制。

基于上述狩猎过程，通过不断的循环、迭代，形成越来越多和越来越完善的高级情报生产流程。

基于上述的威胁狩猎过程依赖于威胁数据，收集终端的操作数据、IDPS、WAF的告警数据、全流量设备的流量特征数据、威胁情报数据等等这些数据都是威胁狩猎过程中的基础。研究员需要从这些数据中分析出攻击者的战略、战术目标。

为了评估狩猎过程的成熟度，引入了狩猎成熟度模型。数据驱动的威胁狩猎成熟度模型是基于威胁狩猎框架，从数据收集能力、数据分析能力和自动化程度

来评估威胁狩猎能力。

HM0：有基本的IDPS威胁数据，但是数据并没有汇聚在一起。几乎无法分析；

HM1：能够把安全设备的告警数据汇聚在一起，但是没有更深一步的分析能力；

HM2：对收集的数据能够使用工具进行分析及基础的安全假设，并使用情报数据进行威胁狩猎；

HM3：能够建立有效的流程使用系统、工具，对收集的威胁数据基于威胁情报进行关联查询，对威胁进行狩猎；

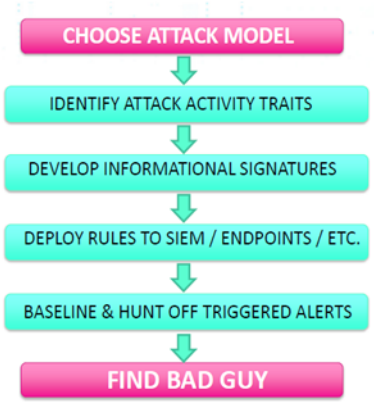
HM4：在HM3的基础上最大程度的使各个流程进行自动化，尽量减少人员的参与。

	HM0 初始阶段	HM1 最小规模阶段	HM2 流程化阶段	HM3 创新阶段	HM4 领导阶段
数据收集	很少，或者没有	能够收集IT环境中一些**关键节点**的数据	能够收集IT环境中**某些类型**的数据	能够收集IT环境中某些类型的数据	能够收集IT环境中某些类型的数据
建立假设	仅仅去处理SIEM/IDS/防火墙中的告警	根据**威胁情报**去构建新假设	根据威胁情报、**专家经验**去构建新假设	根据威胁情报、专家经验、**人工风险评分**去构建新假设	根据威胁情报、专家经验、**自动化**的风险评分去构建新假设
通过工具和技术去验证假设	在告警终端、SIEM中搜索，没有主动的调查	以**全文检索或者sql**的方式，利用**SIEM或日志分析工具**进行搜索	**基于现在的捕获流程**，利用**简单的工具**去搜索分析数据，来验证假设	**具备可视化和关联分析能力，构建新的捕获流程**	具备**高效的可视化和关联分析能力**，实现了新流程的**构建自动化**
检测模式&TTP	无，或者仅有SIEM/IDS告警	通过**金字塔底层的IOC**检测	通过金字塔**中层**和下层的IOC进行检测，并根据时间分析这些**ioc的趋势变化**	能够根据**对手的TTP**和金字塔**顶层的IOC**进行检测	**自动化的检测复杂TTP，追踪战役**，支持组织间的**情报IOC共享**
分析自动化	无	使用**威胁情报feed**进行自动化告警	**建立有效的捕捉流程库**，并定期运行	建立有效的捕捉流程库，并**经常**运行，具备**基础的数据分析能力**（基线、离群点分析）	**自动化的捕捉流程发布与构建，高水平**的数据分析能力（**机器学习**）

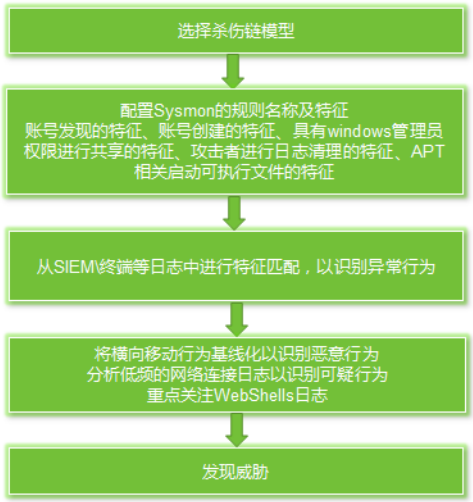
【图】威胁狩猎成熟度分级[2]

威胁狩猎技术路线大致可分为两类：基于流量进行狩猎和基于主机进行狩猎。RSA 2021大会中由来自美国的DLP厂商的CISO Tim Bandos分享的《Hunt

and Gather:Developing Effective Threat Hunting Techniques》主题，介绍了一个从无到有，怎样基于Sysmon、Shimcache、Autorun等主机侧的系统工具建立威胁狩猎体系。

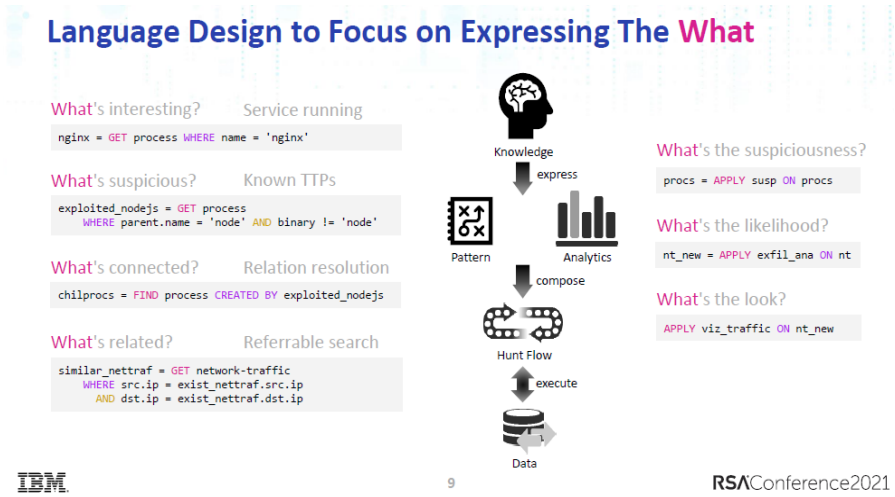


【图】狩猎过程



【图】以Sysmon为示例的狩猎过程

自动化程度是威胁狩猎成熟度的标志性特征，怎样从手工狩猎达到自动化狩猎呢？IBM的两位研究员推荐一个开源项目Kestrel，一种用于威胁狩猎的编程语言，提供了一套对狩猎目标进行描述的表达语法，威胁猎人只需输入狩猎目标，Kestrel会实时输出狩猎结果。Kestrel提高了自动化狩猎的程度，帮助威胁猎人进行更高效地狩猎。



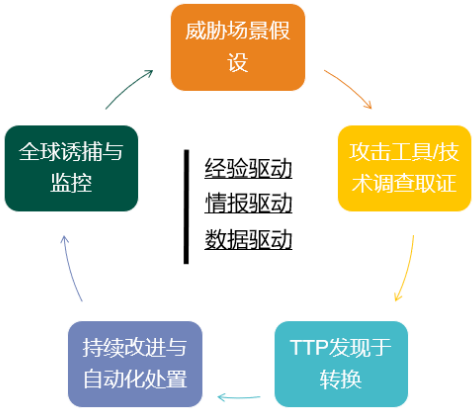
【图】 “狩猎目标”表达语法示例[3]

四、绿盟威胁狩猎体系

绿盟科技有着20余年的攻防经验，对威胁狩猎有着自己独特的理解和落地方式，下面会详细介绍绿盟的威胁狩猎体系。

4.1 绿盟威胁狩猎的循环和过程

威胁狩猎的核心首先是人，然后是数据，最后是自动化。绿盟科技能创中心，在威胁狩猎理论基础上加入了威胁诱捕和反制能力环节，通过对攻击者进行反制能够更充分的了解到攻击者的战略意图和战术目的，从而丰富和增强情报数据。狩猎活动基于经验、情报和数据三个维度驱动。绿盟科技在云端完整的运行了一套威胁狩猎流程，不断的增加狩猎规则完成狩猎过程，最终形成狩猎成果。



4.2 绿盟威胁狩猎体系

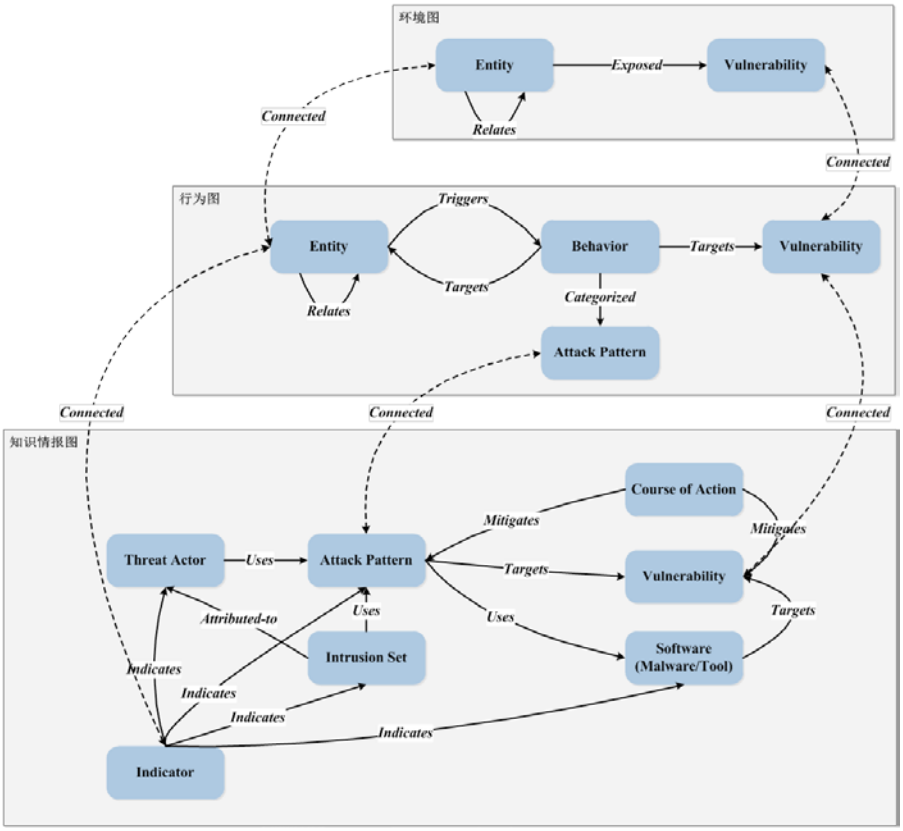
基于威胁场景的假设首先要建立在完善的狩猎体系中，才能在体系中进行后续的狩猎过程。绿盟科技威胁情报中心，依托完整的安全产品线设备和健全的安全服务能力建立完整的狩猎数据基础，借助多年积累的威胁情数据，结合安全研究院对攻防的理解和经验形成的知识库，建立完整的威胁狩猎体系，支撑从行为、风险、环境等多个维度进行威胁狩猎。

4.2.1基于假设的线索关联图分析

威胁假设并不是凭空进行假设，而是将资产、环境、知识、行为、告警、情报等数据，通过关联分析找出线索，使用线索进行威胁假设。

通常，数据中会包含攻击者攻击的结果、目标和使用手法，这些数据无序的分布在浩瀚的数据中。将所有的数据的威胁特征、行为特征结合产生的环境（战

场）进行特征抽取和数据归一，结合知识库和情报数据对威胁数据进行关联并提取可疑线索。线索包括攻击者的所处环境、使用手段、攻击技术等特征。研究人员通过这些线索特征大致推断攻击者的意图，并对威胁场景进行假设。



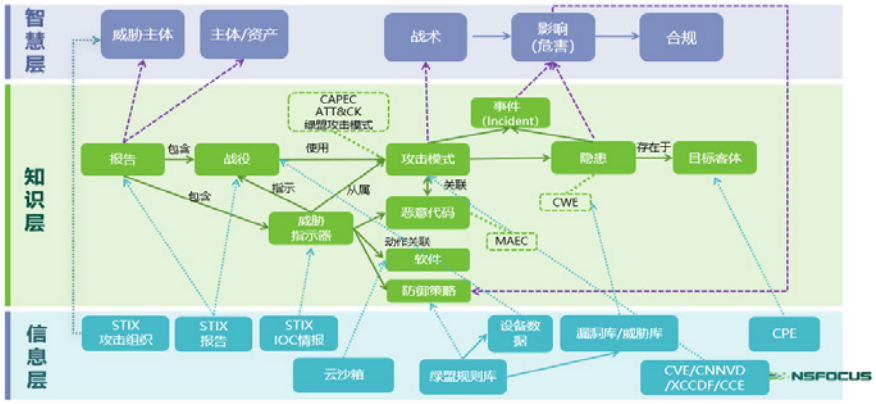
4.2.2情报知识库建立

绿盟科技威胁情报中心，依托多年的攻防经验和安全数据，基于知识组织层次模型进行情报知识库构建，自顶而下定义情报知识库框架，分为信息层、知识层和智慧层。

1）信息层作为知识库的基础，基于STIX2.0表示方法，使用云沙箱，威胁告警规则形成基础的知识库信息层。信息层抽象出21个知识本体和963481个知识实体；

2）知识层利用MITRE定义的ATT&CK框架利用信息曾数据，将攻击模式、威胁指示器、恶意代码、战役等情报数据进行关联抽象形成知识层；

3）智慧层描述了每次狩猎过程中验证完成的威胁主体（攻击者/组织），包括威胁主题的战略战术、影响和危害。



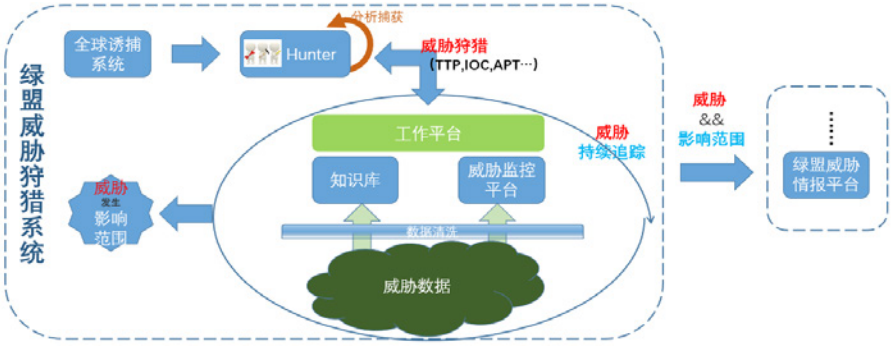
4.2.3全球诱捕系统

通过在全球范围内部署威胁诱捕系统，对攻击者/组织进行全方位的诱捕和监控。诱捕数据结合知识库通过威胁研判和分析，对已知攻击者进行实时监控，对未知攻击者进行及时发现。

诱捕节点遍布世界五大洲，涵盖了20多个国家致力于通过部署在不同的地区，更加全面的捕获威胁攻击，增强威胁狩猎能力。

4.2.4威胁狩猎系统

绿盟科技威胁狩猎系统的目标是能够让Hunter（威胁猎人）在一个统一的自动化平台上使用海量威胁数据完成威胁狩猎过程。使用工作平台检索威胁数据，结合知识库发现威胁关键线索，利用线索进行威胁假设，结合全球诱捕系统进行威胁狩猎系。狩猎成功后，将发现的已知或未知的威胁和影响范围以情报的方式输入至绿盟威胁情报平台。并将攻击者信息作为全球诱捕系统的输入对攻击者进行持续监控。



结束语

威胁狩猎是一个重要的威胁发现过程，狩猎的结果可以作为高可靠的情报供企业进行安全防护和威胁监控。绿盟科技情报中心自成立以来一直致力于对威胁的发现和感知，通过自研情报数据源、交换情报数据源、开源情报数据源每天产生超过千万级的高质量情报数据。威胁狩猎是自研情报数据源的重要一环。相信这些高质量的情报数据能够为广大客户的安全能力带来新的提升。

绿盟威胁情报中心（NSFOCUS Threat Intelligence center, NTI）是绿盟科技为落实智慧安全3.0战略，促进网络空间安全生态建设和威胁情报应用，增强客户攻防对抗能力而组建的专业性安全研究组织。其依托公司专业的安全团队和强大的安全研究能力，对全球网络安全威胁和态势进行持续观察和分析，以威胁情报的生产、运营、应用等能力及关键技术作为核心研究内容，推出了绿盟威胁情报平台以及一系列集成威胁情报的新一代安全产品，为用户提供可操作的情报数据、专业的情报服务和高效的威胁防护能力，帮助用户更好地了解和应对各类网络威胁。

参考

[1]【公益译文】网络安全滑动标尺模型–SANS分析师白皮书，绿盟技术博客，http://blog.nsfocus.net/sliding-scale-cyber-security/

[2] WHITE PAPER A Framework for Cyber Threat Hunting，@sqrrl

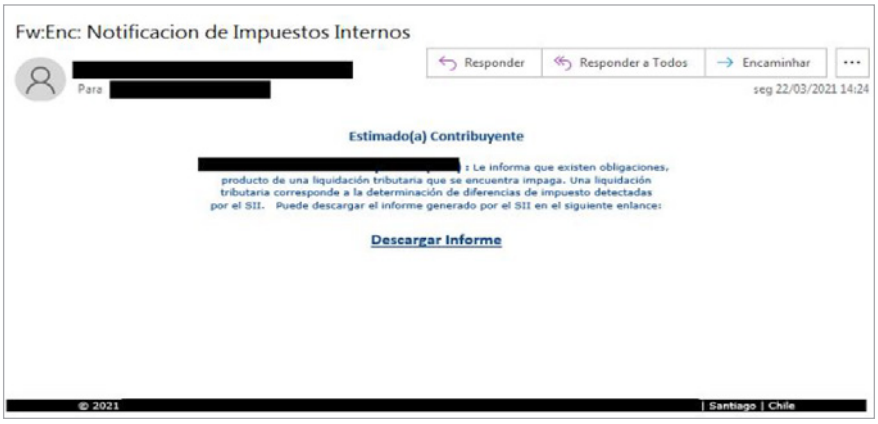
[3] RSAC 2021 《Introducing Kestrel:The Threat Hunting Language》

新网银木马 Bizarro 正在欧洲和南美地区肆虐

摘　要： 卡巴斯基警告称：一款被叫做Bizarro 的新网银木马，正在窃取欧洲和南美地区数十家银行客户的详细财务信息和加密货币钱包。就算你此前从未中招，也请务必小心提防此类恶意软件攻击。尽管最初起源于南美（据说来自有多个木马家族正在泛滥的巴西），但现在它已波及到包括阿根廷、智利、德国、西班牙、葡萄牙、法国和意大利等地的70多家不同的银行客户。

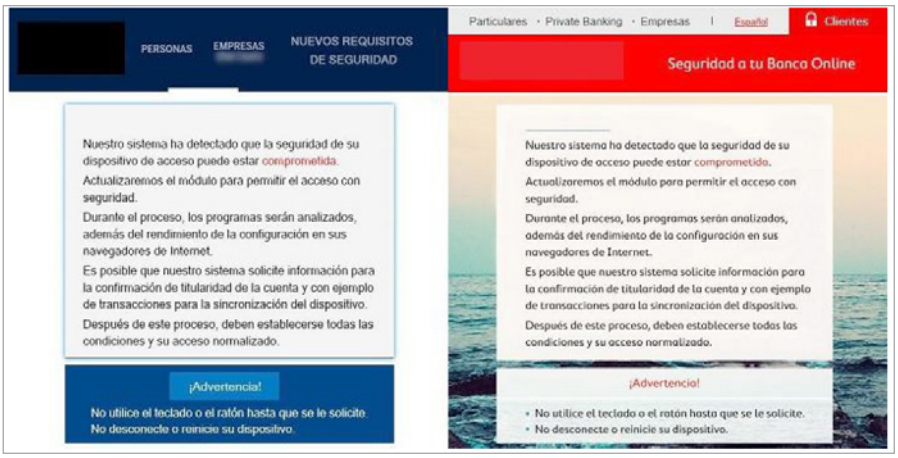
关键词： 标签（网银木马、Bizarro、卡巴斯基），技术问题（安全事件）。

内　容： 卡巴斯基研究人员通过遥测技术发现，他们已在不同的国家或地区见到了Bizarro 网银恶意软件的受害者，且受害者早就从南美波及到了欧洲本土。



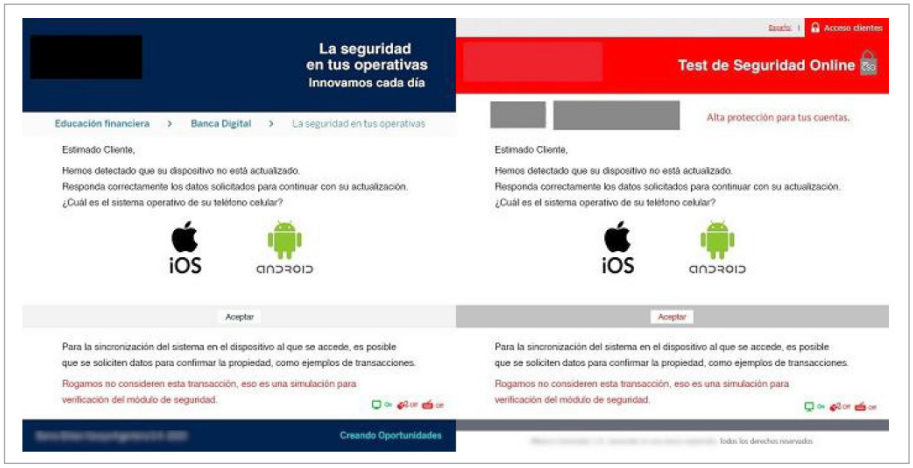
阻止登录网银，欺骗用户正在安装安全更新。

回顾历史，幕后攻击者可利用多种手段来窃取或诱骗受害者的数据，比如常见的社会工程学或网络钓鱼网站。



忽悠用户的系统已受到攻击

不过Bizarro 首选的还是通过嵌入嵌入垃圾邮件的恶意链接、或包含特洛伊木马的应用程序来引诱受害者上钩。

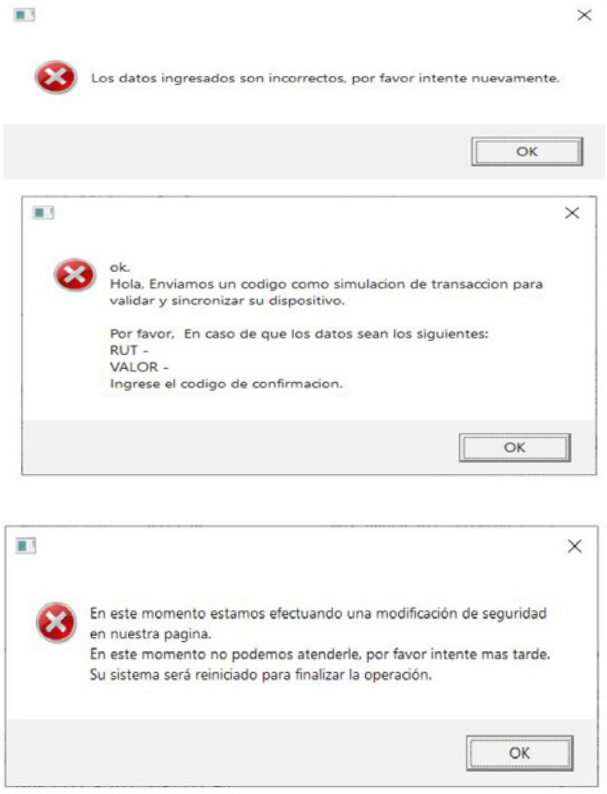


要求用户选择手机操作系统

在目标计算机上安装了恶意软件之后，Bizarro 会利用包含百余条指令的复杂后门程序，让攻击者能够窃取受害者的网银账户凭据。

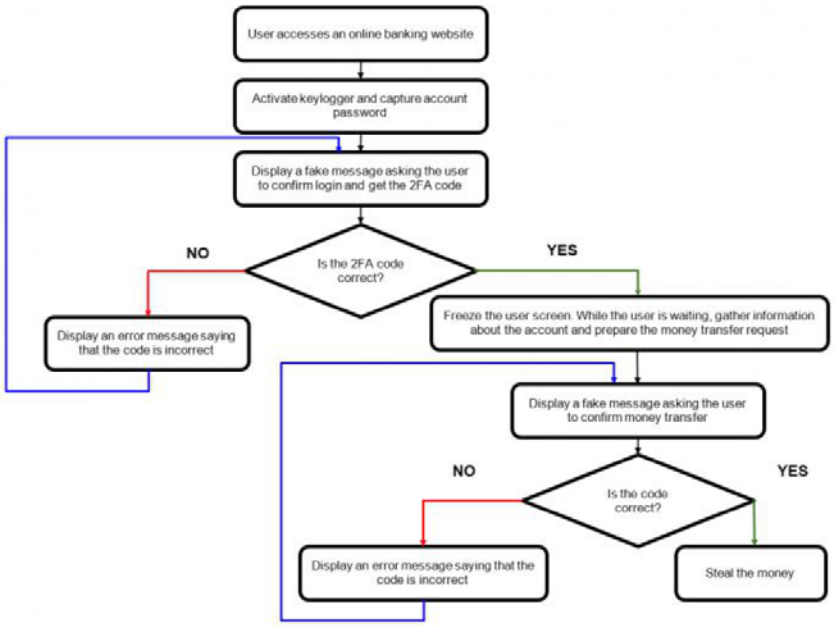
到了扫码这一步还没醒悟，基本意味着被攻击者吃定了。

卡巴斯基研究人员披露，Bizarro 后门中包含了用于操纵目标用户的各种命令，比如用于手机个人登录信息的键盘记录器。



诱骗受害者输入数据和系统需要重启的错误提示框

某些情况下，该恶意软件还可能使网络犯罪分子摸到受害者的加密货币钱包。



Bizarro 套路流程图

当然，这不是安全研究人员近期发现的唯一一款新恶意软件。因为从2021年3月下旬开始，TeaBot（又名Anatsa）就留意到了以Android 金融App 为目标的攻击事件。

信息来源：https://www.cnbeta.com/articles/tech/1130939.htm

新型 Smishing 钓鱼木马曝光：冒充 Chrome 窃取用户信用卡信息

摘　要：网络安全公司Pradeo 近日发现了一个先进的移动攻击活动，该活动利用网络钓鱼技术窃取受害者的信用卡信息，并使他们感染了一个冒充Android 端Chrome 浏览器应用程序的恶意软件。该恶意软件再利用受害者的设备作为载体，发送成千上万条钓鱼短信。

关键词：标签（钓鱼、安卓、恶意软件），技术问题（安全事件）。

内　容：网络安全公司Pradeo 近日发现了一个先进的移动攻击活动，该活动利用网络钓鱼技术窃取受害者的信用卡信息，并使他们感染了一个冒充Android 端Chrome浏览器应用程序的恶意软件。该恶意软件再利用受害者的设备作为载体，发送成千上万条钓鱼短信。Pradeo 的研究人员将其定性为Smishing 木马。

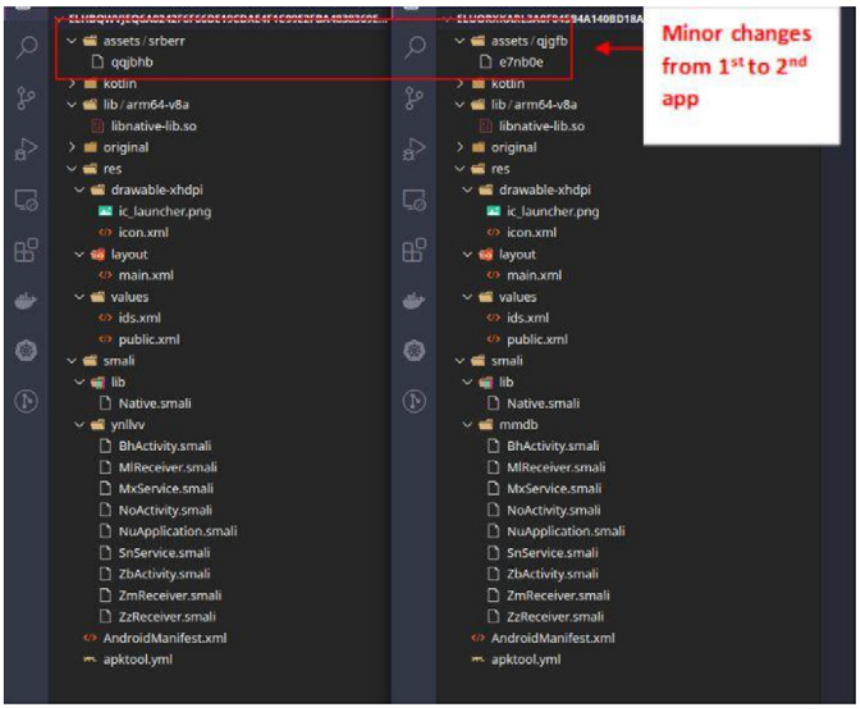
通过结合高效的网络钓鱼技术、积极传播的恶意软件以及绕过安全解决方案的方法，这个活动特别危险。安全公司Pradeo 评估，它的传播速度使它在过去几周内已经让数十万人受到影响。

首先，攻击者会向受害者发送要求支付海关费用以释放包裹的短信。当他们打开链接时，他们首先被哄骗去更新他们的Chrome 应用，但所谓的更新是一个恶意软件。

然后，他们被引导支付一小笔钱（通常最多1 或2 美元）。当他们这样做时，这种攻击背后的网络犯罪分子就得到了受害者的信用卡信息。

一旦用户安装虚假的Chrome 应用程序，那么每周就会通过受害者的设备发送超过2000 条短信，每天发送时间维持2 或3 个小时，向随机的电话号码发送，这些号码似乎是相互关联的。这种机制确保了攻击活动的成功传播。为了不被发现，该恶意软件通过使用官方Chrome 应用程序的图标和名称隐藏在移动设备上，但其软件包、签名和版本与官方应用程序没有任何共同之处。

```
# direct methods
.method static constructor <clinit>()V
    .locals 1

    const-string v0, "native-lib"

    invoke-static {v0}, Ljava/lang/System;->loadLibrary(Ljava/lang/String;)V

    return-void
.end method

.method public static native cr(Ljava/lang/Class;)Ljava/lang/Object;
.end method

.method public static native gs(I)Ljava/lang/String;
.end method

.method public static native hd([Ljava/lang/Object;)V
.end method

.method public static native set(Ljava/lang/Object;Ljava/lang/Object;)V
.end method

.method public static native st(Ljava/lang/Object;Ljava/lang/Object;Ljava/lang/Object;Ljava/lang/Object;)V
.end method
```



该活动正努力绕过现有的移动安全解决方案。首先，他利用受害者的电话号码加速发送钓鱼短信，以确保这些短信不会被短信应用程序的垃圾邮件过滤器所屏蔽。其次，该恶意软件使用混淆技术并调用外部代码来隐藏其恶意行为，因此躲过了大多数威胁检测系统。第三，一旦该应用程序被大多数杀毒软件识别并引用，网络犯罪分子只需用新的签名重新包装，就可以重新躲避扫描。

Pradeo 的引擎已经识别出两个假的Chrome 应用程序，作为该活动的一部分。当比较我们所分析的两个应用程序时，我们看到它们99%是相同的，只有一些文件名似乎被随机改变，另一方面它们的容量也是相同的。

信息来源：https://mp.weixin.qq.com/s/_qm0l7w_YYgno6-UsusVZg

所有 Wi-Fi 设备皆存在 FragAttacks 漏洞 个人信息可能因此遭窃

摘　要：新发现的Wi-Fi 安全漏洞统称为FragAttacks（碎片聚合攻击），影响所有的Wi-Fi 设备（包括电脑、智能手机和智能设备），最早可以追溯到1997 年。

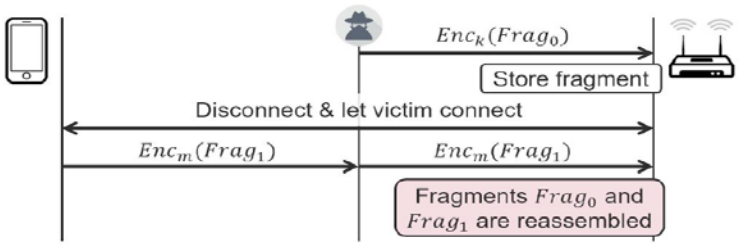
关键词：标签（Wi-Fi、FragAttacks），技术问题（安全事件）。

内　容：知名网络安全研究人员Mathy Vanhoef 发表一系列Wi-Fi 设备安全漏洞，这些漏洞被统称为FragAttacks，是碎片（Fragmentation）以及聚合攻击（Aggregation Attacks）的组合字，全球Wi-Fi 设备无一幸免，连最新的WPA3 规范都存在设计缺陷。位在受害者无线电范围内的攻击者，可以利用FragAttacks 漏洞窃取用户信息并且攻击设备。

FragAttacks 一系列的漏洞其中3 个来自Wi-Fi 标准中的设计缺陷，所以大多数的设备都受到影响，而更重要的是，Mathy Vanhoef 还发现了一些漏洞，这些漏洞是由Wi-Fi 产品中普遍存在的程序错误引起。经证实，每个Wi-Fi 产品都至少受一个FragAttacks 漏洞影响，并且绝大多数的产品都存在多个漏洞。

这些漏洞影响所有Wi-Fi 的安全协议，包括最新的WPA3 规范，甚至是Wi-Fi 最初的安全协定WEP 都在影响范围中，也就是说，从1997 年Wi-Fi 发布一样，这些设计缺陷已经成为Wi-Fi 的一部分。值得庆幸的是，设计缺陷难以被黑客利用，MathyVanhoef 提到，因为这些设计缺陷必须要有用户参与，才有可能被滥用，又或是只有在使用不常见的网络配置时，才有可能被实现。

因此FragAttacks 漏洞最大的隐忧，还是在Wi-Fi 产品的程序错误，其中几个漏洞可轻易地被恶意攻击者利用。



FragAttacks 漏洞包括了一个明文注入漏洞，恶意攻击者可以滥用实作缺陷，将一些恶意内容注入到受保护的Wi-Fi 网络中，尤其是攻击者可以注入一个精心建构的未加密Wi-Fi 讯框（Frame），像是透过诱使客户端使用恶意DNS 服务器，以拦截用户的流量，或是路由器，也可能被滥用来绕过NAT 或防火墙，进而使攻击者之后可以攻击本地端中的Wi-Fi 设备。

另外还有一些实作漏洞，例如即便发送者未通过身分验证，部分路由器也会将交握讯框发送给另一个客户端，这个漏洞让攻击者不需要用户交握，即可执行聚合攻击注入任意讯框。还有一个极为常见的实作错误，便是接收者不检查所有片段是否属于同一讯框，这代表攻击者可以混和两个不同讯框的片段，来伪造讯框。

即便部分设备不支持分段或是聚合功能，但是仍然容易受到攻击，因为这些设备会将分段的讯框，当做完整的讯框进行处理，在部分情况这可能会被滥用来注入数据封包。

Mathy Vanhoef 表示，发现这些漏洞很让人惊讶，因为在过去几年中，Wi-Fi 的安全性实际上应该获得改善。过去Mathy Vanhoef 团队所发现的KRACK 攻击，其后来加入的防御机制已经被证明其安全性，而且最新的WPA3 安全规范也获得安全性改进，但是本来可以被用来防止新发现的设计缺陷之一的功能，并未在实践中实际被采用，而另外两个设计缺陷则是在先前未被广泛研究的Wi-Fi 功能中被发现。

因此Mathy Vanhoef 也强调，即便是最著名的安全协议，都要仔细进行分析，定期测试Wi-Fi 产品的安全漏洞也是非常重要的工作。为了保护广大的用户，安全更新工作已经进行了9 个月，现在才对外揭露漏洞信息，漏洞修补工作由Wi-Fi 联盟和ICASI 进行监督，MathyVanhoef 提到，当设备还没接收到关于FragAttacks 漏洞的安全更新，用户要确保网站使用HTTPS 协议，并且尽可能安装所有可用的更新，以缓解部分攻击。

信息来源：https://www.cnbeta.com/articles/tech/1127089.htm

黑客团队搞瘫美国最大燃油管道后解散：已获得 9000 万美元比特币

摘　要： 黑客组织“黑暗面”（DarkSide）攻击了美国最大的燃油管道运营商后让其声名大噪，也因此宣布团队解散。不过，在解散前，其已经获得了巨额的加密货币。

据外媒报道，来自区块链分析公司Elicipat 的数据显示，黑客组织DarkSide在宣布解散前，其加密货币的账户中已经获得了至少价值9000 万美元的比特币。

关键词： 标签（燃油管道、勒索赎金），技术问题（安全事件）。

内　容： 黑客组织“黑暗面”（DarkSide）攻击了美国最大的燃油管道运营商后让其声名大噪，也因此宣布团队解散。不过，在解散前，其已经获得了巨额的加密货币。

据外媒报道，来自区块链分析公司Elicipat 的数据显示，黑客组织DarkSide在宣布解散前，其加密货币的账户中已经获得了至少价值9000 万美元的比特币。

近期，DarkSide 攻击了美国最大燃油管道公司Colonial Pipeline，导致其运输管道关闭了数天。最终，该公司向DarkSide 支付了价值500 万美元的加密货币赎金。

受此次事件影响，DarkSide 宣布该团队计划解散。据悉，这是因为迫于执法机构压力，该组织失去了对其运营架构的访问权限。

虽然该黑团组织已经解散，但是区块链分析公司Elicipat 在上周五表示，已经确定了该组织的加密货币账户，并且在解散前其账户中至少已经拥有价值9000 万美元的比特币。

Elicipat 表示，DarkSide 及其附属公司从47 个不同的加密货币账户中获得了至少9000 万美元的比特币赎金。平均来说，每个受害者支付了价值190 万美元的比特币。

而这9000 万美元的赎金中，有1550 万美元归DarkSide 的开发商所有，7470 万美元归其附属公司所有。其中大部分都被转移到加密货币交易所，并在那里兑换成法定货币。

不过，DarkSide 的加密货币账户中仍有价值530 万美元的加密货币没有来得及转移，并且这些加密货币有可能已经被美国执法机构查封。

值得一提的是，Colonial Pipeline 只是近期受到DarkSide 攻击的公司之一。

东芝公司的位于法国的一个部门表示，也受到了该黑客组织的攻击，并被盗取了740GB 的资料。此外，爱尔兰的医疗服务部门也遭到勒索软件攻击。

信息来源：https://news.mydrivers.com/1/757/757518.htm

美国当局追回管道公司向黑客支付的 230 万美元比特币赎金

摘　要： 美国执法官员表示，他们追回了支付给网络犯罪集团DarkSide 的价值230万美元的比特币，该网络犯罪集团参与了上月对美国最大燃油管道运营商Colonial Pipeline 的勒索软件攻击。

关键词： 标签（DarkSide、Colonial Pipeline、比特币），技术问题（安全事件）。

内　容： 美国司法部副部长丽萨-莫纳科（Lisa Monaco）在一次新闻发布会上说：“今天我们从DarkSide 那里扳回了一局，”并补充称，这笔钱是通过法院命令没收的。美国联邦调查局（FBI）副局长保罗-阿贝特（Paul Abbate）在发布会上解释称，该局的特工们确认了DarkSide 黑客用来从Colonial Pipeline 收钱的一个虚拟货币钱包。“通过执法机构，受害者的资金被从钱包中没收，以防止DarkSide 的人使用它们。”

FBI 拒绝透露具体是如何进入该比特币钱包的，理由是需要对情报技术保密。但负责此次行动的FBI 助理特别探员埃尔维斯·陈（Elvis Chan）告诉记者，即使是DarkSide 这样的外国网络犯罪分子，在犯罪过程中的某个时刻，也会使用美国的基础设施。一旦他们这样做，就给了FBI 一个收回资金的合法窗口。

据知情人士称，在上个月的袭击事件中，Colonial Pipeline 向黑客支付了价值近500 万美元比特币。目前尚不清楚这笔交易是何时进行的。

信息来源：https://www.cnbeta.com/articles/tech/1137895.htm

NSFOCUS

漏洞聚焦

Windows Print Spooler 权限提升漏洞（CVE-2021-1675）通告

发布日期 2021-06-09

一、漏洞概述

6 月9 日，绿盟科技CERT 监测到微软发布6 月安全更新补丁，修复了50 个安全漏洞，其中包括一个Windows Print Spooler 权限提升漏洞（CVE-2021-1675），此漏洞为绿盟科技天机实验室向微软报告并获得官方致谢。

Print Spooler 是Windows 系统中用于管理打印相关事务的服务，虽然微软在公告中将该漏洞标记为Important 级别的本地权限提升漏洞，但实际上在域环境中合适的条件下，无需任何用户交互，未经身份验证的远程攻击者就可以利用该漏洞以SYSTEM 权限在域控制器上执行任意代码，从而获得整个域的控制权。

我们认为该漏洞实际威胁等级较高，建议相关用户尽快采取措施进行防护，尤其是域控制器等服务器。

参考链接：https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-1675

二、影响范围

受影响版本

- ☐ Windows Server 2012 R2 (Server Core installation)
- ☐ Windows Server 2012 R2
- ☐ Windows Server 2012 (Server Core installation)
- ☐ Windows Server 2012
- ☐ Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
- ☐ Windows Server 2008 R2 for x64-based Systems Service Pack 1
- ☐ Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
- ☐ Windows Server 2008 for x64-based Systems Service Pack 2
- ☐ Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
- ☐ Windows Server 2008 for 32-bit Systems Service Pack 2
- ☐ Windows RT 8.1
- ☐ Windows 8.1 for x64-based systems
- ☐ Windows 8.1 for 32-bit systems
- ☐ Windows 7 for x64-based Systems Service Pack 1
- ☐ Windows 7 for 32-bit Systems Service Pack 1
- ☐ Windows Server 2016 (Server Core installation)
- ☐ Windows Server 2016
- ☐ Windows 10 Version 1607 for x64-based Systems

- ☐ Windows 10 Version 1607 for 32-bit Systems
- ☐ Windows 10 for x64-based Systems
- ☐ Windows 10 for 32-bit Systems
- ☐ Windows Server, version 20H2 (Server Core Installation)
- ☐ Windows 10 Version 20H2 for ARM64-based Systems
- ☐ Windows 10 Version 20H2 for 32-bit Systems
- ☐ Windows 10 Version 20H2 for x64-based Systems
- ☐ Windows Server, version 2004 (Server Core installation)
- ☐ Windows 10 Version 2004 for x64-based Systems
- ☐ Windows 10 Version 2004 for ARM64-based Systems
- ☐ Windows 10 Version 2004 for 32-bit Systems
- ☐ Windows 10 Version 21H1 for 32-bit Systems
- ☐ Windows 10 Version 21H1 for ARM64-based Systems
- ☐ Windows 10 Version 21H1 for x64-based Systems
- ☐ Windows 10 Version 1909 for ARM64-based Systems
- ☐ Windows 10 Version 1909 for x64-based Systems
- ☐ Windows 10 Version 1909 for 32-bit Systems
- ☐ Windows Server 2019 (Server Core installation)
- ☐ Windows Server 2019
- ☐ Windows 10 Version 1809 for ARM64-based Systems
- ☐ Windows 10 Version 1809 for x64-based Systems
- ☐ Windows 10 Version 1809 for 32-bit Systems

三、漏洞防护

3.1 官方升级

目前微软官方已针对支持的系统版本发布了修复该漏洞的安全补丁，强烈建议受影响用户尽快安装补丁进行防护，官方下载链接：

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-1675

注：由于网络问题、计算机环境问题等原因，Windows Update 的补丁更新可能出现失败。用户在安装补丁后，应及时检查补丁是否成功更新。

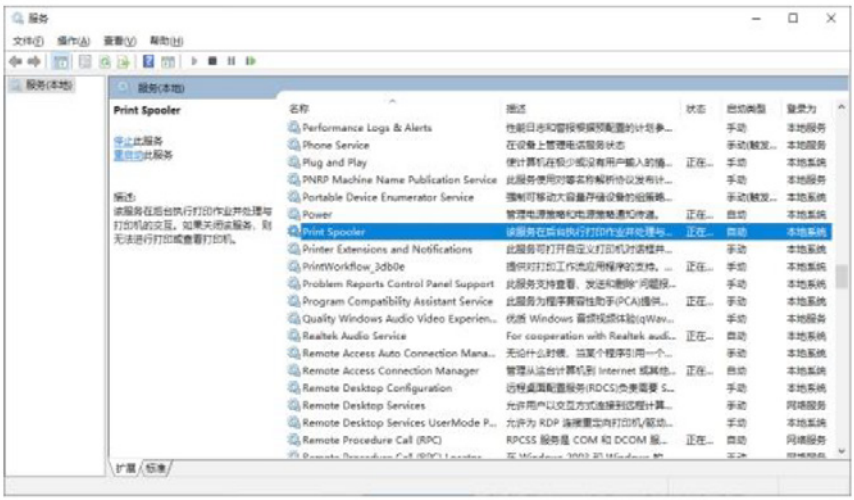
右键点击Windows 图标，选择“设置(N)”，选择“更新和安全”-“Windows 更新”，查看该页面上的提示信息，也可点击“查看更新历史记录”查看历史更新情况。

针对未成功安装的更新，可点击更新名称跳转到微软官方下载页面，建议用户点击该页面上的链接，转到“Microsoft 更新目录”网站下载独立程序包并安装。

3.2 临时防护措施

若相关用户暂时无法进行补丁更新，可通过禁用Print Spooler 服务来进行缓解：

一、在服务应用（services.msc）中找到 Print Spooler 服务。



二、停止运行服务，同时将“启动类型”修改为“禁用”。

声明

微软 5 月安全更新多个产品高危漏洞通告

发布日期 2021-06-09

一、漏洞概述

6 月 9 日，绿盟科技 CERT 监测到微软发布 6 月安全更新补丁，修复了 50 个安全漏洞，涉及 Windows、Microsoft Office、Microsoft Edge、Visual Studio 、SharePoint Server 等广泛使用的产品，其中包括远程代码执行和权限提升等高危漏洞类型。

本月微软月度更新修复的漏洞中，严重程度为关键（Critical）的漏洞有5个，重要（Important）漏洞有45个。请相关用户尽快更新补丁进行防护。完整漏洞列表请参考附录。

绿盟远程安全评估系统（RSAS）已具备微软此次补丁更新中大多数漏洞的检测能力（包括CVE-2021-31959、CVE-2021-31963、CVE-2021-33742 等高危漏洞），请相关用户关注绿盟远程安全评估系统系统插件升级包的更新，及时升级至 V6.0R02F01.2305，官网链接：http://update.nsfocus.com/update/listRsasDetail/v/vulsys。

参考链接：

https://msrc.microsoft.com/update-guide/en-us/releaseNote/2021-Jun

二、重点漏洞简述

根据产品流行度和漏洞重要性筛选出此次更新中包含影响较大的漏洞，请相关用户重点进行关注：

Windows MSHTML Platform 远程代码执行漏洞（CVE-2021-33742）：

Windows MSHTML Platform 存在远程代码执行漏洞，该漏洞由MSHTML的渲染引擎Trident 导致，未授权的远程攻击者可通过诱导用户打开特制文件或访问恶意网站进行利用，从而控制用户计算机系统，目前此漏洞已发现在野利用。

官方通告链接：

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-33742

Microsoft Defender 远程代码执行漏洞（CVE-2021-31985）：

Microsoft Defender 存在远程代码执行漏洞，该漏洞可绕过Defender 的防御策略，攻击者通过构造特制的二进制程序并诱导用户打开，即可在目标系统上执行任意代码。

官方通告链接：

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-31985

Microsoft SharePoint Server 远程代码执行漏洞（CVE-2021-31963）：

Microsoft SharePoint Server 存在远程代码执行漏洞，经过身份认证的攻击者可通过构造恶意http 请求执行反序列化攻击，从而接管目标服务器。

官方通告链接：

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-31963

Kerberos AppContainer 安全功能绕过漏洞（CVE-2021-31962）：

Kerberos AppContainer 存在安全功能绕过漏洞，此漏洞允许攻击者绕过Kerberos 身份验证，对任意服务主体名称进行身份验证。

官方通告链接：

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-31962

Windows Print Spooler 权限提升漏洞（CVE-2021-1675）：

Windows Print Spooler 存在权限提升漏洞，Print Spooler 是Windows 系统中用于管理打印相关事务的服务，微软在公告中将该漏洞标记为Important级别的本地权限提升漏洞，但实际上在域环境中合适的条件下，无需任何用户交互，未授权的远程攻击者就可以利用该漏洞以SYSTEM 权限在域控制器上执行任意代码。

官方通告链接：

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-1675

Microsoft Enhanced Cryptographic Provider 权限提升漏洞（CVE-2021-31199/CVE-2021-31201）：

Microsoft Enhanced Cryptographic Provider 存在两个权限提升漏洞（CVE-2021-31199/CVE-2021-31201），本地攻击者可以绕过Microsoft

Enhanced Cryptographic Provider 的安全限制读取和修改受限制的信息。这两个漏洞被攻击者用于与Adobe Reader 的漏洞（CVE-2021-28550）结合使用，攻击者通过诱导用户打开特制的PDF 文件，从而实现远程任意代码执行。目前已发现在野利用。

官方通告链接：

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-31199

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-31201

Windows NTFS 权限提升漏洞（CVE-2021-31956）：

Windows NTFS 存在权限提升漏洞，此漏洞为ntfs.sys 中基于堆的缓冲区溢出漏洞，经过身份认证的攻击者可通过运行特制的程序进行系统提权。攻击者通常通过诱导用户打开特制的文件来利用此漏洞。该漏洞由卡巴斯基的研究人员发现，并将其关联到PuzzleMaker Group，该组织将此漏洞与Windows Kernel 信息泄露漏洞（CVE-2021-31955）以及Chrome 远程代码执行漏洞结合使用，可实现Chrome 沙箱逃逸并获取目标系统权限。目前已发现在野利用。

官方通告链接：

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-31956

Microsoft DWM Core Library 权限提升漏洞（CVE-2021-33739）：

Microsoft DWM Core Library 存在权限提升漏洞，经过身份认证的攻击者可通过运行特制的程序进行提权。攻击者通常通过诱导用户打开特制的文件来利用此漏洞。目前该漏洞细节已公开，且已发现在野利用。

官方通告链接：

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-33739

三、影响范围

以下为重点关注漏洞的受影响产品版本，其他漏洞影响产品范围请参阅官方通告链接。

漏洞编号	受影响产品版本
CVE-2021-33742	Windows Server 2012 R2 Windows Server 2012 Windows Server 2008 R2 for x64-based Systems Service Pack 1 Windows Server 2008 for x64-based Systems Service Pack 2 Windows Server 2008 for 32-bit Systems Service Pack 2 Windows RT 8.1 Windows 8.1 for x64-based systems Windows 8.1 for 32-bit systems Windows 7 for x64-based Systems Service Pack 1 Windows 7 for 32-bit Systems Service Pack 1 Windows Server 2016 Windows 10 Version 1607 for x64-based Systems Windows 10 Version 1607 for 32-bit Systems Windows 10 for x64-based Systems Windows 10 for 32-bit Systems Windows 10 Version 20H2 for ARM64-based Systems Windows 10 Version 20H2 for 32-bit Systems Windows 10 Version 20H2 for x64-based Systems Windows 10 Version 2004 for x64-based Systems Windows 10 Version 2004 for ARM64-based Systems Windows 10 Version 2004 for 32-bit Systems Windows 10 Version 21H1 for 32-bit Systems Windows 10 Version 21H1 for ARM64-based Systems Windows 10 Version 21H1 for x64-based Systems Windows 10 Version 1909 for ARM64-based Systems Windows 10 Version 1909 for x64-based Systems Windows 10 Version 1909 for 32-bit Systems Windows Server 2019 Windows 10 Version 1809 for ARM64-based Systems Windows 10 Version 1809 for x64-based Systems Windows 10 Version 1809 for 32-bit Systems
CVE-2021-31985	Microsoft Malware Protection Engine < 1.1.18200.3
CVE-2021-31963	Microsoft SharePoint Foundation 2013 Service Pack 1 Microsoft SharePoint Server 2019 Microsoft SharePoint Enterprise Server 2013 Service Pack 1 Microsoft SharePoint Enterprise Server 2016

漏洞编号	受影响产品版本
CVE-2021-31962 CVE-2021-1675 CVE-2021-31199 CVE-2021-31201 CVE-2021-31956	Windows Server 2012 R2 (Server Core installation) Windows Server 2012 R2 Windows Server 2012 (Server Core installation) Windows Server 2012 Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) Windows Server 2008 R2 for x64-based Systems Service Pack 1 Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) Windows Server 2008 for x64-based Systems Service Pack 2 Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) Windows Server 2008 for 32-bit Systems Service Pack 2 Windows RT 8.1 Windows 8.1 for x64-based systems Windows 8.1 for 32-bit systems Windows 7 for x64-based Systems Service Pack 1 Windows 7 for 32-bit Systems Service Pack 1 Windows Server 2016 (Server Core installation) Windows Server 2016 Windows 10 Version 1607 for x64-based Systems Windows 10 Version 1607 for 32-bit Systems Windows 10 for x64-based Systems Windows 10 for 32-bit Systems Windows Server, version 20H2 (Server Core Installation) Windows 10 Version 20H2 for ARM64-based Systems Windows 10 Version 20H2 for 32-bit Systems Windows 10 Version 20H2 for x64-based Systems Windows Server, version 2004 (Server Core installation) Windows 10 Version 2004 for x64-based Systems Windows 10 Version 2004 for ARM64-based Systems Windows 10 Version 2004 for 32-bit Systems Windows 10 Version 21H1 for 32-bit Systems Windows 10 Version 21H1 for ARM64-based Systems Windows 10 Version 21H1 for x64-based Systems Windows 10 Version 1909 for ARM64-based Systems Windows 10 Version 1909 for x64-based Systems Windows 10 Version 1909 for 32-bit Systems Windows Server 2019 (Server Core installation) Windows Server 2019 Windows 10 Version 1809 for ARM64-based Systems Windows 10 Version 1809 for x64-based Systems Windows 10 Version 1809 for 32-bit Systems

漏洞编号	受影响产品版本
CVE-2021-33739	Windows Server, version 20H2 (Server Core Installation) Windows 10 Version 20H2 for ARM64-based Systems Windows 10 Version 20H2 for 32-bit Systems Windows 10 Version 20H2 for x64-based Systems Windows Server, version 2004 (Server Core installation) Windows 10 Version 2004 for x64-based Systems Windows 10 Version 2004 for ARM64-based Systems Windows 10 Version 2004 for 32-bit Systems Windows 10 Version 21H1 for 32-bit Systems Windows 10 Version 21H1 for ARM64-based Systems Windows 10 Version 21H1 for x64-based Systems Windows 10 Version 1909 for ARM64-based Systems Windows 10 Version 1909 for x64-based Systems Windows 10 Version 1909 for 32-bit Systems

四、漏洞防护

4.1 补丁更新

目前微软官方已针对受支持的产品版本发布了修复以上漏洞的安全补丁，强烈建议受影响用户尽快安装补丁进行防护，官方下载链接：

https://msrc.microsoft.com/update-guide/en-us/releaseNote/2021-Jun

注：由于网络问题、计算机环境问题等原因，Windows Update 的补丁更新可能出现失败。用户在安装补丁后，应及时检查补丁是否成功更新。

右键点击Windows 图标，选择“设置(N)”，选择“更新和安全”-“Windows 更新”，查看该页面上的提示信息，也可点击“查看更新历史记录”查看历史更新情况。

针对未成功安装的更新，可点击更新名称跳转到微软官方下载页面，建议用户点击该页面上的链接，转到“Microsoft 更新目录”网站下载独立程序包并安装。

五、附录：漏洞列表

影响产品	CVE 编号	漏洞标题	严重程度
Windows	CVE-2021-31959	Scripting Engine 内存泄露漏洞	Critical
Microsoft Office	CVE-2021-31963	Microsoft SharePoint Server 远程代码执行漏洞	Critical
Windows	CVE-2021-31967	VP9 Video Extensions 远程代码执行漏洞	Critical
Windows	CVE-2021-33742	Windows MSHTML Platform 远程代码执行漏洞	Critical
System Center	CVE-2021-31985	Microsoft Defender 远程代码执行漏洞	Critical
Windows	CVE-2021-1675	Windows Print Spooler 权限提升漏洞	Important
Windows	CVE-2021-26414	Windows DCOM Server Security Feature Bypass	Important
Microsoft Office	CVE-2021-26420	Microsoft SharePoint Server 远程代码执行漏洞	Important
Visual Studio Code - Kubernetes Tools	CVE-2021-31938	Microsoft VsCode KubernetesTools Extension 权限提升漏洞	Important
Microsoft Office	CVE-2021-31939	Microsoft Excel 远程代码执行漏洞	Important
Microsoft Office	CVE-2021-31940	Microsoft Office Graphics 远程代码执行漏洞	Important
Microsoft Office	CVE-2021-31941	Microsoft Office Graphics 远程代码执行漏洞	Important
Apps	CVE-2021-31942	3D Viewer 远程代码执行漏洞	Important
Apps	CVE-2021-31943	3D Viewer 远程代码执行漏洞	Important
Apps	CVE-2021-31944	3D Viewer 信息披露漏洞	Important
Apps	CVE-2021-31945	Paint 3D 远程代码执行漏洞	Important
Apps	CVE-2021-31946	Paint 3D 远程代码执行漏洞	Important
Windows	CVE-2021-31951	Windows Kernel 权限提升漏洞	Important
Windows	CVE-2021-31952	Windows Kernel-Mode Driver 权限提升漏洞	Important
Windows	CVE-2021-31953	Windows Filter Manager 权限提升漏洞	Important
Windows	CVE-2021-31954	Windows Common Log FileSystem Driver 权限提升漏洞	Important
Windows	CVE-2021-31955	Windows Kernel 信息披露漏洞	Important
Windows	CVE-2021-31956	Windows NTFS 权限提升漏洞	Important
.NET,.NET Core,Visual Studio,Microsoft Visual Studio	CVE-2021-31957	ASP.NET 拒绝服务漏洞	Important
Windows	CVE-2021-31958	Windows NTLM 权限提升漏洞	Important
Windows	CVE-2021-31960	Windows Bind Filter Driver 信息披露漏洞	Important

影响产品	CVE 编号	漏洞标题	严重程度
Windows	CVE-2021-31962	Kerberos AppContainer 安全功能绕过漏洞	Important
Microsoft Office	CVE-2021-31964	Microsoft SharePoint Server 欺骗漏洞	Important
Microsoft Office	CVE-2021-31965	Microsoft SharePoint Server 信息披露漏洞	Important
Microsoft Office	CVE-2021-31966	Microsoft SharePoint Server 远程代码执行漏洞	Important
Apps	CVE-2021-31980	Microsoft Intune ManagementExtension 远程代码执行漏洞	Important
Apps	CVE-2021-31983	Paint 3D 远程代码执行漏洞	Important
Windows	CVE-2021-33739	Microsoft DWM Core Library 权限提升漏洞	Important
Windows	CVE-2021-31199	Microsoft EnhancedCryptographic Provider 权限提升漏洞	Important
Windows	CVE-2021-31201	Microsoft EnhancedCryptographic Provider 权限提升漏洞	Important
Microsoft Office	CVE-2021-31948	Microsoft SharePoint Server 欺骗漏洞	Important
Microsoft Office	CVE-2021-31949	Microsoft Outlook 远程代码执行漏洞	Important
Microsoft Office	CVE-2021-31950	Microsoft SharePoint Server 欺骗漏洞	Important
Windows	CVE-2021-31968	Windows Remote DesktopServices 拒绝服务漏洞	Important
Windows	CVE-2021-31969	Windows Cloud Files Mini FilterDriver 权限提升漏洞	Important
Windows	CVE-2021-31970	Windows TCP/IP Driver 安全功能绕过漏洞	Important
Windows	CVE-2021-31971	Windows HTML Platform 安全功能绕过漏洞	Important
Windows	CVE-2021-31972	Event Tracing for Windows 信息披露漏洞	Important
Windows	CVE-2021-31973	Windows GPSVC 权限提升漏洞	Important
Windows	CVE-2021-31974	Server for NFS 拒绝服务漏洞	Important
Windows	CVE-2021-31975	Server for NFS 信息披露漏洞	Important
Windows	CVE-2021-31976	Server for NFS 信息披露漏洞	Important
Windows	CVE-2021-31977	Windows Hyper-V 拒绝服务漏洞	Important
System Center	CVE-2021-31978	Microsoft Defender 拒绝服务漏洞	Important
Microsoft Edge (Chromium-based)	CVE-2021-33741	Microsoft Edge (Chromium-based) 权限提升漏洞	Important

声明

NSFOCUS

安全态势

互联网安全威胁态势

行业动态回顾

1. Bizarro特洛伊木马针对多国银行进行攻击

【概述】

Bizarro是一种新银行木马，针对欧洲和南美数数十家银行用户，该木马可以捕获受害者的在线银行凭证并劫持比特币钱包。Bizarro木马通过Microsoft Installer程序包分发的，受害者从垃圾邮件中包含的链接中下载该程序，一旦点击启动，该恶意软件会杀死所有正在运行的浏览器进程，以终止与在线银行网站的任何现有会话，然后当受害者将重新启动浏览器并尝试访问家庭银行服务时，将被迫重新输入凭据，这些凭据将被恶意软件捕获。Bizarro还能够收集系统信息，包括计算机名称、操作系统版本、默认浏览器名称、已安装的防病毒软件。

【参考链接】

https://ti.nsfocus.com/security-news/4qYGR

2. Avaddon勒索软件团伙入侵金融机构

【概述】

Avaddon勒索软件团伙入侵了总部位于法国的金融咨询公司Acer Finance，并声称在开始泄露贵公司敏感信息之前，给Acer Finance 240小时与他们进行沟通。Acer Finance是一家投资管理公司，提供风险管理、共同基金、财务计划和咨询服务等。上周，联邦调查局（FBI）和澳大利亚网络安全中心（ACSC）警告说，正在进行的Avaddon勒索软件活动针对全球多个行业的组织，包括政府，金融，能源，制造业和医疗保健。

【参考链接】

https://ti.nsfocus.com/security-news/4qYGr

3. Simps僵尸网络感染IoT设备并发起大规模DDoS攻击

【概述】

新发现的恶意软件Simps利用已知的安全漏洞，与大量Gafgyt僵尸网络一起感染物联网设备。Simps是基于Linux僵尸网络，它针对易受攻击的物联网设备，例如华为路由器、Realtek路由器和ASUS设备，然后将其用于发起大规模DDoS攻击，并将下一阶段的有效负载下载到受感染的计算机。Simps是Keksec网络犯罪团伙使用的工具集的一部分。

【参考链接】

https://ti.nsfocus.com/security-news/4qYH3

4. macOS SMB服务器中的信息泄漏漏洞

【概述】

Cisco Talos最近在Apple macOS的SMB服务器上发现了一个可利用的整数溢出漏洞，可能导致信息泄露。服务器消息块(SMB)是一种在Windows网络环境中常见的网络文件共享，但是macOS包含它自己的服务器和客户端组件的专有实现。此漏洞编号：CVE-2021-1878是一个整数溢出漏洞，存在于macOS SMB服务器处理SMB3复合数据包的方式中。攻击者可以通过向目标SMB服务器发送特制数据包来利用此漏洞。除了能够看到敏感信息之外，攻击者还可以使用整数溢出来绕过加密检查并导致拒绝服务。

【参考链接】

https://ti.nsfocus.com/security-news/4qYGU

5. 云服务配置错误暴露超过1亿用户的数据

【概述】

在检查了23个Android应用程序之后，Check Point Research（CPR）注意到移动应用程序开发人员可能通过各种错误的第三方云服务配置来暴露超过1亿Android用户的个人数据。这些个人数据包括电子邮件、聊天消息、位置、密码和照片等，在威胁行为者的手中，这可能导致欺诈、身份盗用和服务刷卡（即在其他服务上使用相同的用户名和密码组合）。

【参考链接】

https://ti.nsfocus.com/security-news/4qYHi

6. 新WastedLocker变种利用Internet Explorer的缺陷

【概述】

一种名为wastdlocker的新型恶意软件变种正在利用Internet Explorer的两个漏洞向合法网站插入恶意广告，与之前的wastdlocker版本不同，新版本不包含勒索软件功能，只起到恶意软件下载的作用。攻击活动瞄准欧洲和美国的受害者。

【参考链接】

https://ti.nsfocus.com/security-news/4qYHk

7. 佛罗里达水处理工厂事件发现水坑攻击

【概述】

工控安全安全公司Dragos对佛罗里达州奥尔德斯马市水处理厂最近的网络攻击进行的调查中发现了一个水坑攻击，该攻击最初似乎是针对水处理基础设施的。执法部门在今年2月初透露，黑客获得了对奥尔兹玛（Oldsmar）水处理工厂系统的访问权限，并试图将某种化学物质的含量提高到可能使公

众面临中毒风险的程度。

攻击者利用了TeamViewer，因为该工厂的员工一直在使用TeamViewer远程监视和控制系统。由于密码共享和其他不良的安全做法，黑客很容易获得访问权限并开始在HMI中进行未经授权的更改。

【参考链接】

https://ti.nsfocus.com/security-news/4qYHg

8. 105款App违法违规收集使用个人信息

【概述】

近期，针对App非法获取、超范围收集、过度索权等侵害个人信息的现象，国家互联网信息办公室依据《中华人民共和国网络安全法》《App违法违规收集使用个人信息行为认定方法》《常见类型移动互联网应用程序必要个人信息范围规定》等法律和有关规定，组织对短视频、浏览器、求职招聘等常见类型公众大量使用的部分App的个人信息收集使用情况进行了检测。

【参考链接】

https://ti.nsfocus.com/security-news/4qYHu

9. REvil风云再起，APT式勒索爆发

【概述】

2021年5月，绿盟科技CERT监测到REvil/Sodinokibi勒索家族的多起活动，REvil为Ransomware Evil（又称Sodinokibi）的缩写，是一个私人勒索软件即服务（RaaS）组织。于2019年4月首次被发现，在一年内就已被用于一些知名网络攻击，2019年8月的PerCSoft攻击，2020年1月的Travelex勒索软件攻击，及2020年1月的Gedia Automotive攻击等事件。近期，该组织入侵了苹果公司的供应商，并窃取了苹果公司即将推出的产品机密原理图。多数网络安全专家认为，REvil是以前一个臭名昭著但已解散的黑客团伙GandCrab的分支。该推测源于REvil在GandCrab停止运营后立刻开始活动，且二者使用的勒索软件存在大量共享代码。

【参考链接】

https://ti.nsfocus.com/security-news/4qYIS

10. 音响设备巨头Bose遭勒索软件攻击

【概述】

Bose透露，2021年3月上旬他们经历了一场网络攻击，破坏了一些IT系统，并于2021年4月29日确定网络攻击的肇事者可能访问了少量内部电子表格，其中包括人力资源部门维护的管理信息。当时一旦发现攻击，Bose启动了必要的事件响应协议，包括其技术团队以防止恶意软件进一步传播，并加强对未经授权的活动的防御。受此次网络攻击影响的数据包括社会安全号码、员工姓名和薪酬数据。

【参考链接】

https://ti.nsfocus.com/security-news/4qYHY

11. 印度最大航空公司450万名乘客信息泄露

【概述】

2021年2月，印度最大航空公司—印度航空公司（Air India）的乘客服务系统提供商SITA遭遇黑客攻击。两个月后，印度航空公司披露，约450万乘客的信息遭泄露。印度航空公司称，此次泄露的数据范围是2011年8月至2021年2月期间登记的乘客数据，泄露信息包括姓名、信用卡帐号、护照、出生日期、联系信息、机票信息、星空联盟信息以及印度航空常旅客信息。

【参考链接】

https://ti.nsfocus.com/security-news/4qYHF

12. TeamTNT组织针对Kubernetes集群进行蠕虫式攻击

【概述】

以云计算为重点的密码劫持团队TeamTNT进行了蠕虫状攻击，跨多个Kubernetes群集破坏了大约50,000个IP。TeamTNT 是一个专注于云的加密劫持组织，他们经常针对受感染的云系统上的 Amazon Web Services 凭证文件来挖掘加密货币 Monero。由谷歌开发和支持的Kubernetes是采用最广泛的容器编排平台之一，用于自动化部署、扩展和管理容器化的应用程序。

【参考链接】

https://ti.nsfocus.com/security-news/4qYI7

13. 美国保险巨头CNA支付4000万美元勒索赎金

【概述】

美国最大的保险公司之一CNA Financial已经向勒索软件组织支付了4000万美元的赎金，原因是该公司的IT系统被勒索软件锁定，攻击者还窃取了数据。据悉，攻击CNA的勒索软件组织Phoenix使用的是Evil Corp编写的Hades勒索软件的变体—Phoenix Locker。

【参考链接】

https://ti.nsfocus.com/security-news/4qYI8

14. StrRAT伪装成勒索软件

【概述】

微软警告一场新的垃圾邮件活动使用基于java的StrRAT恶意软件的更新变体，该恶意软件将自己伪装成勒索软件感染，窃取机密数据，尽管它实际上并不加密数据。同时这种远程访问木马因其类似勒索软件的行为而臭名昭著，它会将文件扩展名.crimson附加到文件中，却不对文件进行加密，该扩展名可以防止用户双击打开文件，使攻击者能够进行快速而简单的勒索尝试，但微软指出，用户可以删除该扩展名来恢复他们的文件。

【参考链接】

https://ti.nsfocus.com/security-news/4qYHJ

15. 苹果修补了MacOS中允许偷拍屏幕的零日漏洞

【概述】

苹果已经修补了 macOS 中的一个严重错误，该错误可被利用来截取某人计算机的屏幕截图，并在该人不知情的情况下捕获他们在应用程序或视频会议中的活动图像。研究人员表示，他们发现 XCSSET 间谍软件正在使用该漏洞，跟踪为 CVE-2021-30713，专门用于在不需要额外权限的情况下截取用户桌面的屏幕截图 ，该漏洞通过绕过透明同意和控制（TCC）框架而起作用，该框架控制应用程序可以访问的资源，例如授予视频协作软件对网络摄像头和麦克风的访问权限，以便参加虚拟会议。

【参考链接】

https://ti.nsfocus.com/security-news/4qYHV

16. Agrius 组织利用磁盘擦除器攻击以色列

【概述】

Apostle 是一种独特且前所未见的磁盘擦除恶意软件，伪装成勒索软件，对以色列的不同目标发动破坏性攻击，主要针对网络基础设施。此次攻击活动由Agrius 黑客组织发起，该组织是与伊朗政府有关的，通常使用定制的工具集和现成的安全软件来部署定制的擦除器兼勒索软件或破坏性的擦除器变体，主要重点是数据破坏和网络间谍活动。

【参考链接】

https://ti.nsfocus.com/security-news/4qYHU

17. BazaLoader伪装成电影流媒体服务

【概述】

BravoMovies网站的功能包括伪造的电影海报和带有FAQ常见问题解答、以及可用来“取消”这项服务的Excel电子表格，但它下载的只是恶意软件BazaLoader。BazaLoader 是一种加载程序，用于部署勒索软件或其他类型的恶意软件，并从受害系统窃取敏感数据。BravoMovies 活动使用精心设计的感染链，与 BazaLoader 附属机构保持一致，这些附属机构诱使受害者跳过多个圈套以触发恶意软件负载，威胁行为者从一封电子邮件开始，告诉收件人除非取消他们对服务的订阅，否则他们的信用卡将被收取费用，这是他们从未签署过的订阅。

【参考链接】

https://ti.nsfocus.com/security-news/4qYI2

18. FBI证实JBS是被REvil勒索软件团伙攻击

【概述】

5 月 30 日，全球最大的新鲜牛肉加工商美国食品加工巨头 JBS Foods 因遭受网络攻击而被迫关闭全球多个地点的生产。网络攻击影响了该公司在全球的多个生产工厂，包括位于美国、澳大利亚和加拿大的工厂，攻击对位于这些地方的基础设施造成了严重影响。FBI将此次攻击归因于REvil（也被称为Sodinokibi）勒索软件团伙，此团伙是与俄罗斯有关。

【参考链接】

https://ti.nsfocus.com/security-news/4qYJz

19. Nobelium网络钓鱼活动冒充美国国际开发署

【概述】

微软发现SolarWinds使用群发邮件服务Constant Contact并冒充总部设在美国的开发组织，向150多个机构提供恶意URL。此攻击事件归因于Nobelium威胁组织，该组织历来针对范围广泛的机构，包括政府机构、非政府组织、智库、军队、IT 服务提供商、医疗技术研究机构、以及电信提供商。

【参考链接】

https://ti.nsfocus.com/security-news/4qYIR

20. WordPress插件高危漏洞被利用

【概述】

攻击者正在利用 WordPress 插件 Fancy Product Designer 中的一个关键零日漏洞，该漏洞允许远程执行代码。由于补丁尚未发布，该团队敦促用户立即卸载易受攻击的插件。攻击者可能正在利用插件中的关键远程代码漏洞上传恶意文件，尽管 WordPress 有一个内置的防火墙，但攻击者正在绕过它来利用该漏洞并在

尝试完全接管网站之前实现远程代码执行。由于这是一个受到主动攻击的关键零日漏洞，即使插件已停用，在某些配置中仍可利用。

【参考链接】

https://ti.nsfocus.com/security-news/4qYJr

21. 攻击者利用NativeZone后门进行网络钓鱼

【概述】

微软发布警告称，在设法控制了美国国际开发署(USAID)的电子邮件营销平台Constant Contact账户后，Nobelium组织当前正在进行网络钓鱼活动。此次网络钓鱼行动的目标是约3000个政府机构、军队、医疗和非政府组织有关的账户，大部分受害者位于美国，除此之外至少还涉及24个国家。

【参考链接】

https://ti.nsfocus.com/security-news/4qYIV

22. Scripps Health机构中超过14,7万名患者信息遭窃取

【概述】

Scripps Health 医疗机构遭勒索软件攻击，超过14.7万患者的个人财务信息和健康信息被勒索软件攻击者窃取，被窃取的数据包含姓名、地址、出生日期、健康保险信息、医疗记录编号、患者帐号和临床信息，例如医生姓名、服务日期和治疗信息，有不到2.5%患者，社会安全号码和驾驶执照号码也被泄露。Scripps Health 表示，迄今为止，没有迹象表明任何被盗数据已被用于实施欺诈。

【参考链接】

https://ti.nsfocus.com/security-news/4qYJI

23. Windows HTTP中高危漏洞也会影响WinRM服务器

【概述】

Windows IIS服务器的HTTP协议堆栈中存在一个可攻击的漏洞，该漏洞还可用于攻击未修补的Windows 10和公开暴露WinRM（Windows远程管理）服务的服务器系统。微软已经在5月补丁中修补了漏洞编号为CVE-2021-31166的严重漏洞。尽管该漏洞可能在远程代码执行（RCE）攻击中被威胁滥用，但该漏洞仅影响Windows 10和Windows Server的2004和20H2版本。Microsoft建议优先考虑修补所有受影响的服务器，因为该漏洞可能允许未经身份验证的攻击者，在易受攻击的计算机上远程执行任意代码。

【参考链接】

https://ti.nsfocus.com/security-news/4qYJE

24. Cisco修复了Webex等软件中的多个高危漏洞

【概述】

Cisco已解决其产品中的多个漏洞，包括 Webex Player、SD-WAN 软件和 ASR 5000 系列软件中的高风险缺陷，其中修复了影响 Windows 和 macOS 的 Webex 播放器的三个高严重性漏洞（CVE-2021-1503、CVE-2021-1526、CVE-2021-1502）。CVE-2021-1502、CVE-2021-1503 都是影响 Webex 网络录音播放器和 Webex 播放器版本 41.4 及以后的内存损坏漏洞。CVE-2021-1526 是一个内存损坏问题，攻击者可以利用该问题在受影响的系统上执行任意代码。

【参考链接】

https://ti.nsfocus.com/security-news/4qYJO

25. 日本中央省厅被黑，富士通SaaS平台成“攻击踏板”

【概述】

黑客通过入侵富士通的ProjectWEB平台，非法访问和窃取日本中央省厅和重要基础设施企业数据。ProjectWEB是富士通在2000年代中期推出的基于云的企业协作和文件共享平台，如今已被日本政府机构广泛使用，此次入侵事件也导致日本相关机构受损严重。受到影响的机构包括了日本中央省厅之一的国土交通省（Ministry of Land, Infrastructure, Transport and Tourism ）以及内阁秘书处、成田机场。

【参考链接】

https://ti.nsfocus.com/security-news/4qYII

26. 黑客袭击西班牙劳动和社会经济部

【概述】

西班牙劳动和社会经济部（MITES）周三遭到网络攻击，正在努力恢复受影响的服务。

MITES 是一个部级部门，年预算近 3900 万欧元，负责协调和监督西班牙的就业、社会经济和企业社会责任政策。

该部说："劳动和社会经济部受到计算机攻击的影响。我部和国家密码学中心的技术官员正在共同努力，以确定起源，并尽快恢复正常。

【参考链接】

https://ti.nsfocus.com/security-news/4qYKC

27. 神秘自定义恶意软件收集数十亿被盗数据点

【概述】

研究人员发现了一个1.2TB的被盗数据数据库，该数据库是两年内被一个未知的自定义恶意软件从320万台基于Windows的计算机中取出的数据。所包含的信息包括 660 万份文件和 2600 万份凭据，以及 20 亿个 Web 登录 Cookie，其中 4 亿个在数据库发现时仍然有效。

【参考链接】

https://ti.nsfocus.com/security-news/4qYKD

28. Exchange服务器成为 "Epsilon Red "恶意软件的攻击目标

【概述】

最近的研究表明，威胁攻击者使用了一套用作加密的PowerShell脚本部署了新的勒索软件，它利用未打补丁的Exchange服务器的漏洞来攻击企业网络。

Sophos首席研究员Andrew Brandt在网上发表的一份报告中写道，安全公司Sophos的研究人员在调查一家总部设在美国的酒店业公司的攻击时发现了这种新的勒索软件，并命名为Epsilon Red。

【参考链接】

https://ti.nsfocus.com/security-news/4qYKq

29. NCSC 警告针对学校的勒索软件攻击激增

【概述】

威胁行为者继续通过利用虚拟专用网络、未修补软件和设备中的漏洞以及使用网络钓鱼电子邮件来针对教育部门的组织。

目前还不清楚迄今已报告了多少案例，但2020年8月和今年2月首次发现袭击激增。截至2021年5月底/6月，NCSC调查发现针对英国学校、学院和大学的勒索软件攻击的又一次增加。

在NCSC观察到的大多数情况下，这些攻击导致学生课业和学校财务记录的丢失，以及与COVID-19测试有关的数据。

【参考链接】

https://ti.nsfocus.com/security-news/4qYKk

30. Siloscape：第一个已知的针对Windows容器危害云环境的恶意软件

【概述】

2021年3月，我发现了第一个已知的针对Windows容器的恶意软件，考虑到过去几年云计算应用的激增，这一发展并不奇怪。我将恶意软件命名为Siloscape（听起来像silo escape），因为它的主要目标是逃离容器，而在Windows中，这主要是由服务器silo实现的。

Siloscape是通过Windows容器针对Kubernetes群集的严重模糊恶意软

件。它的主要目的是打开一个后门进入配置不良的Kubernetes集群，以便运行恶意容器。

【参考链接】

https://ti.nsfocus.com/security-news/4qYK9

31. 黑客扫描利用CVE-2021-21985 RCE攻击的VMware vCenter服务器

【概述】

黑客正在积极扫描互联网上的 VMware vCenter 服务器，这些服务器容易受到 VMware 最近修复的关键 RCE 缺陷的影响。

【参考链接】

https://ti.nsfocus.com/security-news/4qYJW

32. 谷歌上的AnyDesk广告为用户提供恶意的应用

【概述】

著名的远程桌面应用程序AnyDesk在谷歌搜索结果中的广告中提供了该程序的一个恶意版本。该恶意版本的搜索排名甚至超过了合法的AnyDesk在谷歌上的广告排名。

该攻击活动自4月22日以来就一直很猖獗，值得注意的是，推送恶意广告的犯罪分子会设法避开谷歌的反恶意广告筛选监控。因此，Crowdstrike的研究人员估计，有40%的点击广告的用户已经安装了恶意软件。根据周三发表的一份关于该事件的报告，其中有20%的受害者可以使得犯罪分子对操作系统进行后续的操作。

【参考链接】

https://ti.nsfocus.com/security-news/4qYJY

33. 与中国有关的攻击者利用Pulse Secure 0 day安全漏洞入侵了大都会交通管理局（MTA）

【概述】

与中国相关的威胁行为者利用脉冲安全零日入侵了纽约市大都会交通管理局（MTA） 网络。入侵发生在4月，但袭击者没有造成任何损害，因为他们无法进

入MTA列车控制系统。管理局在Pulse Secure和美国CISA于4月发布公告，警告在野外积极利用这一缺陷的第二天就解决了这个问题。

【参考链接】

https://ti.nsfocus.com/security-news/4qYJV

34. 英特尔在CPU、蓝牙和安全系统中插入29个补丁

【概述】

英特尔发布了 29 条安全建议，以堵塞英特尔处理器的 BIOS 固件以及蓝牙产品、主动管理技术工具、NUC迷你 PC 系列以及具有讽刺意味的是，在其自己的安全库中的一些严重错误。

【参考链接】

https://ti.nsfocus.com/security-news/4qYKE

35. 谷歌修补了Android RCE的关键漏洞

【概述】

谷歌6月份发布的安全公告解决了Android和像素设备中90多个漏洞。

谷歌修补了影响像素设备和第三方安卓手机的安卓操作系统中的90多个安全漏洞，其中包括一个关键的远程代码执行漏洞，该漏洞可让攻击者霸占目标易受攻击的移动设备。

谷歌6月发布的安全公告称，该漏洞（CVE-2021-0507）存在于Android操作系统的系统组件中，可能使远程攻击者能够使用特制的传输在特权进程的上下文中执行任意代码。该公司表示，这是今年6月迄今为止修补过的漏洞中最严重的一个。

【参考链接】

https://ti.nsfocus.com/security-news/4qYKl

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/ https://www.nsfocus.com.cn/html/7/20/34/