金融行业

8 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

个人信息安全法律保护伞 |
《中华人民共和国个人信息保护法》解读

行业研究

筑牢国家安全屏障 |
《关键信息基础设施安全保护条例》浅析

深度解读 |《金融数据安全 数据生命周期安全规范》

金融行业供应链安全风险

Zimbra 新漏洞或造成 20 万家
企业数据泄漏

你的屏幕被“偷”了，新恶意软件
Vultur 已控制数千台设备

NSFOCUS

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

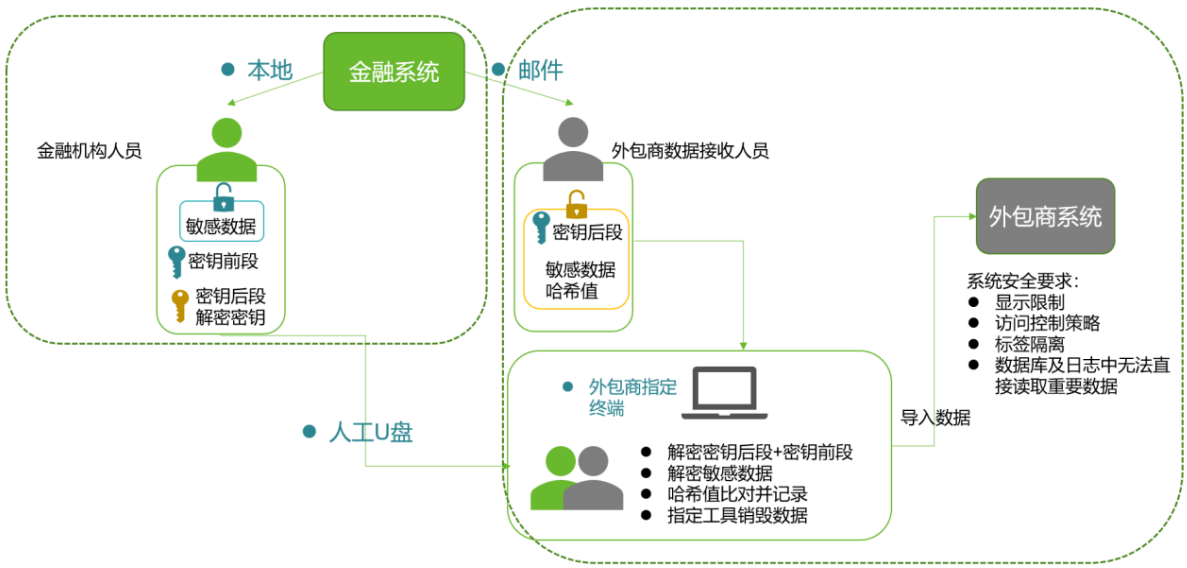
多年以来，绿盟科技致力于安全攻防的研究，为金融、政府、运营商、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。在这些巨人的背后，他们是备受信赖的专家。

NSFOCUS绿盟科技

本|期|看|点

P04 个人信息安全法律保护伞 | 《中华人民共和国个人信息保护法》解读

P28 金融行业供应链安全风险



安全月报

2021年第8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

个人信息安全法律保护伞 | 《中华人民共和国个人信息保护法》解读

——为个人信息的安全，撑起了法律“保护伞”

绿盟咨询设计部 曾令平

2021年8月20日，第十三届全国人民代表大会常务委员会第三十次会议通过《中华人民共和国个人信息保护法》（以下简称“《个人信息保护法》”）。自2020年10月以来，《个人信息保护法》历经三次审议与修订后，将于2021年11月1日正式施行。

1. 背景介绍

1.1 发布背景

最新数据显示：2020年中国网民总体规模已占全球网民的五分之一，2020年中国网民规模为9.89亿人。而互联网网站443万个，手机应用程序数量302万款。2021年以来，国家网信办对地图导航、运动健身、短视频等十多种类型的手机应用程序进行了检测。351款APP因违法收集个人信息被通报，25款因严重违法违规收集使用个人信息被下架。

“为及时回应广大人民群众的呼声和期待，落实党中央部署要求，制定一部个人信息保护方面的专门法律，将广大人民群众的个人信息权益实现好、维护好、发展好，具有重要意义。”全国人大常委会法工委副主任刘俊臣表示，制定个人信息保护法是进一步加强个人信息保护法制保障的客观要求，是维护网络空间良好生态的现实需要，也是促进数字经济健康发展的重要举措。

从现有颁布的法律来看，虽有部分内容与个人信息保护的相关，但在社会实践中，这些法律的适用大多规定的较为原则，并不能满足公民对个人信息保护的各类迫切需求。此外，纵观其他法规及规范性文件，例如《关于加强网络信息保护的决定》、《电信和互联网用户个人信息保护规定》、《信息安全技术 个人信息安全规范》（GB/T 35273—2020）等规定，虽然在司法案例中起到着极强的合规参考价值，但其同时也存在着一定的滞后性，并不能够适应各类互联网企业的合规需要。近年来，对个人信息滥用的案例不断涌现，对司法及行政监管部门也带来了较大挑战。

1.2 发展历程

自2003年起，我国就启动了保护个人信息的立法程序。经过了十几年不断摸索，个人信息保护立法才逐渐趋于完善。以下从几个重要时间节点进一步说明：

- 2003年，《个人信息保护法》专家建议稿开始起草，2005年初已经完成；
- 2009年，《刑法修正案(七)》第7条 非法提供与获取公民个人信息行为纳入刑法规制；
- 2013年，《电信和互联网用户个人信息保护规定》对“公民个人电子信息“做了界定，并明确了信息收集、使用的原则和相关规则；

- 2017年，《网络安全法》的实施，对“公民个人信息”进一步界定、对用户“知情同意”作出明确规定、对“网络运营者”提出明确要求；
- 2020年，《民法典》强调“以人为本”，加大了对公民隐私权和个人信息的保护力度；
- 2020年6月，全国人大常委会调整2020年度立法工作计划，个人信息保护法草案将提请审议。

《个人信息保护法》在2018年被列入全国人大常委会未来五年任期的立法议程中，经历了从2020年初次评审到2021年的二审、三审，《个人信息保护法》的具体内容也不断发生变化，具体变化情况详细请参见附录A三次审议稿全文对照。而关于《个人信息保护法》立法过程如下图所示：

1.3 法律地图

本文从国家法律、行政法规、司法解释、部门规章、技术规范五个层面入手，梳理国内数据安全与个人信息保护相关制度，整理形成可直观查看的“中国数据新秩序的法律地图”。

国内安全工作坚持总体国家安全观，在不同领域均有相关文件指导安全工作。其中与数据安全和个人信息保护领域相关性较强的有：民事领域通过了《民法典》；在网络空间安全领域，具有《网络安全法》、等保2.0系列标准、《网络安全审查办法》等；在数据安全领域：具有刚刚出台的《数据安全法》。在个人信息保护领域，具有刚颁布的《个人信息保护法》。在儿童个人信息领域、密码领域、网络犯罪、消费者权益保护、电子商务等领域也有专门立法。总体来说，《网络安全法》、《数据安全法》与《个人信息保护法》在总体国家安全观框架下，共同构成了我国数据新秩序下的三根支柱。

中国数据新秩序的法律地图

	总体国家安全观	刑法	消费者权益保护领域	电子商务领域	民事领域	网络空间安全领域	数据领域	个人信息领域	儿童个人信息领域	密码领域
法律	《中华人民共和国国家安全法》	《中华人民共和国刑法修正案》	《中华人民共和国消费者权益保护法》	《中华人民共和国电子商务法》	《中华人民共和国民法典》	《中华人民共和国网络安全法》	《中华人民共和国数据安全法》	《中华人民共和国个人信息保护法》	《中华人民共和国未成年人保护法》	《中华人民共和国密码法》
行政法规						《关键信息基础设施安全保护条例（国务院令第745）》	**国务院2021年立法工作计划：**数据安全管理条例	常见类型移动互联网应用程序必要个人信息范围规定		**国务院2021年立法工作计划：**商用密码管理条例（修订）
司法解释		两高关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释			最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定					
部门规章						·网络安全审查办法 ·计算机信息网络国际联网安全保护管理办法	·数据安全管理办法（征求意见稿）	·电信和互联网用户个人信息保护规定 ·个人信息出境安全评估办法（征求意见稿）	·儿童个人信息网络保护规定	
技术规范						·网络安全等级保护基本要求 ·网络安全等级保护实施指南 ·等等	·数据安全能力成熟度模型 ·数据出境安全评估指南 ·重要数据识别指南	·个人信息安全规范 ·个人信息安全影响评估指南 ·等等		·信息系统密码应用基本要求

2. 内容解读

2.1 标准概述

在信息化时代，个人信息保护已成为广大人民群众最关心最直接最现实的利益问题之一。《个人信息保护法》坚持和贯彻以人民为中心的法治理念，牢牢把握保护人民群众个人信息权益的立法定位，聚焦个人信息保护领域的突出问题和人民群众的重大关切。

全文共八章七十四条，明确了法律适用范围，聚焦目前个人信息保护的突出问题，在有关法律的基础上，该法进一步细化、完善个人信息保护应遵循的原则和个人信息处理规则，明确个人信息处理活动中的权利义务边界，健全个人信息保护工作机制。确立以“告知—同意”为核心的个人信息处理规则，落实国家机关保护责任，加大对违法行为的惩处力度。

2.2 七大关键点

2.2.1术语界定

《个人信息保护法》规定了三个术语定义和四个相关用语的含义，详细参考附录A，本文仅对“个人信息”、“敏感个人信息”、“个人信息的处理”和“自动化决策”的定义或含义做进一步解读：

- “个人信息”，其定义采取的是“识别”的方式，仅采取定义式的规定方式，好在已发布的《个人信息安全规范》进行了不完全列举。随着数据经济不断发展，本文大胆预测，有关个人信息的定义和范围也将再次被延申。
- “敏感个人信息”，该说法与《个人信息安全规范》中“个人敏感信息”措辞不同但所表示的内容基本一致，只不过本法中的“敏感个人信息”更加强调了“人格尊严”。值得关注的是，本法中也对列举的信息做了新增和调整：生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。
- “个人信息的处理”，相较于一审稿中主要变化在于删除了“活动”，强调了个人信息的处理动作或场景。
- “自动化决策”，主要变化在于主谓宾的顺序调整，强调了人工智能技术的重要应用对公民个人信息权益的影响。

2.2.2适用范围

本法明确了“我国境内”和“境外管辖”两大适用范围，“境外管辖”同等回应了欧盟GDPR、美国CCPA等国外立法的长臂管辖效力。

- 我国境内：在中华人民共和国境内处理自然人个人信息的活动，适用本法。
- 境外管辖：在中华人民共和国境外处理中华人民共和国境内自然人个人信息的活动，有下列情形之一的，也适用本法。
- 以向境内自然人提供产品或者服务为目的；
- 分析、评估境内自然人的行为；
- 法律、行政法规规定的其他情形。

2.2.3基本原则

在“第一章 总则：第一节 一般规定”部分，进一步明确了处理个人信

息的基本原则，本文参考相关法律法规，结合企业实践，总结了以下六大基本原则。

2.2.4“点”“面”“球”生态融合

本文从“点”、“面”、“球”构建个人信息保护生态融合体系，以达到相互影响、相互制约、相互信任、不断演变，并在一定时期内处于相对稳定的动态平衡状态。

- “点”：指全民守护，坚守基本底线。

任何组织、个人不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息；不得从事危害国家安全、公共利益的个人信息处理活动。

- “面”：指共同参与，建设良性生态。

国家建立健全个人信息保护制度，预防和惩治侵害个人信息权益的行为，加强个人信息保护宣传教育，推动形成政府、企业、相关社会组织、公众共同参与个人信息保护的良好环境。

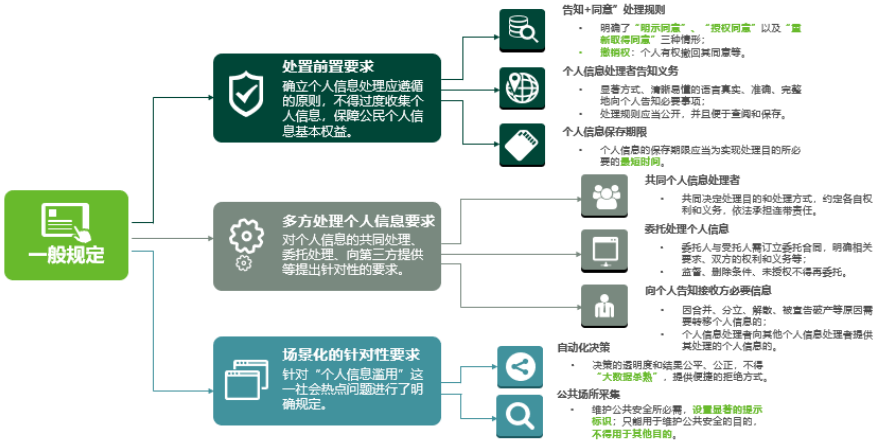
- “球”：指国际合作，推进生态互融。

国家积极参与个人信息保护国际规则的制定，促进个人信息保护方面的国际交流与合作，推动与其他国家、地区、国际组织之间的个人信息保护规则、标准等互认。

2.2.5处理规则

- 个人信息处理规则：包括了一般规定、敏感个人信息的处理规则、国家机关处理个人信息的特别规定三个方面。需要注意的是，本法确立以“告知—同意”为核心的个人信息处理规则，同时也新增了同意的例外

事由，如《个人信息保护法》第十三条中提到的“前款第二项至第七项规定情形的，不需取得个人同意”。



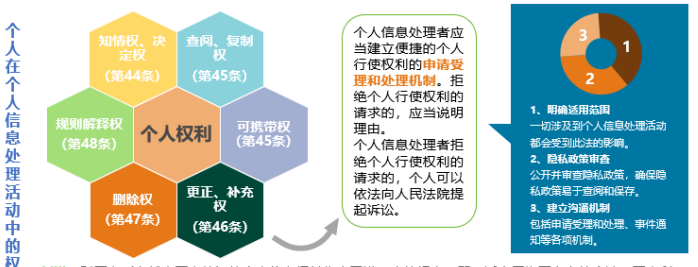
敏感个人信息的处理规则

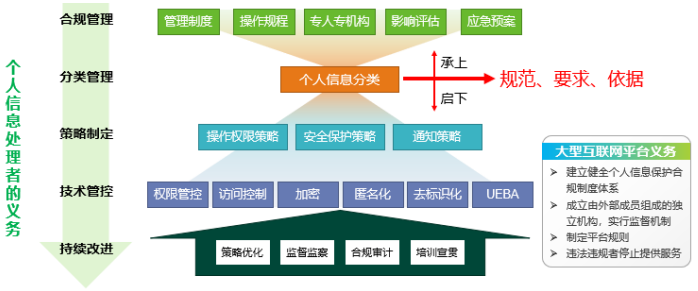
国家机关处理个人信息的特别规定

- 个人信息跨境提供的规则：本法构建了一套清晰、系统的个人信息跨境流动规则，以满足保障个人信息权益和安全的客观要求，适应国际经贸往来的现实需要。关于跨境提供场景下的规则要求详细如下图所示：

2.2.6相关主体

本法涉及个人、个人信息处理者、监管部门三大强相关的主体，如下图所示，分别就个人权利、个人信息处理者的义务、监管部门所履行个人信息保护职责进行阐述。





履行个人信息保护职责的部门

部门	职能分工	角色	个人信息保护职责	具体措施	责任
国家网信部门	负责统筹协调个人信息保护工作和相关监督管理工作。	国家通用监管	***基本职责：*** （1）宣传教育和指导、监督； （2）接受、处理相关的投诉、举报； （3）组织对应用程序等个人信息保护情况进行测评，并公布测评结果； （4）调查、处理违法个人信息处理活动； （5）法律、行政法规规定的其他职责。 ***国家网信部门统筹协调职责：*** （1）组织制定个人信息保护相关规则、标准； （2）针对小型个人信息处理者制定相关个人信息保护规则和标准； （3）推进网络身份认证公共服务建设； （4）推进个人信息保护社会化服务体系建设，支持有关机构开展个人信息保护评估、认证服务； （5）完善个人信息保护投诉举报工作机制。	（1）询问有关当事人，调查具体情况； （2）查阅、复制合同、记录、账簿以及其他有关资料； （3）实施现场检查； （4）检查有关的设备、物品，对有证据证明的，经书面报告并经批准，可查封或者扣押； （5）约谈法定代表人或者主要负责人； （6）处理投诉与举报。	国家机关不履行本法规定的个人信息保护义务的，由其上级机关或者履行个人信息保护职责的部门责令改正；对直接负责的主管人员和其他直接责任人员依法给予处分。（第68条）
国务院有关部门	在各自职责范围内负责个人信息保护和监督管理工作。	部门监管/行业监管			
县级以上地方人民政府有关部门	按照国家有关规定确定。	基层监管落地			

2.2.7强监管和惩处力度

近年来，有关个人信息权益侵权案件逐渐增多，比如“告知—同意”的认定、人格权纠纷、人脸识别等与个人信息主体强相关的权益。因此，本法在这方面加强了监管和提高了惩处力度。本法规定了“一般的个人信息违法行为”和“情节严重的个人信息违法行为”，虽然对这两者没有严格的界定和说明，但可参照以往的司法案例或借鉴GDPR相关处罚案例。详细惩处要求如下图所示：

惩罚力度	违规行为	处置情况	单位	直接负责的主管人员和其他直接责任人员
一般的个人信息违法行为	违反本法规定处理个人信息，或者处理个人信息未履行本法规定的个人信息保护义务的。	由履行个人信息保护职责的部门责令改正，给予警告，没收违法所得，对违法处理个人信息的应用程序，责令暂停或者终止提供服务。	拒不改正的：100万以下	1-10万
情节严重的个人信息违法行为	有前款规定的违法行为，情节严重的。	禁止其在一定期限内担任相关企业的董事、监事、高级管理人员和个人信息保护负责人。	五千万元或上一年度营业额5%以下	10-100万元
记入信用档案，并予以公示	有本法规定的违法行为的，依照有关法律、行政法规的规定记入信用档案，并予以公示。			
依法给予处分	国家机关不履行本法规定的个人信息保护义务的，责令改正；对直接负责的主管人员和其他直接责任人员依法给予处分。履行个人信息保护职责的部门的工作人员玩忽职守、滥用职权、徇私舞弊，尚不构成犯罪的，依法给予处分。			
民事责任	**私益诉讼：**处理个人信息侵害个人信息权益造成损害，个人信息处理者不能证明自己没有过错的，应当承担损害赔偿等侵权责任。 其难以确定的，由人民法院根据实际情况确定赔偿数额。			
	公益诉讼：个人信息处理者违反本法规定处理个人信息，侵害众多个人的权益的。 人民检察院、法律规定的消费者组织、和由国家网信部门确定的组织可以依法向人民法院提起诉讼。			
刑事责任	**刑事惩处：**违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚。			
	治安处罚：违反本法规定，构成犯罪的，依法追究刑事责任。			

2.3 横向对比

为了便于对《个人信息保护法》进一步理解，本文通过列表的方式对国内强相关的几部法律法规进行横向对比，如下图所示。本文对照仅限于非法律专业视角进行对照，因此严格意义上来说不能准确对比分析法律效力位阶的相关问题。

对比项	网络安全法	民法典	数据安全法	个人信息保护法	个人信息安全规范
个人信息定义	识别 采取了不完全列举方式。	识别 采取了不完全列举方式，扩大个人信息的范围。	对“数据”、“数据安全”等概念进行了定义，仅采取定义式的规定方式。	识别 仅采取定义式的规定方式，将匿名化的信息排除在个人信息之外。	识别+关联 采取了不完全列举方式，对个人信息和个人敏感信息进行例举。
侧重方向	**方向：网络空间安全** • 维护网络空间良好生态； • 个人信息保护仅提出总体性原则和概括性要求，未进行颗粒度要求。	**方向：个人信息权益** • 个人信息权益的定位其人格属性； • 确立了个人信息受法律保护的原则和设立了相关的民事权利。	**方向：数据安全** • 数据领域的基础性法律，重点确立数据安全保护管理各项基本制度； • 明确规定了开展数据活动的组织和个人的责任和义务。	**方向：个人信息安全** • 个人信息保护的专门法律； • 兼顾个人信息的安全和利用； • 明确边界，适用范围更为直接明确。	**方向：个人信息安全** • 提供了具有可操作性的指引； • 规范了个人信息处理活动应遵循的原则和安全要求。
局限性	在社会实践中，将用户同意作为唯一的合法依据，其适用性有限且缺乏细节。	仅适用于民事领域，且未能向监管者进行个人信息保护提供实施细则或赋予其明确的权力。	立足数据安全工作实际，着力解决数据安全领域突出问题，不涉及具体个人信息保护层面。	仍采取国家主管部门监督、指导，有关部门对应执法的模式，并未确立集中监管机构。	不具有强制效力，但不排除实践中执法机构的参考借鉴。

通过以上从定义、侧重方向、局限性三个方面进行横向对比后，本文得出如下参考结论：

1) 随着我国法律法规的不断完善，各行各业首先需要考虑的是“合规”问题，特别需要关注具体的、可落地的安全要求；

2) 各项法律法规间各有侧重点和存在一定的相互关联性，需特别注意上位法的法律效力；在具体实践过程中，均需遵照执行；

3) 《数据安全法》和《个人信息保护法》都提出落实处理者的责任和义务，对企业而言，是否需要建立两套标准呢？答案是否定的，建议将其融合，组织建设、制度流程等可合二为一，人员能力、技术措施需有所针对性实施，具体要求方面再进行细化和管控。

2.4 解读思考

2.4.1典型问题 QA

◆ 典型问题一：关于“告知+同意”。

依据：第14条将“充分知情”作为“同意”的前提条件”，需要取得“单独同意”的情况：第23、25、26、29、39条。

解答：通过用户主动勾选、浏览隐私政策等获得个人信息的授权使用，并赋予用户撤回同意的权利；同时梳理“单独同意”的场景并进行对应功能调整。

◆ 典型问题二：关于生物特征等敏感个人信息。

依据：第26条规定的“所收集的个人图像、身份识别信息只能用于维护公共安全的目的”、第28条规定的“特定的目的和充分的必要性”的前提，第29规定的处理敏感个人信息的“单独同意”，第30条规定的“必要性以及对个人权益的影响”的告知。

解答：重视敏感个人信息的处理规则，并做好相关充分告知和影响评估等工作。

◆ 典型问题三：关于“个人信息保护负责人”。

依据：第52条规定“处理个人信息达到国家网信部门规定数量的个人信息处理者应当指定个人信息保护负责人。”

解答：其中“规定数量”在本法中未明确规定，但可参照《个人信息安全规范》的规定从业人员规模大于200人、处理超过100万人的个人信息、处理超过10万人的个人敏感信息的。

◆ 典型问题四：关于影响评估。

依据：第55条规定“有下列情形之一的，个人信息处理者应当事前进行个人信息保护影响评估，并对处理情况进行记录。”

解答：结合《个人信息安全规范》和《影响评估指南》相关要求，进行个人信息安全影响评估落地执行。

以上思考的问题仅为冰山一角，建议组织结合自身实际情况，制定相应安全策略，落实个人信息保护责任。

2.4.2主要关注点

1) 明确个人信息保护责任制，落实全生命周期管控责任。

内容：建立个人信息保护组织架构，明确岗位职责，制定对应的全流程管理规范、制度、流程等。

方案支撑：数据安全管理体系建设。

2) 通过个人信息分类（分级）管理，实现建设第一步。

内容：建立个人信息管理机制，明确保护对象及策略。

方案支撑：数据分类分级。

3) 发现企业个人信息安全隐患，降低信息泄露风险。

内容：利用风险评估手段识别发现企业的个人信息安全风险，协助企业进行整改，提升企业个人信息保护建设水平。

方案支撑：个人信息安全影响评估、APP个人信息安全评估。

4) 识别个人信息处理活动，落实安全技术措施。

内容：梳理个人信息全生命周期处理活动，制定相对应的安全要求，对各风险点进行提示，包含可落地执行的机制等。

方案支撑：个人信息保护专项规划、数据安全管控平台。

5) 建立个人信息安全事件应急响应机制。

内容：建立个人信息安全应急预案，明确个人信息事件的应急方针、政策，应急组织结构及相关应急职责。

方案支撑：应急响应体系建设。

6) 组织开展个人信息安全培训教育。

内容：组织开展个人信息安全专业培训，提升企事业单位个人信息安全保护意识，加强个人信息安全人员专业能力提升。

方案支撑：个人信息安全专业教育培训。

7) 聚焦个人信息跨境提供，保障国家安全、公共利益及个人权益。

内容：建立个人信息跨境提供全流程管理规范、制度、流程等；明确合规路径，并征得用户的单独同意，确保个人信息安全流通。

方案支撑：遵循国家个人信息出境相关规定。

3. 总结与展望

2021年可谓是数据保护元年，《数据安全法》、《个人信息保护法》、《关键信息基础设施安全保护条例（国务院令第745）》等一些列法律法规的颁布和即将实施，标志着我国在数据安全和个人信息保护方面正式进入2.0时代。而数据安全和个人信息保护密不可分，就像是一对孪生兄弟。针对个人信息保护的应对思路，可在数据安全建设的基础上进行专项设计和实施，形成个人信息保护体系的长效机制（IRCSS）。主要通过五个方面进行个人信息安全落地建设，帮助客户确立管理制度和操作流程，全面了解个人信息安全状况，提升个人信息安全监测与防护措施，通过优化改进与持续运营，实现持续自适应的个人信息安全防护能力。

4. 场景探讨：“双十一”的狂欢

近年来，“双十一”的狂欢背后，也是个人信息泄露的高峰。《个人信息保护法》正巧将于2021年11月1日施行，面对今年的“双十一”，消费者、商家、互联网平台运营者、监管部门等该如何将这“狂欢”推向高潮呢？接下来，本文将站在这四类主体的角度来思考如何面对。


消费者角度
虽然知道“双十一”套路多，但今年似乎以往年不同：《个人信息保护法》即将于11月1日施行啦！那么，以下六大主要问题是不是会有不同以往的体验？
个人信息泄露
个人信息泄露是不是不公那么突出了，信息骚扰是不是也会少很多。
大数据杀熟
不同手机终端、不同地区、不同时段等访问同一个商品时，价格是不是都一样了。
个性化推荐
从设置过个性化推荐是不是不再默认推荐了；当天讨论话题，隔天是不是还会有推荐。
充分知情权益
平台、商家收集我的个人信息时是否遵循了“告知+同意”基本原则，隐私政策是否友好可达、内容清晰明了等。
个人使用体验
相关权限是否不再过度索取，访问、更正、删除等是否操作方便；投诉举报是否及时处理。
个人维权之路
再次遇到侵犯了“我”的权益时，个人维权时是否相应及时处理结果是否保护了“我”的权益。
商家角度
大数据杀熟禁用
确保自动化决策透明度和结果公平、公正，否中禁止使用。
客户个人信息慎处理
客户姓名、手机号码、地址等信息谨慎处理，避免批量下载、网络发送、U盘拷贝、明文存储等。
KPI
大数据分析慎用
使用客户数据进行大数据分析（如用户画像），对客户类型进行甄别后慎用“精准营销”和“价格歧视”。
信息推送、商业营销慎发
商品促销短信、商品优惠信息要怎么发？还是不发了吧！
隐私政策需审查
审查收集、使用（自动化决策）、共享（向第三方提供）等生命周期有关个人信息处理规则；
需建立机制以证明同意是有效的，并确保同意可以被撤回等。
用户权益保障需到位
促进个人信息合理使用和平衡各方权益；
对收集的用户个人信息严格保密，未经用户授权同意，不得向包括关联方在内的任何第三方提供。
安全运营与持续更新
通过优化改进与持续运营，如制度流程、数据运营机制等，实现持续自适应的个人信息安全防护能力。
互联网平台运营者
采取必要措施保障用户信息安全
建立健全个人信息保护合规制度体系；
采取数据加密、数据脱敏、数据防泄漏等技术手段；
细化平台规则，监测异常操作行为，及时安全审计等；
独立外部机构，实行监督机制，及时发现安全风险等等。
运输运营者强化用户信息流转安全
建立健全个人信息保护合规制度体系；
用户物流信息执行场景化脱敏模式；
细化平台规则，监测异常操作行为；
物流从业者恪守规章制度和守护安全底线；
……
监管部门
履行监督义务，守护用户权益
调查、处理用户投诉举报的个人信息泄露、大数据杀熟等事件
规范App以及其他形态的产品等个人信息处理活动
对应用程序等个人信息保护情况进行测评，并公布测评结果
明确处理个人信息的规范和履行保护个人信息应尽义务
开展个人信息保护宣传教育，提升公民个人信息保护安全意识
落实个人信息保护安全意识提升，强化人员个人信息保护技能水平

NSFOCUS

行业研究

攻防论道之总结篇 | 往者不可谏，来者犹可追

以攻促防，攻防相长

——绿盟科技

网络攻防演练的目的是发现当前关键信息基础设施防护体系中存在的不足，找出解决的方案。因此在演练结束之后，必须及时进行复盘总结，以期全面改进。在总结阶段，需要做三项工作：过程复盘、经验总结和提升规划。

一、过程复盘

1. 安全事件汇总分析

攻防演练防护结束后，攻防演练防护项目组将对演练期间的数据进行汇总，并从以下维度展开分析：

攻击事件

针对不同的攻击事件进行攻击时段、频率、次数的统计，分析常见攻击事件行为，识别已受攻击的业务风险。

风险等级

风险等级由高到低排序，重点关注高危行为，根据高危行为指向的目的地址，识别易受攻击的业务模块。

攻击路径

复现环境拓扑，还原攻击者的入侵路径，分析攻击思路，回溯业务薄弱环

节，根据薄弱点制定对应的加固措施。

漏洞利用

汇总攻击者入侵路线所利用的漏洞，追溯漏洞形成原因。

2. 缺陷问题输出闭环

攻防演练防护项目组将针对重大保障前期的待处理事件和中期发生的安全事件进行梳理，根据安全问题风险程度由高到低设置处理优先级，绘制输出安全事件跟踪表，内容包括但不限于：问题分类、影响范围、问题描述、发现时间、处置完成时间、主要跟进人、问题进展、是否闭环、事件优先级等。

二、经验总结

完成对演练过程中安全事件的全面复盘之后，就进入了经验总结环节。经验总结一般从两方面进行：防守经验和反制经验。

1. 防守经验

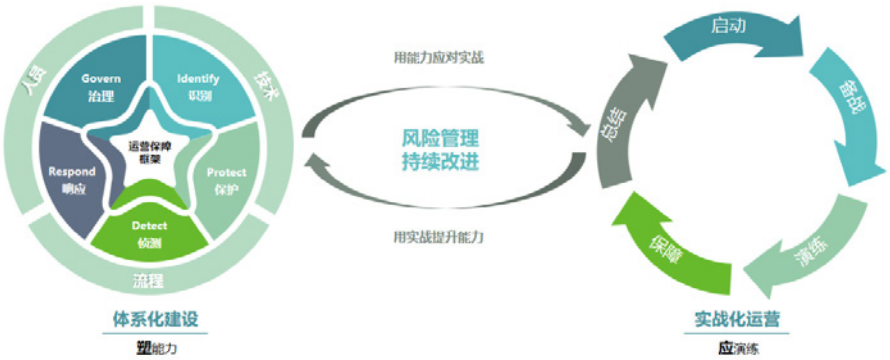
在备战阶段，项目组进行了资产安全评估、业务缺陷识别、风险整改推进、防护能力补差、整体策略优化和意识能力培训。在做经验总结时，项目组需要全面回顾前期的工作，判断在资产安全评估中是否有遗漏的资产被攻击方发现，是否有未修复的漏洞被攻击方利用；在业务缺陷识别中是否有未识别的缺陷造成数据泄露，是否有供应链被攻击方利用；在风险整改中是否已知风险未闭环使得攻击方得分；在防护能力补差中是否有短板未消除，新增的安全防护设备是否真正起到了作用；在整体策略优化中是否能从优化后的日志中快速定位攻击事件，是否切实减少了误报而没有增加漏报；在意识能力培训中是否做到了全员安全意识增强，而没有被攻击队钓鱼利用。

2. 反制经验

攻防演练的过程也是项目组溯源反制能力的检验过程。在本阶段主要总结是否发现了攻击方利用的0day漏洞，是否定位了攻击方的真实IP，是否通过溯源发现了攻击方的人员真实信息。

三、提升规划

通过经验总结，项目组可以明晰整个攻防演练过程中的成绩和不足。这些不足暴露了当前网络和业务系统中存在的安全薄弱部分，也就是需要改进的方向。



网络攻防演练，既是检查网络安全建设成果的试金石，也是指导开展下一步建设的指路灯。通过攻防演练，企业应以体系化建设为指引，构建“全场景、可信任、实战化”的安全运营能力，实现“全面防护，智能分析，自动响应”的防护效果，使得企业的网络安全平稳健康的发展。

关于云原生应用，这些安全风险了解一下

绿盟科技

摘要：云原生应用究竟和传统应用有何不同，安全风险上有何变化？本文将从传统应用风险、应用架构变革带来的风险、云计算模式带来的风险三个维度进行介绍。

一、概述

随着云计算技术的不断发展，上云已经不再是一种选择，而是一种共识，是企业数字化转型的必要条件。在相应实践过程中，传统应用存在升级缓慢、架构臃肿、无法弹性扩展及快速迭代等问题，于是近年来云原生的概念应运而生，凭借着云原生弹性、敏捷、资源池和服务化等特性，解决了业务在开发、集成、分发和运行等整个生命周期中遇到的问题。

云原生环境中，应用由传统的单体架构转向微服务架构，云计算模式也相应的从基础设施即服务（Infrastructure as a Service，IaaS）转向为容器即服务（Container as a Service，CaaS）和函数即服务（Function as a Service，FaaS）。应用架构和云计算模式的变革是否会导致进一步的风险，这些风险较之传统应用风险又有哪些区别？在讲述云原生应用具体风险前，首先列举以下三个观点，这些观点有助于大家更好地理解本文所讲述的内容。

观点一　云原生应用继承了传统应用的风险和API的风险

云原生应用源于传统应用，因而云原生应用风险也就继承了传统应用的风险。此外，由于云原生应用架构的变化进而导致应用API交互的增多，可以说云原生应用中大部分交互模式已从Web请求/响应转向各类API请求/响应 ，例如RESTful/HTTP、gRPC等，因而API风险也进一步提升。

观点二 应用架构变革将会带来新的风险

由于应用架构变革，云原生应用遵循面向微服务化的设计方式，从而导致功能组件化、服务数量激增、配置复杂等问题，进而为云原生应用和业务带来了新的风险。

观点三 计算模式变革将会带来新的风险

随着云计算的不断发展，企业在应用的微服务化后，会进一步聚焦于业务自身，并将功能函数化，因而出现了无服务器计算（Serverless Computing）这类新的云计算模式，进而引入了Serverless应用和Serverless平台的新风险。

综上所述，可以看出云原生应用带来的风险是不容小觑的。本文将从传统应用风险、应用架构变革带来的新风险、云计算模式变革带来的新风险三个维度分别进行介绍，希望可以引发大家更多的思考。

二、传统应用面临的风险

云原生应用风险可以参考传统应用风险。传统应用风险以Web应用风险为主，主要包括注入、敏感数据泄露、跨站脚本、使用含有已知漏洞的组件、不足的日志记录和监控等风险。

此外，云原生环境中，应用的API交互模式逐渐由“人机交互”转变为“机机交互”，虽然API大量出现是云原生环境的一大特点，但本质上来说，API风险并无新的变化，因而其风险可以参考现有的API风险，主要包括安全性错误配置、注入、资产管理不当、资源缺失和速率限制等风险。

有关传统应用风险和API风险的更多细节可以分别参考OWASP组织在2017和2019年发布的应用十大风险报告[1]和API十大风险报告[2]。

三、应用架构变革带来的新风险

3.1 云原生应用带来的新风险

云原生应用面临的新风险主要体现在：新应用架构的出现。新应用架构遵循微服务化的设计模式，通过应用的微服务化，我们能够构建容错性好、易于管理的松耦合系统，与此同时，新应用架构的出现也会引入新的风险，为了较为完整地对风险进行分析，本文将以信息系统安全等级三要素，即机密性（Confidentiality）、完整性（Integrity）、可用性（Availability）作为导向介绍应用架构变化带来的新风险。

机密性受损的风险

典型的如信息泄露风险，攻击者可通过利用资产脆弱性和嗅探、暴力破解等攻击方式窃取用户隐私数据，从而造成信息泄露风险。

完整性受损的风险

典型的如未授权访问风险，攻击者可通过利用资产脆弱性和中间人攻击等行为绕过系统的认证授权机制，执行越权操作，从而造成未授权访问的风险。

可用性受损的风险

典型的如系统被拒绝服务的风险，一方面，攻击者可通过畸形报文、SYN泛洪等攻击方式为目标系统提供非正常服务，另一方面，系统供不应求的场景也会导致系统遭受拒绝服务风险。

本小节接下来的内容，将以信息泄露、未授权访问、拒绝服务为例，分别介绍上述三类风险。

3.1.1 数据泄露的风险

云原生环境中，虽然造成应用数据泄露风险的原因有很多，但都离

不开以下几个因素：

应用漏洞：通过资产漏洞对应用数据进行窃取。

密钥不规范管理：通过不规范的密钥管理对应用数据进行窃取。

应用间通信未经加密：通过应用间通信未经加密的缺陷对传输中数据进行窃取，进而升级到对应用数据的窃取。

3.1.1.1 应用漏洞带来的风险

应用中存储的数据多是基于API进行访问，若应用中某API含有未授权访问漏洞，例如Redis未授权访问漏洞，攻击者便可利用此漏洞绕过Redis认证机制，访问到内部数据，进而导致了敏感信息泄露的风险。

传统单体应用架构下，由于API访问范围为用户到应用，攻击者只能看到外部进入至应用的流量，无法看到应用内部的流量，所以针对恶意使用API漏洞进行数据窃取造成的损失范围通常是有限的。

反观微服务化应用架构，当单体应用被拆分为若干个服务后，这些服务会根据业务情况进行相互访问，API访问范围变为服务到服务（Service to Service），若某服务因API漏洞导致攻击者有利可图，那么攻击者将会看到应用内部的流量，这无疑为攻击者提供了更多的攻击渠道，因而针对数据泄露的风险程度而言，微服务架构相比传统单体应用架构带来的风险更大。此外，随着服务数量达到一定规模，API数量将不断递增，进而扩大了攻击面，增大了数据泄露的风险。

3.1.1.2 密钥不规范管理带来的风险

在应用的开发过程中，开发者常疏于对密钥的管理从而导致数据泄露的风险，例如开发者将密钥信息、数据库连接密码等敏感信息硬编码在应用程序中，从而增大了诸如应用程序日志泄露、应用程序访问密钥泄露的风险。

传统单体应用架构中，开发者常将配置连同应用一起打包，当需要修改配置时，只需登录至服务端进行相应修改，再对应用进行重启便可实现，这种单个集中式配置文件的存储方式从密钥管理风险的角度上讲是相对可控的。

微服务应用架构中，应用的配置数量与服务数量的逐渐增多是成正比的，例如微服务应用中会存在各种服务、各种数据库访问、各种环境变量的配置，且各配置支持动态调整。同时，微服务应用架构对服务的配置管理也提出了更高的要求，例如代码与配置可分离、配置支持分布式、配置更新的实时性、配置可统一进行治理等，因而微服务下的配置管理更加复杂，对运维人员的要求更高，密钥管理的难度也在不断提升，最终会造成更大的数据泄露风险。

3.1.1.3 应用通信未经加密带来的风险

如果应用采用HTTP协议进行数据传输，那么HTTP页面的所有信息将都以纯文本形式进行传输，并且默认不提供任何加密措施。因而在数据传输过程中易被攻击者监听、截获和篡改，典型的攻击流程为攻击者通过Fiddler、Wireshark等抓包工具进行流量监听，截获传输的敏感信息（例如数据库密码、登录密码等），最后攻击者根据自身意图对敏感数据进行篡改并发送至服务端，进而导致数据泄露的风险。

传统单体应用架构中，由于网络拓扑相对简单，且应用通信多基于HTTP/HTTPS，因而造成的数据泄露风险多是因为采用了HTTP协议。微服务应用架构中，网络拓扑相对复杂，因遵循分布式的特点，应用间的通信不仅采用HTTP/HTTPS协议，还采用gRPC等协议，由于gRPC协议默认不加密，因而将会导致攻击面的增多，为数据泄露带来了更多的风险。

3.1.2 未授权访问的风险

云原生环境中，应用未授权访问的风险多是由于应用自身漏洞或访问权限错误地配置导致。

3.1.2.1 应用漏洞带来的风险

应用漏洞是造成未授权访问的一大因素。未授权访问漏洞非常之多，较为常用的如Redis、MongoDB、Jenkins、Docker、Zookeeper、Hadoop等应用都曾曝光过相关漏洞，例如Docker曝出的Docker Remote API未授权访问漏洞，攻击者可通过Docker Client或HTTP请求直接访问Docker Remote API，进而对容器进行新建、删除、暂停等危险操作，甚至是获取宿主机shell权限。再如MongoDB未授权访问漏洞，该漏洞造成的根本原因在于MongoDB在启动时将认证信息默认设置为空口令，从而导致登录用户可通过默认端口无需密码对数据库进行任意操作并且可以远程访问数据库。

从漏洞成因的出发点来看，认证及授权机制的薄弱是其主要原因，在单体应用架构下，应用作为一个整体对用户进行认证授权，且应用的访问来源相对单一，基本为浏览器，因而风险是相对可控的，微服务应用架构下，其包含的所有服务均需对各自的访问进行授权，从而明确当前用户的访问控制权限，此外，服务的访问来源除了用户外还包含内部的其他服务，因而在微服务架构下，应用的认证授权机制更为复杂，为云原生应用带来了更多的攻击面。

3.1.2.2 访问权限错误配置带来的风险

由于运维人员对用户的访问权限进行了错误配置，进而会增大被攻击者利用

的风险。例如，运维人员对Web应用访问权限进行相应配置，针对普通用户，运维人员应只赋予其只读操作，若运维人员进行了错误的配置，例如为普通用户配置了写操作，那么攻击者便会利用此缺陷绕过认证访问机制对应用发起未授权访问攻击。

传统应用架构中，应用由于设计相对单一，其访问权限也相对单一，几乎只涉及用户对应用的访问权限这一层面，因此对应的访问权限配置也相对简单。因为访问权限配置简单的特点，用户身份凭据等敏感信息常存储在应用的服务端，一旦攻击者利用配置的缺陷对应用发起未授权访问入侵，就有可能拿到所有保存在后端的数据，从而造成巨大风险。

微服务应用架构下，由于访问权限还需涉及服务对服务这一层面，因此将会导致权限映射关系变得更加复杂，相应的权限配置难度也在同步增加，例如一个复杂应用被拆分为100个服务，运维人员需要严密地对每个服务赋予其应有的权限，如果因疏忽导致为某个服务配置了错误的权限，攻击者就有可能利用此缺陷对服务展开攻击，若该服务中包含漏洞，进而可能会导致单一漏洞扩展至整个应用的风险。所以如何对云原生应用的访问权限进行高效率管理成为了一个较难的问题，这也是导致其风险的关键因素。

3.1.3 被拒绝服务的风险

被拒绝服务是应用程序的面临的常见风险。造成拒绝服务的主要原因包括两方面，一方面是由于应用自身漏洞所致，例如ReDoS漏洞、Nginx拒绝服务漏洞等，另一方面是由于访问需求与资源能力不匹配所致，例如某电商平台的购买API由于处理请求能力有限，因而无法面对突如其来的大量购买请求，导致了平台资源（CPU、内存、网络）的耗尽甚至崩溃。这种场景往往不带有恶意企图，而带有恶意企图的则主要以ACK、SYNC泛洪攻击及CC（Challenge Collapsar）等攻击为主，其最终目的也是应用资源的耗尽。

3.1.3.1应用漏洞带来的风险

应用漏洞可以导致应用被拒绝服务，那么具体是如何导致的呢？以ReDoS（Regular expression Denial of Service）漏洞为例，ReDoS为正则表达式拒绝服务，攻击者对该漏洞的利用通常是这样的一个场景，应用程序为用户提供了正则表达式的输入类型又没有对具体的输入进行有效验证，那么攻击者便可通过构造解析效率极低的正则表达式作为输入进而在短时间内引发100%的CPU占用率，最终导致资源耗尽，甚至应用程序崩溃的风险。

3.1.3.2 访问需求与资源能力不匹配带来的风险

此处以CC攻击举例，其攻击原理通常是攻击者通过控制僵尸网络、肉鸡或代理服务器不断地向目标主机发送大量合法请求，从而使正常用户的请求处理变得异常缓慢。

传统Web场景中，攻击者利用代理服务器向受害者发起大量HTTP GET请求，该请求主要通过动态页面向数据库发送访问操作，通过大量的连接，数据库负载极高，超过其正常处理能力，从而无法响应正常请求，并最终导致服务器宕机。

在微服务应用架构下，由于API数量会随着服务数量的递增而递增，因而可能将会导致单一请求生成数以万计的复杂中间层和后端服务调用，进而更容易引起被拒绝服务的风险，例如若微服务应用的API设计未考虑太多因单个API调用引起的耗时问题，那么当外部访问量突增时，将会导致访问需求与资源能力不匹配的问题，使服务端无法对请求作出及时的响应，造成页面卡死的现象，进而会引起系统崩溃的风险。

3.2 云原生业务带来的新风险

云原生应用业务风险和云原生应用风险有何区别？云原生应用风险主要

是Web应用风险，即网络层面的风险，而云原生应用业务风险无明显的网络攻击特征，多是利用业务系统的漏洞或规则对业务系统进行攻击来牟利，从而造成一定的损失。

此外，与传统应用架构中的业务风险不同，微服务应用架构中，若服务间的安全措施不完善，例如用户授权不恰当、请求来源校验不严格等，将会导致针对微服务业务层面的攻击变得更加容易，例如针对一个电商应用，攻击者可以对特定的服务进行攻击，例如通过API传入非法数据，或者直接修改服务的数据库系统等。攻击者可以绕过验证码服务，直接调用订单管理服务来进行薅羊毛等恶意操作。攻击者甚至可以通过直接修改订单管理和支付所对应的服务系统，绕过支付的步骤，直接成功购买商品等。

综上，应用微服务化的设计模式带来的业务风险可包含两方面，一方面是未授权访问风险，典型场景为攻击者通过权限绕过对业务系统的关键参数进行修改从而造成业务损失，另一方面则是API滥用的风险，典型的是对业务系统的薅羊毛操作。

3.2.1 未授权访问的风险

在云原生业务环境中，造成未授权访问风险的原因，可以大致分为业务参数异常和业务逻辑异常两方面，为了更为清晰的说明上述异常如何导致未授权访问的风险，这里以一个微服务架构的电商系统举例说明。如图1所示：

图 1 某电商系统流程图

3.2.1.1 业务参数异常带来的风险

API调用过程中往往会传递相关的参数。参数的取值根据业务场景的不同会有不同的取值范围。例如商品数量必须为非负整数，价格必须大于0等。若API对相应参数的监测机制不完善，那么攻击者便可通过输入异常参数导致业务系统受到损失。例如在图1所示的电商系统中，若商品价格只在商品介绍服务中进行校验，而未在订单管理和支付服务中进行校验，那么攻击者则可以通过直接调用订单管理和支付服务的API将订单价格修改为0元或者负值，从而给业务系统造成损失。

3.2.1.2业务逻辑异常带来的风险

相比于前一类异常，此类异常一般较为隐蔽。攻击者采用某些方法使API调用的逻辑顺序出现异常，包括关键调用步骤缺失、颠倒等。例如在图1所示的电商系统中，攻击者可以利用漏洞绕过支付的步骤直接提交订单。这样就会出现业务逻辑关键步骤缺失的情况，进而会为业务系统带来损失，例如验证码绕过异常就属于业务逻辑异常的一种。

3.2.2 API 滥用的风险

针对此类风险，通常指的是攻击者对业务系统的薅羊毛操作，风险成因则是由于业务频率异常所致，这里以电商系统举例说明。

业务频率异常主要指针对一个或一组API的频繁调用。业务系统往往通过图形验证码的方式来避免机器人刷单的操作。例如在图1所示的电商系统中，攻击者可以绕过验证码所对应的服务，直接对订单进行操作，进而实现机器刷单，对电商进行薅羊毛。

四、云计算模式变革带来的新风险

作为一种新的云计算模式，Serverless具备许多特性，典型的主要有输入源的不确定性、服务器托管云服务商、供应商锁定等，这些特性可能会给Serverless带来新的风险。

此外，由于Serverless最终呈现的还是多个函数组成的应用，且被Serverless提供的服务端运行，因此Serverless风险还应包括Serverless应用的风险及Serverless平台的风险。

最后Serverless因购买、部署成本低、函数访问域名相对可信等将会使Serverless面临被滥用的风险。

4.1 Serverless特征带来的风险

4.1.1 输入源不确定带来的风险

Serverless函数是由一系列事件触发的，如云存储事件（S3、Blobs和其他云存储）、流数据处理（如：AWS Kinesis）、通知（如：SMS、电子邮件、IoT）等，鉴于此特性，我们不应该把来自API调用的输入作为唯一攻击面。此外，我们不再控制源到资源间的这条线，如果函数被邮件或数据库触发，将无处可设置防火墙或任何其他控制措施来验证事件源[4]。可见输入源的不确定性将可能导致一定的风险。

在传统应用程序开发中，开发者根据自身实践经验，在数量有限的可能性中可判定出恶意输入来源，但Serverless模式下函数调用是由事件源触发，输入来源的不确定性限制了开发者的判定。例如当函数订阅一个事件源后，该函数在该类型的事件发生时被触发，这些事件可能来源于FaaS平台，也可能来源于未知的事件源，对于来源未知的事件源可以被标注为不受信任。在实际应用场景中，如果开发者没有良好的习惯对事件源进行分类，则会经常导致将不受信任的事件错认为是FaaS平台事件，进而将其视为受信任的输入来处理，最终带来了风险。

具体地，输入来源的不确定性会为Serverless应用带来注入的风险，与传统应用相同的是，注入攻击过程与并无太大区别，不同的是攻击向量的变化，传统应用中用于注入攻击的向量通常指攻击者可以控制或操纵应用输入的任何位置，但Serverless应用由于输入的不确定性因而带来了更大的攻击面。

4.1.2 服务托管云服务厂商带来的风险

传统应用中，例如Web应用常部署在本地/远程服务器上，关于服务端的操

作系统漏洞修补、网络拓扑的安全、应用在服务端的访问日志及监控等均需要特定的运维人员去处理，而Serverless的服务器托管云服务商的特点将导致开发者无法感知到服务器的存在，实际上开发者也无须对服务器进行操作，只需关注应用本身的安全即可，服务器的安全则交由云厂商管理Serverless的这一特征实际上降低了安全风险。

4.1.3 供应商锁定带来的风险

“供应商锁定”是指用户依赖特定供应商提供的产品及服务，并且在不产生实质性转换成本或运营影响的情况下无法使用其他供应商的云服务，在Serverless中，“供应商锁定”是目前存在的一大问题，例如用户选择AWS作为应用的运行环境，由于一些原因，该应用需迁移至Microsoft Azure平台，但“供应商锁定”的问题导致无法轻易的将之前运行的应用及使用的相应资源如S3存储桶等平滑迁移至Microsoft Azure平台中，进而导致企业面临应用转换成本的风险。

4.2 Serverless应用风险

Serverless应用属于云原生应用，其应用本身与传统应用基本是相同的，唯一区别是应用代码编写需要参照云厂商提供的特有代码模版，而传统应用通常没有这个限制。

Serverless应用属于云原生应用，云原生应用又源于传统应用，因而传统应用面临的风险几乎可以全面覆盖Serverless应用风险，关于风险分析部分可以参考之前传统应用风险的内容，更详细的内容可以参考OWASP组织在2017年发布的Serverless应用十大风险报告[4]。

4.3 Serverless平台风险

Serverless平台主要指FaaS平台，目前主流的FaaS平台分为两种类型，一种是面向公有云提供商的FaaS平台，常见的有AWS Lambda、Microsoft Azure Functions、Google Cloud Functions等，另一方面则是面向私有云的FaaS平台，此类以开源项目居多，且均支持在Kubernetes上进行部署，常见的有Apache OpenWhisk[7]、Kubeless[8]、OpenFaaS[9]、Fission[10]等。类似在IaaS平台上运行虚机、PaaS平台上运行操作系统和应用，FaaS平台较之上述平台的主要区别为其运行的是一个个Serverless函数。FaaS平台自身负责云环境地安全管理，主要包括数据、存储、网络、计算、操作系统等。

4.4 Serverless被滥用的风险

Serverless被滥用具体是指攻击者通过恶意构建Serverless函数并利用其充当整个

攻击中的一环，这种方式可在一定程度上规避安全设备的检测。导致Serverless被滥用的原因主要包括以下几点：

1. 云厂商提供 Serverless 函数的免费试用

近些年，各大云厂商为了用户体验，均对用户提供免费的Serverless套餐，包括每月免费的函数调用额度，这种方式虽然吸引了更多的用户去使用Serverless函数, 但也使得攻击者的攻击成本大幅降低。

2. 用户部署 Serverless 函数的成本低

由于Serverless服务端托管云厂商的机制，故用户只需实现函数的核心逻辑，而无须关心函数是如何被部署及执行的，利用这些特点，攻击者可以编写对其有利的Serverless函数并能省去部署的成本。

3. Serverless 函数访问域名可信

当用户部署完Serverless函数后，需要通过触发器去触发函数的执行，通常用户使用云厂商提供的API网关作为触发器，创建API网关触发器之后，云厂商会为用户提供一个公网的域名，用于访问用户编写的Serverless函数。需要注意的是，该公网域名通常是云厂商域名相关的子域名，因而是相对可信的，鉴于此，攻击者可以利用函数访问域名的可信去隐藏其攻击资产，躲避安全设备的检测。

五、总结

本文详细分析了云原生应用面临的风险，可以看出，云原生应用相比传统应用面临的风险主要为应用架构变革及新的云计算模式带来的风险，而针对应用本身的风险并无较大变化，因而对云原生应用架构和无服务器计算模式的深度理解将会有助于了解整个云原生应用安全。

参考文献

[1] https://owasp.org/www-project-top-ten/
[2] https://owasp.org/www-project-api-security/
[3] https://netflixtechblog.com/starting-the-avalanche-640e69b14a06
[4] https://www.owasp.org/index.php/OWASP_Serverless_Top_10_Project
[5] https://github.com/apache/openwhisk
[6] https://github.com/kubeless/kubeless
[7 https://github.com/openfaas/faas
[8] https://github.com/fission/fission

金融行业供应链安全风险

绿盟科技金融事业部 梁晴

金融行业供应链安全现状

因业务需要金融行业会采购大量第三方服务，例如：账单打印，IT运维，机房，软件开发，数据处理，业务办理等。这些提供专业各种服务的供应商已形成完善的金融机构服务供应链体系。供应链体系支撑着大量重要金融业务的正常运行，保障供应链中各个供应商的安全是金融机构信息科技风险管理工作重要的组成部分。

银保监会明确要求金融机构对信息科技供应商定期针对内部控制、质量管理、信息安全进行风险评估。并且金融机构在很多业务场景下必须把原始敏感数据明文发送给外部供应商，数据安全存在重大安全隐患。在实践场景中也经常会出现因供应商服务支持能力不足而导致的金融业务连续性问题。

金融机构安全部门一般会依据银保监监管合规要求以及自身业务需要，制定了信息科技供应商战略、信息科技供应商风险管理办法以及相关的执行要求，形成了健全、完善的信息科技供应商管理制度流程体系。但通常风险评估的方法及技术措施会比较薄弱。具体体现在以下几个方面：

- 没有根据业务场景对供应链进行合理分类。
- 各类供应商需承担的安全职责及所需的安全能力不明确，安全设计缺失。
- 没有针对供应链体系，定制风险评估方法并标准化。
- 供应商风险处置机制不完善。

解决方案

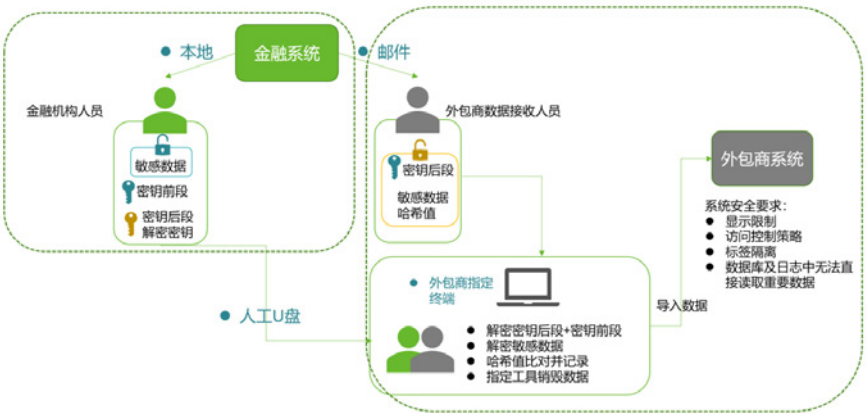
1）**现状调研：**访谈相关业务部门，理解目标金融机构的业务安全需求和科技服务外包现状，基于现有的信息科技风险评估框架、绿盟安全设计经验和国内外，针对各业务场景对供应链进行分类。

2）**安全设计：**针对涉及敏感数据处理的外包服务进行场景化的安全设计，最大限度保障数据的机密性及完整性。

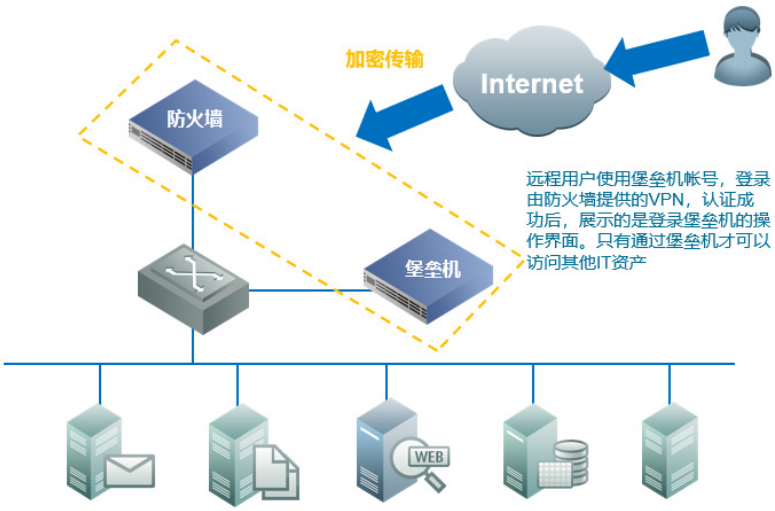
3）**定制风险评估标准化：**针对不同类别供应商制定风险评估方法、工作底稿和工具模板等。提升供应商安全能力。实现可以准确判断供应商安全风险情况，其中数据安全及服务连续性是风险评估重点。

4）**风险评估实施：**基于定制的风险评估标准化，定期对供应商进行风险评估，了解供应商安全状况及服务保障能力，提交评估报告并协助进行整改。为金融机构内部供应链管理提供参考。

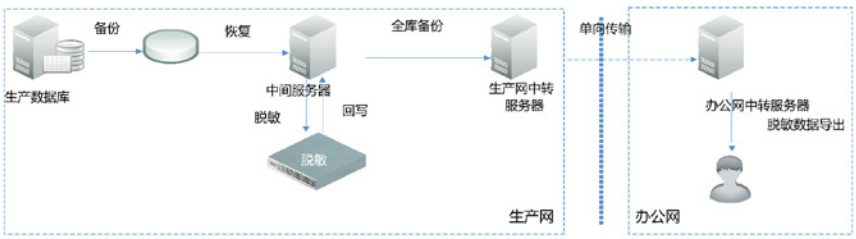
金融机构敏感数据外发到供应商处理安全场景设计：



供应商远程IT运维安全场景设计：



金融敏感数据脱敏导出安全场景设计：



价值

- ☐ 进一步规范金融机构信息科技供应链管理工作、对标国内外金融企业先进水平、促进供应商服务持续改进
- ☐ 保障与供应商数据交互过程中的数据安全
- ☐ 保障金融机构与外部服务相关业务持续稳定运行
- ☐ 完善并标准化供应商评价体系

深度解读 | 《金融数据安全 数据生命周期安全规范》

绿盟科技咨询设计部 陈淑娣

2021年4月8日，《金融数据安全 数据生命周期安全规范》（JR/T0223-2021）（以下简称《规范》）正式获批发布并实施。《规范》由中国人民银行科技司发起，全国金融标准化技术委员会归口管理。本标准为金融业机构数据安全建设提供了指导依据。

一、发布背景

随着信息技术的发展，众多金融基础业务、核心流程、行业间往来等事务和活动均已运行在信息化支撑载体之上，金融业机构生产运营产生的信息也逐步以不同形式转化为数字资产流转在金融业信息系统中。

过去，安全工作的重心一直在与采集、处理和存储数据的信息系统上，而非数据本身。但随着大数据、人工智能、云计算等新技术在金融业深入应用，金融数据逐步实现从信息化资产到生产要素的转变，其重要性日益凸显。仅保护承载数据的信息系统的方式太过狭窄，且数据泄露、滥用、篡改等安全威胁的影响逐步从机构内转移扩大至机构间和行业间，甚至影响国家安全、社会秩序、公众利益和金融市场稳定。

如何在满足金融业务基本需求和数据开发利用的基础上，强化数据保护能力，保障金融数据安全流动，已成为当前亟待解决的问题。金融行业持续密集地发布了数据安全相关的标准，以确保金融业机构能够应对当前日新月异的环境和形势。

二、标准特点和意义

《规范》构建了金融业机构覆盖数据全生命周期的数据安全框架，同时与各标准联系紧密，如数据安全能力成熟度模型、个人信息安全规范及金融行业的数据安全分级指南等。能够全面整体地指导金融业机构建设和完善自

身的数据安全防护体系，同时有助于金融行业的数据安全保护和应用的标准化，推动金融业机构形成统一规范的数据安全防护体系，利于各组织和机构间数据互联互通，从其数据安全保护措施中获得最大化价值。

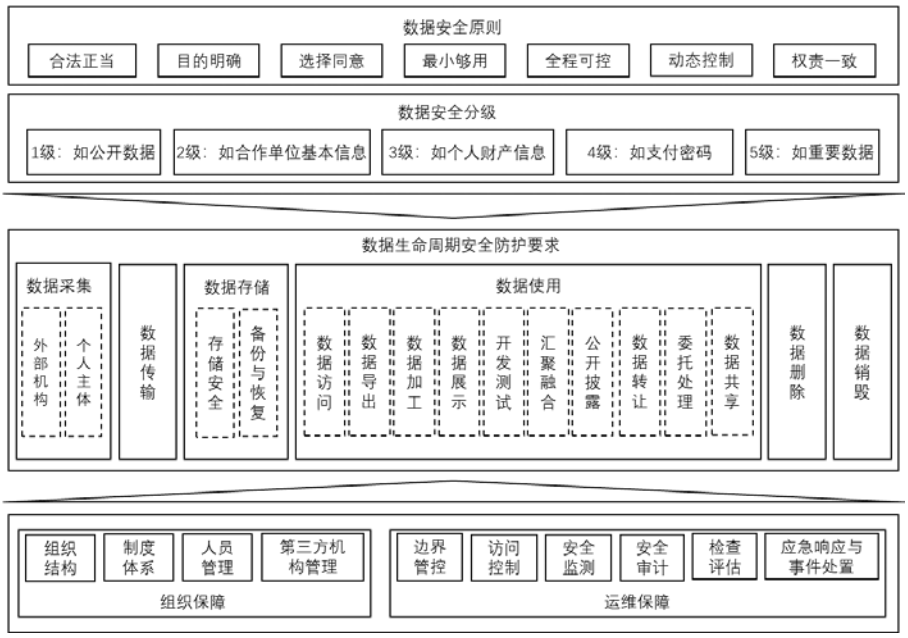
三、内容解读

1. 适用范围

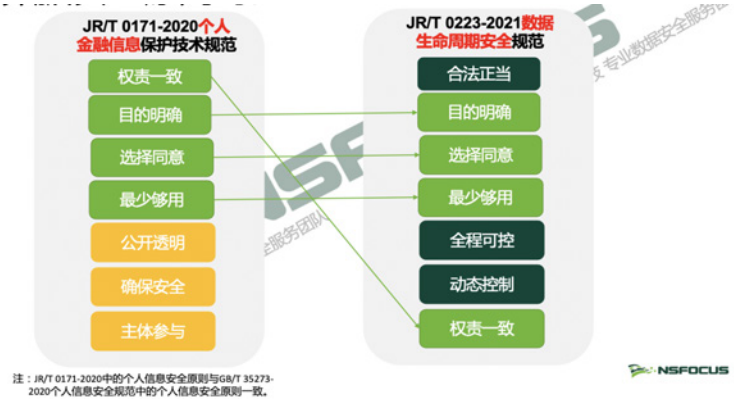
《规范》适用于指导金融业机构开展电子数据安全防护工作，并为第三方测评机构等单位开展数据安全检查与评估工作提供参考。需要注意的是，证券期货业仍参照JR/T0158-2018《证券期货业数据分类分级指引》等证券行业标准开展数据安全分类分级和保护工作。

2. 数据安全框架

《规范》中构建的数据生命周期安全框架遵循数据安全原则，以数据安全分级（JR/T 0197 金融数据安全分级指南）为基础，建立覆盖数据生命周期全过程的安全防护体系，并通过建立健全数据安全组织架构和明确信息系统运维环节中的数据安全需求，全面加强金融业机构数据安全保护能力。



3. 数据安全原则



个人信息安全规范、个人金融信息保护技术规范与《规范》三者约束的对象是不同的。由于个人金融信息与金融数据的差异，对应的数据安全或个人信息保护的基本原则也不尽相同。

个人金融信息保护技术规范中“公开透明、确保安全、主体参与”原则强调对金融信息主体的权利和权益。《规范》中不同于另两个标准的原则是“合法正当、全程可控、动态控制”，这三个原则更多的是站在金融业机构在使用金融数据过程中需要站在安全与发展并重的基础上，这也是数据安全保护与个人信息保护的最大区别。

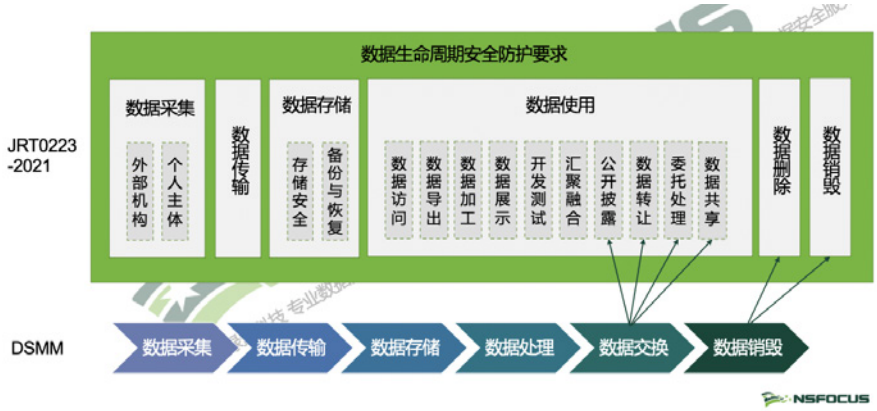
4. 数据安全分类分级

《规范》所构建的数据生命周期安全框架，是以数据分类分级作为基础的。金融数据安全级别应按照JR/T 0197—2020相关要求，根据安全性遭到破坏后的影响范围和影响程度，将金融数据安全级别由高到低划分为5级、4级、3级、2级、1级。

最低安全级别参考	数据定级要素		数据一般特征
	影响对象	影响程度	
5	国家安全	严重损害/一般损害/轻微损害	• 重要数据，通常主要用于金融行业大型或特大型机构、金融交易过程中重要核心节点类机构的关键业务使用，一般针对特定人员公开，且仅为必须知悉的对象访问或使用； • 数据安全性遭到破坏后，对国家安全造成影响，或公众权益造成严重影响。
5	公众权益	严重损害	
4	公众权益	一般损害	• 数据通常主要用于金融行业大型或特大型机构金融交易过程中重要核心节点类机构的重要业务使用，一般针对特定人员公开，且仅为必须知悉的对象访问或使用； • 个人金融信息中的C3类信息； • 数据安全性遭到破坏后，对公众权益造成一般影响，或对个人隐私或企业合法权益造成严重影响，但不影响国家安全。
4	个人隐私	严重损害	
4	企业合法权益	严重损害	
3	公众权益	轻微损害	• 数据用于金融业机构关键或重要业务使用，一般针对特定人员公开，且仅为必须知悉的对象访问或使用； • 个人金融信息中的C2类信息； • 数据的安全性遭到破坏后，对公众权益造成轻微影响，或对个人隐私或企业合法权益造成一般影响，但不影响国家安全。
3	个人隐私	一般损害	
3	企业合法权益	一般损害	
2	个人隐私	轻微损害	• 数据用于金融业机构一般业务使用，一般针对受限对象公开，通常为内部管理且不宜广泛公开的数据； • 个人金融信息中的C1类信息； • 数据的安全性遭到破坏，对个人隐私或企业合法权益造成轻微影响，但不影响国家安全、公众权益。
2	企业合法权益	轻微损害	
1	国家安全	无损害	• 数据一般可被公开或可被公众获知、使用； • 个人金融信息主体主动公开的信息； • 数据的安全性遭到破坏，可能对个人隐私或企业合法权益不造成影响或仅造成微弱影响，但不影响国家安全、公众权益。
1	公众权益	无损害	
1	个人隐私	无损害	
1	企业合法权益	无损害	

NSFOCUS

5. 数据生命周期安全防护要求

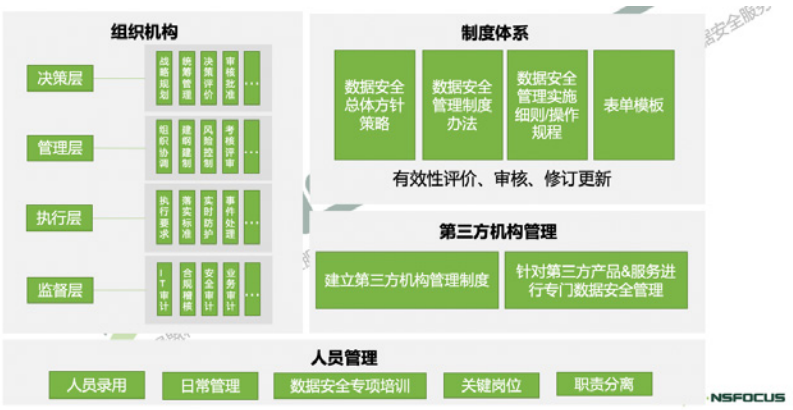


《规范》与数据安全能力成熟度模型DSMM中数据生命周期阶段划分的主要区别在于数据交换和数据销毁。《规范》中没有单独划分数据交换这个阶段，均纳入到数据使用这一阶段中，并划分不同场景。

两者对于数据生命周期阶段划分不完全一致的主要原因是基于业务的实践。《规范》针对金融行业自身的业务实践和金融数据特性得出的，而DSMM是适用于各行业的通用标准。同时DSMM架构也指出，特定的数据所经历的生存周期由实际的业务所决定，可为完整的6个阶段或是其中的几个阶段，所以《规范》与DSMM的数据生命周期仍是一致的。

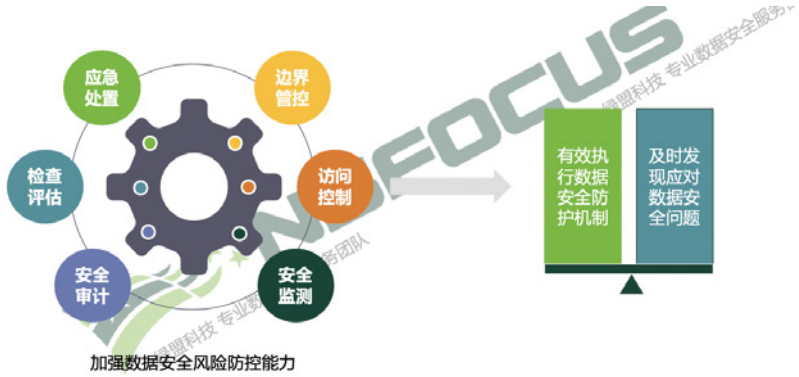
6. 组织保障

《规范》中的数据安全组织保障要求可以确保数据安全工作具有包括决策层、管理层、执行层以及监督层的完善管理体系，为数据安全相关工作的组织和落实奠定基础。



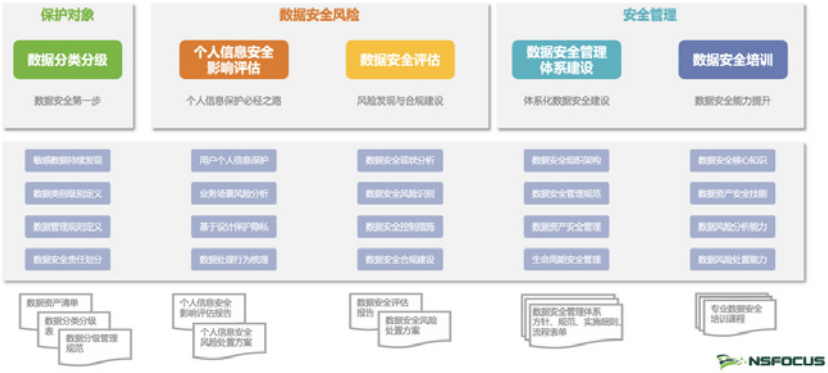
7. 运维保障

在金融业机构的日常运营过程中，应加强在边界管控、访问控制、安全监测、安全审计、检查评估、应急响应与事件处置等过程中的数据安全风险防控能力，可以有力保障数据安全防护机制的有效执行和数据安全问题的及时发现与应对。



四、绿盟科技数据安全服务方案

绿盟科技设计开发了整套数据安全服务方案并经过了多次实际验证，能够为金融业机构提供一系列数据安全咨询服务，包括数据分类分级、数据安全评估、数据安全管理体系建设以及数据安全专业培训。



同时可结合绿盟科技多年的安全技术能力和安全运营能力，实现对数据基础资源的管理和数据安全风险的运营，帮助金融业客户打造数据安全的整体防护体系。

筑牢国家安全屏障 | 《关键信息基础设施安全保护条例》浅析

两个统筹、四个基本问题

——绿盟科技

近日，国务院正式颁布《关键信息基础设施安全保护条例》（以下简称《条例》）。《条例》的颁布，不仅提升了我国关键信息基础设施安全保护依据的效力层级，更对一系列重要制度、机制加以完善和固化，必将推动开启我国关键信息基础设施安全保护的新格局。

一、总体特点概述：两个统筹

《条例》共六章51条，第一章总则（第一至七条）、第二章关键信息基础设施认定（第八至十一条）、第三章运营者责任义务（第十二至二十一条）、第四章保障和促进（第二十二至三十八条）、第五章法律责任（第三十九至四十九条）、第六章附则（第五十至五十一条）。除法律责任和附则外，《条例》重点通过前四个章节对关键信息基础设施保护攸关的管理体系、适用对象、主体责任和管理职责进行了规定。

整体来看，《条例》内容集中体现了“两个统筹”的特点。一是注重立法内容的统筹。与此前的征求意见版本相比，《条例》大幅减少了有关授权立制（规定、标准）的内容，对相关保护工作要求尽可能在条文中明确、不再过多以开放的方式留待未来制度或标准解决。从而能够大大减少因立制周期长带来的效率延误。二是注重权责划分的统筹。《条例》立足关键信息基础设施保护工作不同主体的核心职能优势，进一步明确了各主体担负的权责、明确了各主体间的工作协同机制。这无疑有利于减少因工作边界不清等带来的效率延误，也可充分调动各方面在保护工作中的主体意识和主动性。关键信息基础设施安全是网络安全的重要一环，《条例》通过“两个统筹”举措的提升，为我国关键信息基础设施的网络安全保护工作奠定良好的效率基础。

二、主要内容分析：四个基本问题

从内容来看，关键信息基础设施的范围界定、管理体系、检查检测机制

和责任机制是《条例》所要重点明确的加强关键信息基础设施安全保护的四个基本问题。

（一）关键信息基础设施的范围界定

关键信息基础设施的范围如何界定，是开展保护要明确的首要和基础性问题，也是《网络安全法》颁布实施以来各界最为关切的问题之一。《条例》采用了“范围列举+授权认定”的方法，对关键信息基础设施的内涵和外延做出规定。

在范围列举方面。《条例》第二条将关键信息基础设施定位于“重要网络设施和信息系统”，并以列举方式明确了其行业属性和影响属性两大界定标准：一是“公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等”8个重要行业和领域；二是“一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益”。

在授权认定方面。《条例》除了在总则第二条进行总体界定外，还以专章（第二章 关键信息基础设施认定）对授权认定做出了规定，这是在关键信息基础设施范围界定方面的一大创新。《条例》对授权认定主要明确了两个要点：一是认定主体，即“关键信息基础设施安全保护工作的部门”（以下称保护工作部门），主要包括了《条例》第二条所述8个重要行业和领域的主管或监管部门；二是认定依据，即“关键信息基础设施认定规则”，《条例》第九条还明确了制定“认定规则”时应依据的“重要程度”“危害程度”和“关联影响”三个主要考量因素。此外，《条例》还对关键信息基础设施的认定流程、报备主体、变更认定做出了规定。

（二）关键信息基础设施安全监管体系

《条例》在《网络安全法》所确定的管理框架内，对关键信息基础设施保护的管理体系进行了细化，进一步强化了保护工作的组织管理基础。《条例》对保护管理体系的规定，主要有以下三方面：

一是确立了管理分类模式。《条例》将管理部门分为三类，即：统筹协调部门（国家网信部门）、指导监督部门（国务院公安部门）、保护工作部门（重要行业和领域的主管、监管部门）。各类管理部门分工不同、又协同配合，共同构成我国关键信息基础设施保护的监管体系，缺一不可。

二是确立了管理分层模式。《条例》主要规定了属地、行业两种管理分层。从属地分层模式来看，《条例》第三条明确了“省级人民政府有关部门”是监

管和保护工作在地方的实施主体，相比之前征求意见稿中的“县级以上”提升了层级，突出了关键信息基础设施保护实施的统筹性要求。从行业分层模式来看，《条例》第三十二条强调“优先保障能源、电信等关键信息基础设施安全运行”，并明确能源、电信行业“为其他行业和领域的关键信息基础设施安全运行提供重点保障”，可见行业属性的特点决定了该两类行业在关键信息基础设施保护中，应发挥更加基础的保障作用。

三是明确了重点管理内容。在确立监管分级分类模式的基础上，《条例》对主要部门的管理内容也做了相应规定。如：国家网信部门统筹协调相关部门建立网络安全信息共享机制、及网络安全检查检测等；国务院公安部门负责开展关键信息基础设施认定相关备案、打击相关违法犯罪活动等；各保护部门负责制定本行业、本领域关键信息基础设施安全规划等。通过对重点管理内容的明确，有助于增进关键信息基础设施运营单位、以及相关产学研用等社会各界对关键信息基础设施保护工作的知悉度，推动形成共识与合力，保障保护工作的推进实施。

（三）关键信息基础设施安全检查检测机制

在明确监管和运行要求的同时，《条例》注重对相关要求落地实施情况的监督手段建设，设置了专门的检查检测机制。

《条例》规定的关键信息基础设施安全检查检测机制由三部分构成。一是运营检测。该类检测的执行主体是关键信息基础设施运营者，具体开展形式可以自行开展也可以委托网络安全服务机构开展。运营检测应定期开展“每年至少进行一次网络安全检测和风险评估”，并需要按要求将检测结果报保护工作部门。二是保护部门检查检测。该类检查检测由保护工作部门组织开展，目的是通过检查检测对运营者予以指导监督，及时整改安全隐患、完善安全措施。三是监督检查检测。该类检查检测由国家网信部门统筹协调，国务院公安部门、保护工作部门开展，通过检查提出改进措施意见。

这三类检测检查工作由不同主体负责，分别立足于运营、保护、监督的不同要求，共同构建起对关键信息基础设施安全合规的监测防线。尤其值得一提的是，《条例》明确规定了监督检查工作的统筹机制，这不仅有利于提升检查工作效率，更在切实减轻监管对象合规负担方面迈出了坚实的一步。

（四）关键信息基础设施安全责任机制

《条例》对关键信息基础设施安全保护重要环节提出了合规要求，并规定了相应的法律责任，以法律威慑手段强化对各项保护职责的落实保障。《条例》对

于责任机制的规定主要有三个要点。

一是突出主体责任。《条例》首先对“主体责任”做出界定，即第四条明确的“强化和落实关键信息基础设施运营者主体责任”，这充分反映了运营者在整个保护工作中，因其肩负重要职责而具有的不可替代作用。根据《条例》第三章“运营者责任义务”，我们可以将运营者肩负的重要职责归纳为：建设管理、安全审查、事件报告、检查配合等4类13项。对于这些职责和义务，《条例》在第五章“法律责任”中，也做出了逐条对应的责任规定。

二是健全责任范围。《条例》在强化主体责任（运营责任）的基础上，还明确了监管责任、保护责任，使责任机制覆盖了保护工作的全部主体和全部主要职责。对于监管部门的监督管理行为、保护部门的保护指导行为，以及其他个人或组织实施的恶意破坏行为等，都明确规定了相应的法律责任，从而形成对关键信息基础设施保护工作的全方位责任保障。

三是明确责任方式。《条例》规定的责任方式，涵盖了行政责任、民事责任和刑事责任三大类别。其中，对于大部分运营者责任适用行政责任的追究方式，包括责令改正、警告和罚款等；对于监管人员的违法行为，主要适用行政或刑事责任；对于从事破坏行为的其他个人，除了适用相应的拘留、罚款等行政责任外，还对该人员的网络安全从业资格做出限制，与《条例》规定的相关岗位人员背景调查相衔接。

三、展望

《条例》的颁布实施，无疑是我国关键信息基础设施安全保护工作的一个重要里程碑。而《条例》自身内容的完善也将是一个循序渐进的过程。例如，省级相关部门在具体实施工作中与行业保护工作部门如何衔接？关键信息基础设施的日常检测与其系统上线前测试如何衔接？监督检查和保护检查检测工作的频次、实施流程如何规范？等等。这些问题，都既需要保护工作实践的验证推进，也需要相关制度规范的延续拓展。

“雄关漫道真如铁，而今迈步从头越”。《条例》已经开启了我国关键信息基础设施安全保护工作的新阶段序章，如何开创和巩固关键信息基础设施安全保护工作的新格局，更呼唤主管部门、行业企业和社会各界的同心戮力。

Zimbra 新漏洞或造成 20 万家企业数据泄漏

摘　要：Zimbra 是一套开源协同办公套件，包括 WebMail、日历、通信录、Web 文档管理和创作。它通过将终端用户的信息和活动连接到私有云中，为用户提供了最具创新性的消息接收体验，因此每天有超过 20 万家企业和 1000 多家政府、金融机构使用 Zimbra 与数百万用户交换电子邮件。

关键词：标签（数据泄露、Zimbra、政府、金融机构），技术问题（安全事件）。

内　容：SonarSource 的专家近期披露了开源 Zimbra 代码中的两个漏洞。这些漏洞可能使未经身份验证的攻击者破坏目标企业的 Zimbra 网络邮件服务器。借此，攻击者就可以不受限制的访问所有员工通过 Zimbra 传输的电子邮件内容。

劫持 Zimbra 服务器的漏洞：

CVE-2021-35208（CVSS 评分：5.4）——跨站脚本错误（XSS）

CVE-2021-35209（CVSS 评分：6.1）——服务器端请求伪造漏洞(SSRF)

安全专家表示，当用户浏览查看 Zimbra 传入的电子邮件时，就会触发跨站点脚本(CVE-2021-35208)漏洞。

恶意电子邮件会包含一个精心设计的 JavaScript 有效负载，当该负载被执行时， 攻击者将能够访问受害者所有的电子邮件（除了他们的 WEBmail

会话）。并获取受害者在 Zimbra 组件中其它功能的访问权限，发起进一步的攻击。

另一个服务器端请求伪造漏洞 (CVE-2021-35209)，绕过了访问控制的允许列表，导致强大的服务器端请求伪造。研究人员指出，该漏洞可以被任何权限角色的经过身份验证的组织成员利用。

上述情况说明了一个这样的事实：基于 Ajax、静态 HTML 和移动优化的 Zimbra 网页客户端，以一种使破坏者注入恶意的 JavaScript 代码的方式，执行清除服务器端接收邮件中的 HTML 内容。

SSRF 漏洞威胁强大有 2 个原因

SSRF 漏洞已经成为一个越来越危险的威胁类别，对云本地应用尤甚。之所以强大一是因为它可以在传出请求中设置任意标头，其次是可以读取响应内容。

如果 Zimbra 实例托管在云供应商处，可以从托管服务器的 VM 访问元数据 API， 则可能会泄漏高敏感信息。

缓解措施

安全专家指出，通过禁止 HTTP 请求处理程序执行重定向的方式来减轻 SSRF 攻击。建议验证 Location 响应报头的值，并在它被验证后创建新的请求。这样可以保护开放的重定向漏洞。XSS 攻击也可以通过完全删除转换表单标签的代码的方式来修复。

可用的补丁

Zimbra 团队修复了 8.8.15 系列的 Patch 18 和 9.0 系列的 Patch 16 的所有问题，这两个分支的早期版本都有脆弱性漏洞。

信息来源：

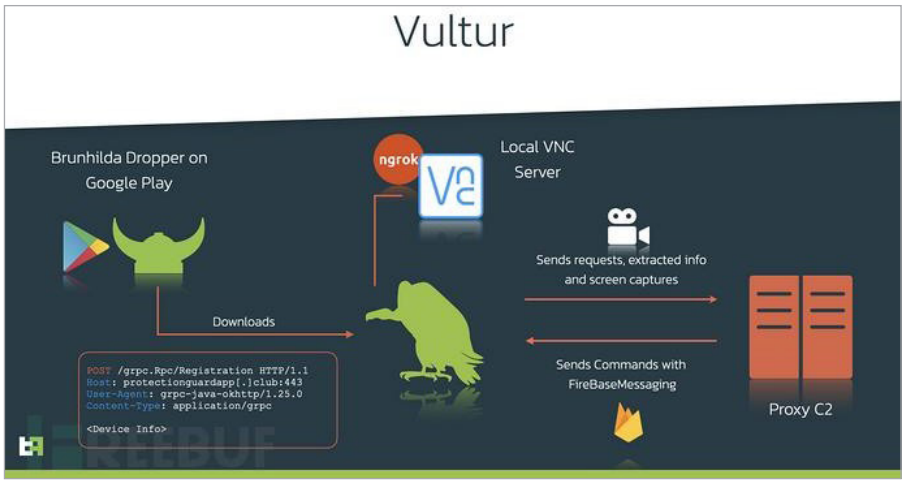
https://mp.weixin.qq.com/s/QbrrIuZffdrp0EleLiVzcQ

你的屏幕被“偷”了，新恶意软件 Vultur 已控制数千台设备

摘　要：最近研究人员在 Google Play 中发现一种新型 Android 恶意软件，已经波及了一百多个银行和加密货币应用程序。

关键词：标签（Google Play、安卓、银行木马、加密货币），技术问题（安全事件）。

内　容：荷兰安全公司 ThreatFabric 的研究人员将该种恶意软件命名为 Vultur。该恶意软件会在目标应用程序打开时记录屏幕，Vultur 会使用 VNC 屏幕共享将失陷主机的屏幕镜像到攻击者控制的服务器。

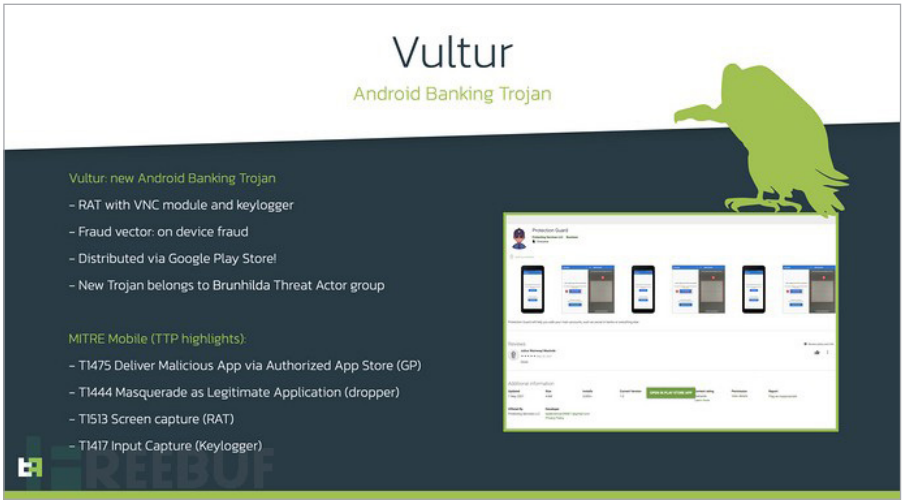


欺诈新时代

Android 窃密恶意软件的典型手法是在目标应用程序的登陆窗口上叠加一层透明窗口或者与目标应用程序相同的界面窗口。将用户的隐私信息收集起来，再

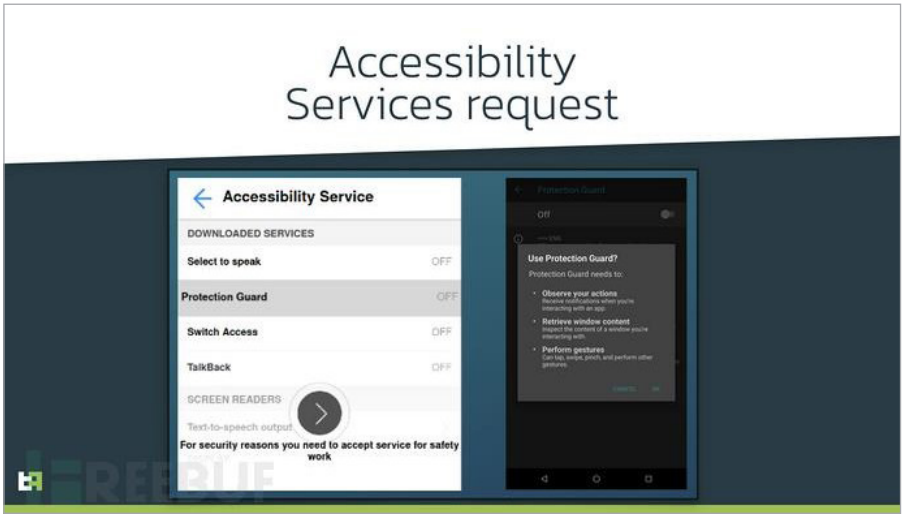
换一个地方转移资金。

ThreatFabric 的研究人员在 Vultur 中发现：“移动平台上的窃密威胁不再仅仅基于众所周知的覆盖层攻击，而是演变成类似远控的恶意软件，却也继承了检测前台应用程序并开始屏幕录制等传统方式”。



这就将威胁继续推高到另一个水平，Vultur 的攻击是可以扩展并自动化的，欺诈的手法可以在后端编写脚本并下发到受害设备。

与许多 Android 银行木马程序一样，Vultur 严重依赖于移动操作系统中内置的辅助功能服务。首次安装时，Vultur 会滥用这些服务来获取所需的权限。而一旦安装成功，Vultur 就会监控所有触发无障碍服务的请求。

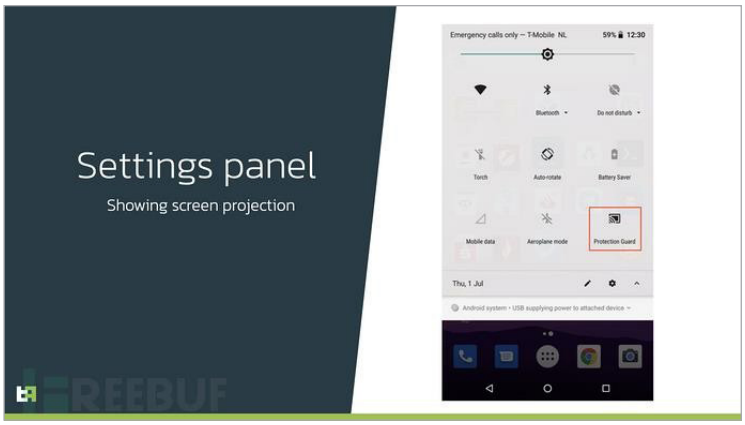


隐蔽性更强

Vultur 使用这些服务监测来自目标应用程序的请求，恶意软件还使用这些服务通过一般手段对恶意软件进行删除和清理。每当用户尝试访问 Android 设置中的应用程序详细信息页时，Vultur 都会自动单击后退按钮。这会妨碍用户点击卸载按钮，而且Vultur 也隐藏了它自己的图标。

Vultur 保持隐蔽的另一种方式：安装它的应用程序是功能齐全的应用程序，实际上会提供真正的服务，例如健身追踪或双因子身份验证。然而不管怎么伪装，Vultur 都会以投影屏幕的形式出现在 Android 通知面板中，这就暴露了它。

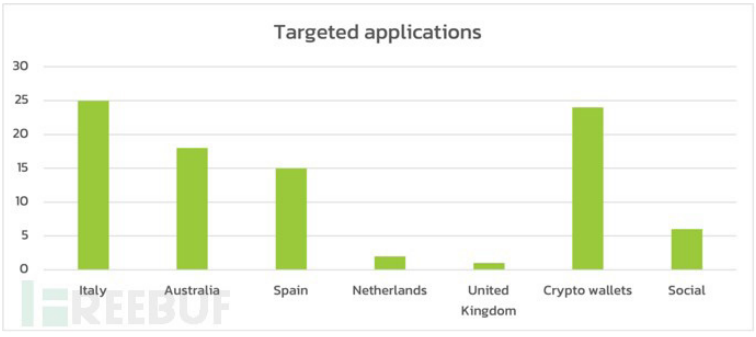
安装成功后，Vultur 会使用 Alpha VNC 的 VNC 开始进行屏幕录制。为了提供对在受感染设备上运行的 VNC 服务器的远程访问，Vultur 使用 ngrok，该应用程序会使用加密隧道将隐藏在防火墙后面的本地系统暴露给公共互联网。



Vultur 会由 Dropper 程序来安装，ThreatFabric 已经在 Google Play 中发现了两个安装 Vultur 的 Dropper 应用程序。共计影响了超过 5000 台设备，与其他依赖第三方 Dropper 的 Android 恶意软件不同，Vultur 使用被称为 Brunhilda 的自定义 Dropper。 Brunhilda 与 Vultur 是由同一个组织开发的，而 Brunhilda 过去曾被用来安装不同

的 Android 银行恶意软件。据估计，Brunhilda 一共感染了超过 3 万台设备。

Vultur 针对 103 个Android 银行应用程序或加密货币应用程序进行窃密，意大利、澳大利亚和西班牙是受攻击最多的国家。



除了银行应用程序和加密货币应用程序外，该恶意软件还会收集 Facebook、WhatsApp Messenger、TikTok 和 Viber Messenger 的凭据。

Google 已经删除了所有已知包含 Brunhilda 的 Googel Play 应用程序，但 Google 表示新的木马应用程序可能仍会出现。Android 用户应该只安装提供有用服务的应用程序，而且尽可能只安装来自知名发行商的应用程序。

信息来源：

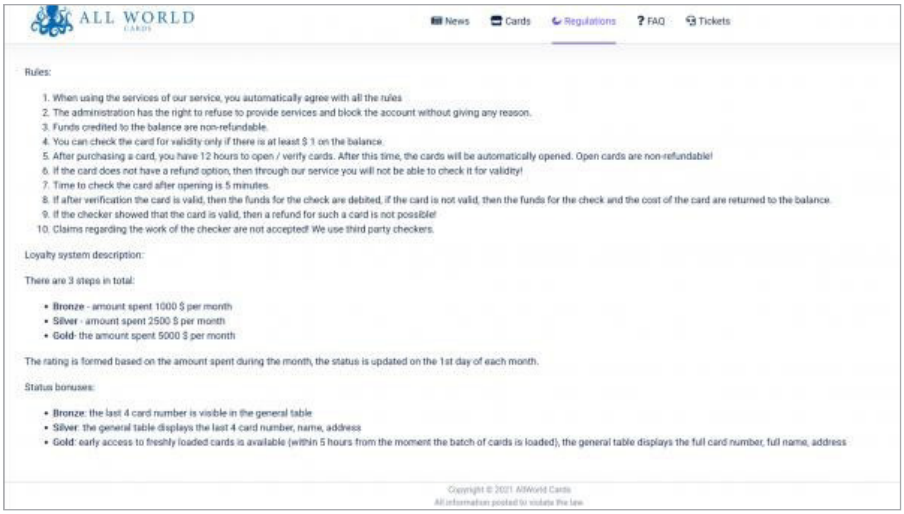
https://www.freebuf.com/news/282992.html

100 万张被盗信用卡在暗网曝光

摘　要：据外媒 softpedia 报道，根据 Threat Post 的说法，一群网络罪犯建立了一个专门在线销售支付卡数据的网站–AllWorld.Cards。威胁行为者泄露了100万张被盗信用卡（收集于 2018 年至 2019 年期间）以帮助宣传他们的犯罪活动。

关键词：标签（数据泄露、信用卡），技术问题（安全事件）。

内　容：来自 Cyble 的网络安全研究人员在对暗网市场和网络犯罪活动进行定期检查时发现了这一漏洞。据研究人员称，该市场在 2021 年 5 月左右开始运营，可以通过 TOR 网络和 Clearnet 访问。意大利 D3 实验室的研究人员在一篇帖子中指出：“可以想象，这些数据是免费共享的，目的是从毫无防备的受害者那里购买额外的被盗数据以引诱其他犯罪分子频繁访问他们的网站。”



正如网络犯罪分子所说的那样，在他们的平台上暴露的信用卡信息包括从一个人的姓名到他们居住的地址、邮政编码、电话号码、信用卡号码和到期日等所有信息。信用卡及一些礼品卡在用于付款时很难追溯到交易的来源。

信用卡数据盗窃在黑市上是一项利润丰厚的业务，黑客可以通过各种方法获取信用卡信息，包括社交工程。针对网站的 Magecart 攻击和从网站窃取信息的木马则是最常用的技术。

根据 Cybersixgill 的数据，在 2020 年的最后六个月里，有超 4500 万张被泄露的信用卡可以在地下信用卡市场上销售。虽然目前尚不清楚有多少卡遭到滥用，但样本中 27%的卡是活跃的并且可能被用于非法购买。

Cyble 根据被发现的信用卡被盗数量编制了 500 强金融公司名单。根据最新数据显示，这一名单包括西班牙对外银行（24307 张卡）、摩根大通银行（27441 张卡）、萨顿银行（30480 张卡）、桑坦德银行（拥有 38010 张卡）、印度国家银行（72937 张卡）。

信息来源：

https://hackernews.cc/archives/35776

日本最大财险公司遭勒索软件攻击：保险行业已成为主要攻击目标

摘　要：日本国内收入最高的财险集团东京海上披露称，新加坡分公司遭到了勒索软件袭击；今年已有多家大型保险公司遭到勒索软件毒手，REvil勒索软件团伙的一名代表表示，保险公司已经成为勒索攻击者眼中极具吸引力的目标。

关键词：标签（勒索软件、保险公司、日本），技术问题（安全事件）。

内　容：日前，日本跨国保险公司东京海上控股（Tokio Marine Holdings）披露称，新加坡分公司新加坡东京海上保险（TMiS）遭受勒索软件攻击。

该公告于本周初发布，除了披露应对措施之外，公告中几乎没有任何事件细节。攻击影响不大

作为日本国内收入最高的财产与意外伤害保险集团，东京海上无疑是网络犯罪分子眼中极具吸引力的目标。他们也一直在寻求可行漏洞，希望从东京海上的客户身上榨取收益。

东京海上指出，此次勒索软件攻击主要影响的是其新加坡东京海上保险分部，集团在新加坡国内的其他公司并未受到波及。

目前还不清楚攻击发动于何时、如何展开，也不明确具体造成了怎样的后果。但新加坡分部在发现问题后立即实施了网络隔离，并向当地政府机构发出通报。

母公司则表示，目前可以“确认没有迹象表明集团的任何客户信息或机密信息遭到泄露。”

目前，大部分勒索软件攻击事件也伴随有数据泄露问题，越来越多的攻击者会在加密之前从受害者网络中窃取敏感文件。

然而，东京海上已经引入第三方机构开展系统分析并评估攻击影响。

该公司在官方网站上以日文及英文通报披露了此次事件，就并“造成的一切不便及担忧”向广大客户致歉。

保险公司成主要攻击目标

外媒 CyberScoop 的 Tim Starks 表示，东京海上是本周第二家宣布遭受网络攻击的保险企业。周一，Ryan Specialty Group 表示今年 4 月曾检测到部分员工账户遭到未授权访问。

此外，今年年初还有其他几家大型保险公司沦为勒索软件攻击的受害者。

今年 3 月，美国第七大商业保险公司 CNA Financial Corporation 遭遇 Phoenix CrypotoLocker 勒索软件攻击，攻击方还窃取了包含客户信息的文件。

今年 5 月，Avaddon 勒索软件团伙攻击了 AXA 在泰国、马来西亚、香港及菲律宾的多家分支机构，并宣称成功窃取到 3 TB 数据。

在早些时候，REvil 勒索软件团伙的一名代表还接受了 Recorded Future 情报分析师 Dmitry Smilyanets 的采访，并坦言保险公司已经成为勒索攻击者眼中极具吸引力的目标。

这位代号“未知”（Unknown）的代表宣称，保险公司是“最鲜嫩多汁的美味”。他们可以通过黑客攻击触及保险公司的客户群体，并以客户为要挟向保险企业施压。

“没错，他们是最鲜嫩多汁的美味。最好的办法是先入侵保险公司，触及他们的客户群体并据此收集针对性的攻击方式。在整理好策略之后，即可向保险企业发动冲击。”--Unknown, REvil 团伙代表

信息来源：

https://mp.weixin.qq.com/s/ tOL7wADwR0KaW086GdvQ

摘　要：这是勒索软件首次成功攻击国家核心金融系统，勒索软件已成为全球网络空间安全的重大破坏因素之一。

关键词：标签（金融保险、网络攻击、勒索软件、巴西国库），技术问题（安全事件）。

内　容：

- 巴西经济部表示，国库在 8 月 13 日遭遇勒索软件攻击，经相关措施处理，初步评估显示未对其造成损害；
- 这是勒索软件首次成功攻击国家核心金融系统，勒索软件已成为全球网络空间安全的重大破坏因素之一。

巴西政府发布声明称，巴西国库（National Treasury）在 8 月 13 日遭遇勒索软件攻击。

巴西经济部表示，他们立即采取了相关措施，以遏制网络攻击引发的影响。初步评估显示，包括公共债务管理平台在内的国库体系化系统没有受到损害。

巴西国库和数字政府秘书处的安全专家们正在此次分析勒索软件攻击引发的影响，联邦警察也已收到通报。国库指出，关于事件的最新消息“将及时披露并保持适当的公开透明度”。

8 月 16 日，巴西证券交易所联合发布的另一份声明则提到，此次攻击并未“以任何方式”影响到巴西政府的个人债券购买项目 Tesouro Direto。

在此次巴西国库遭遇攻击之前，2020 年 11 月巴西高等选举法院就曾经受到重大网络攻击的影响，并导致法院系统瘫痪达两个多星期。

当时，该事件以其远超常规的复杂性和所造成的损害范围，被认为是有史以来针对巴西公共部门策划的最全面的攻击。

今年 7 月，巴西政府宣布将建立一个网络攻击响应网络，希望协调联邦政府各部门，以促进对网络威胁及漏洞的快速响应能力。

隶属于经济部的数字政府秘书处将在该响应网络的构建工作中发挥重要作用。数字政府秘书处属于 SISP 系统的中央负责机构，这套系统专门用于规划、协调、组织、运营、控制并监控联邦政府 200 多个机构之内的信息技术资源。

2021 年，巴西境内有多家大型企业同样受到重大勒索软件攻击的影响，包括医疗保健企业 Fleury、巴西航空工业公司等。

信息来源：

https://www.secrss.com/articles/33567

NSFOCUS

漏洞聚焦

INFRAHALT：NicheStack TCP/IP 堆栈多个高危漏洞通告

一、漏洞概述

近日，JFrog 和 Forescout 的研究人员发布了一份联合报告，公开披露了在 NicheStack TC P/IP 堆栈中发现的 14 个安全漏洞(统称为 INFRA:HALT)，这些漏洞可导致远程代码执行、拒绝服务、信息泄漏、TCP 欺骗或 DNS 缓存中毒。研究人员表示，成功利用 INFRA:HALT 漏洞的攻击者可能会破坏建筑物的 HVAC 系统或接管用于制造和其它关键基础设施的控制器，导致 O T 和 ICS 设备离线并被劫持，并且攻击者可以通过劫持的设备传播恶意软件。

CVE-2020-25928：解析 DNS 响应时发生越界读/写，导致远程代码执行，CVSS 评分：9.8 CVE-2021-31226：解析 HTTPpost 请求时的堆缓冲区溢出漏洞，可导致远程代码执行，CVSS 评分：9.1

CVE-2020-25927：解析 DNS 响应时越界读取，可导致拒绝服务，CVSS 评分：8.2

CVE-2020-25767：解析 DNS 域名时越界读取，可导致拒绝服务和信息泄露，CVSS 评分：7.5 CVE-2021-31227：解析 HTTPpost 请求时的堆缓冲区溢出漏洞，可导致拒绝服务，CVSS 评分： 7.5

CVE-2021-31400：TCP 带外紧急数据处理功能中存在无限循环情况，导致拒绝服务，CVSS 评分：7.5

CVE-2021-31401：TCP 头部处理代码中的整数溢出漏洞，CVSS 评分：7.5

CVE-2020-35683：解析 ICMP 数据包时越界读取，导致拒绝服务，CVSS 评分：7.5 CVE-2020-35684：解析 TCP 数据包时越界读取，导致拒绝服务，CVSS 评分：7.5

CVE-2020-35685：TCP 连接中可预测的初始序列号 (ISN)，导致 TCP 欺骗，CVSS 评分：7.5 CVE-2021-27565：收到未知 HTTP 请求时出现拒绝服务情况，

CVSS 评分：7.5

CVE-2021-36762：TFTP 数据包处理功能中的越界读取，导致拒绝服务，CVSS 评分：7.5

CVE-2020-25926：DNS 客户端没有设置足够随机的事务 ID，导致缓存中毒，CVSS 评分：4.0 CVE-2021-31228：可以预测 DNS 查询的源端口发送伪造的 DNS 响应包，导致缓存中毒，CVSS 评分：4.0

NicheStack（又名 InterNiche）是一个常用的、专有的嵌入式系统 TCP/IP 堆栈，旨在提供互联网连接工业设备，被至少 200 家供应商用于生产环境，并被部署在制造厂、发电、水处理等关键基础设施领域的数百万个操作技术（OT）设备中。

参考链接：

https://jfrog.com/blog/infrahalt-14-new-security-vulnerabilities-found-in-nichestack/
https://www.forescout.com/blog/new-critical-operational-technology-vulnerabilities-found-on-nichestack/

二、影响范围

受影响版本

☐ NicheStack < 4.3

不受影响版本

☐ NicheStack = 4.3

三、漏洞检测

人工监测

用户可使用 Forescout 发布的开源脚本（持续更新签名），检测运行 NicheStack 的设备：

https://github.com/Forescout/project-memoria-detector

建议相关用户实施分段控制，监控恶意数据包的所有网络流量，以降低易受攻击设备的 风险。

四、漏洞防护

官方升级

目前 HCC Embedded 官方已发布新版本中修复了以上漏洞，请受影响的用户尽快升级 Ni cheStack 版本进行防护，下载链接：

https://www.hcc-embedded.com/support/security-advisories

Linux Kernel 任意代码执行漏洞（C VE-2021-3490）通告

一、漏洞概述

近日，绿盟科技 CERT 监测到有研究人员公开披露了 eBPF 中的一个任意代码执行漏洞（C VE-2021-3490）的细节信息和 PoC，并演示利用此漏洞在 Ubuntu 20.10 和 21.04 上实现本地权限提升，该漏洞是由于 Linux 内核中按位操作（AND、OR 和XOR）的eBPF ALU32 边界跟踪没有正确更新 32 位边界，造成 Linux 内核中的越界读取和写入，从而导致任意代码执行。官方已于 5 月 11 号发布修复版本，请相关用户及时采取措施防护。

ExtendedBerkeley Packet Filter（eBPF）是一种内核技术（从 Linux 4.x 开始），允许程序运行而无需改变内核源代码或添加额外的模块。它是 Linux 内核中的一种轻量级的沙盒虚拟机（V M），可以在其中运行利用特定内核资源的 BPF 字节码。

参考链接：

https://www.openwall.com/lists/oss-security/2021/05/11/11

二、影响范围

受影响版本

☐ Linux kernel < 5.13-rc4

三、漏洞检测

3.1 版本检测

Linux 系统用户可以通过查看版本来判断当前系统是否在受影响范围内，查看操作系统版本信息命令如下：

```
cat /proc/version
```

```
[root@test ~]# cat /proc/version
Linux version 3.10.0-514.26.2.el7.x86_64 (builder@kbuilder.dev.centos.org) (gcc version 4.8.5 20150623 (Red Hat 4.8.5-11) (GCC) ) #1 SMP Tue Jul 4 15:04:05 UTC 2017
```

四、漏洞防护

4.1 官方升级

目前官方已在新版本中修复了该漏洞，请受影响的用户尽快升级版本进行防护，官方下 载链接：https://www.kernel.org

方法一、通过升级 Linux 系统内核的方式进行防护。下载链接：https://github.com/torvalds/linux/releases

方法二、Linux 代码库已发布补丁，请相关用户尽快应用此补丁。详细信息可参见：

https://git.kernel.org/pub/scm/linux/kernel/git/bpf/bpf.git/commit/?id=049c4e13714ecbc a567b4d5f6d563f05d431c80e

Windows Print Spooler 远程代码执行 0day 漏洞（CVE-2021-36958）通告

发布时间：2021-08-11

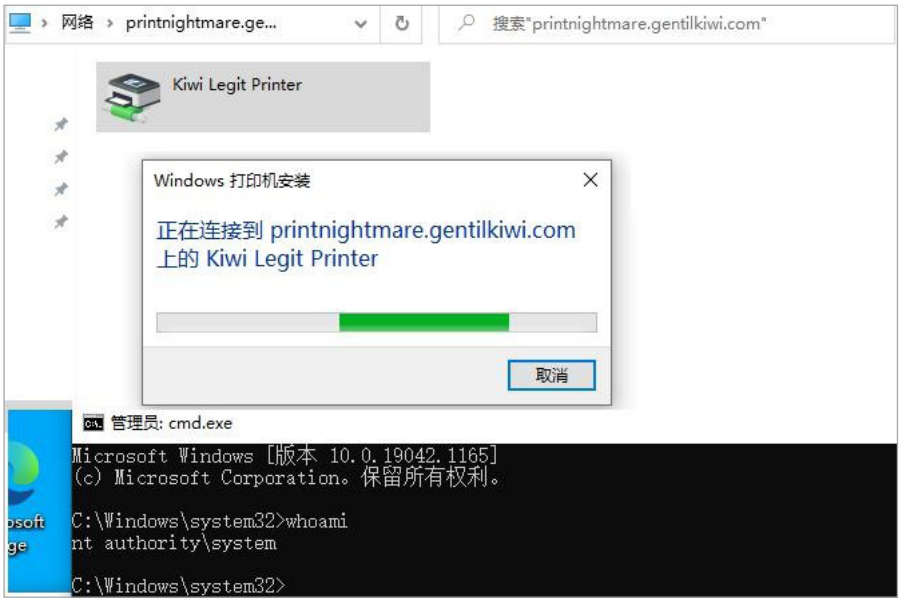
一、漏洞概述

北京时间 8 月 11 日，绿盟科技 CERT 监测到微软发布 8 月安全更新补丁，其中包括了在7 月 16 日紧急发布的 Windows Print Spooler 权限提升漏洞（CVE-2021-34481），对应的补丁编号为 KB5005652，微软同时将漏洞名称修改为远程代码执行。当 Windows Print Spoole r 服务不正确地执行特权文件操作时，攻击者利用此漏洞可以使用 SYSTEM 权限运行任意代码。有国外研究人员在安装了最新补丁的 Windows 系统上进行测试，发现此次更新的 CVE- 2021-34481 安全补丁无效，当受害者连接并安装攻击者控制的打印机时，可成功触发此漏洞。

8 月 12 日，微软为此发布紧急安全通告，并分配了一个新的漏洞编号 CVE-2021-36958， 但暂未发布安全补丁进行修复，请相关用户采取措施进行防护。

绿盟科技第一时间安装补丁进行测试：

成功复现此漏洞的补丁绕过：



参考链接：

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36958

二、影响范围

受影响版本

- ☐ Windows Server, version 20H2 (Server Core Installation)
- ☐ Windows Server, version 2004 (Server Core installation)
- ☐ Windows Server 2019 (Server Core installation)
- ☐ Windows Server 2019
- ☐ Windows Server 2016 (Server Core installation)
- ☐ Windows Server 2016
- ☐ Windows Server 2012 R2 (Server Core installation)
- ☐ Windows Server 2012 R2
- ☐ Windows Server 2012 (Server Core installation)
- ☐ Windows Server 2012
- ☐ 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 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 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 10 for x64-based Systems
- ☐ Windows 10 for 32-bit Systems
- ☐ Windows 10 Version 21H1 for x64-based Systems
- ☐ Windows 10 Version 21H1 for ARM64-based Systems
- ☐ Windows 10 Version 21H1 for 32-bit Systems
- ☐ Windows 10 Version 20H2 for x64-based Systems
- ☐ Windows 10 Version 20H2 for ARM64-based Systems
- ☐ Windows 10 Version 20H2 for 32-bit Systems
- ☐ Windows 10 Version 2004 for x64-based Systems

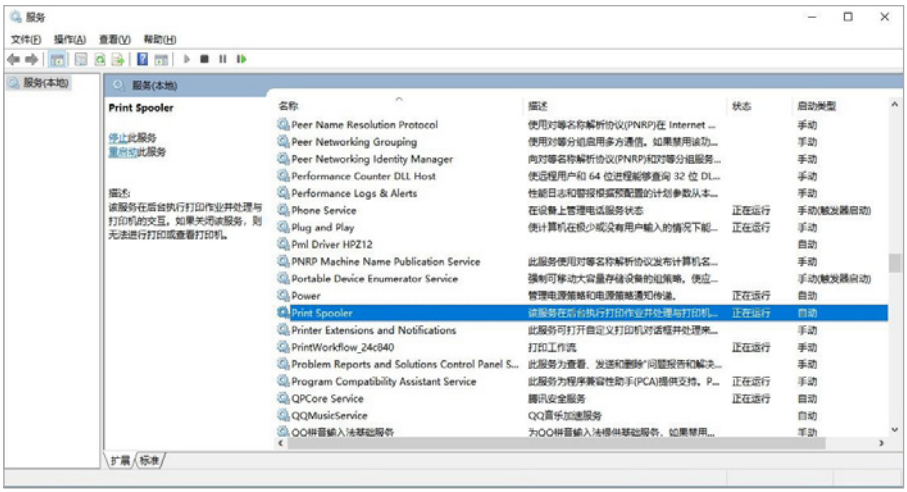
三、漏洞防护

3.1 防护措施

目前微软官方暂未对此漏洞发布修复补丁，建议受影响的用户仅安装受信任的打印机， 或关闭打印服务（Print Spooler）对此漏洞进行防护。

（1）用户可通过停止并禁用 Print Spooler 服务对此漏洞进行缓解：

进入任务管理器，选择“服务”→“打开服务”→“选择 Print Spooler”→“右键属性”，



“启动类型”选择“禁用”，并点击“停止”，关闭服务，点击“应用”和“确定”

注：停用此服务将导致打印功能失效。

(2) 通过组策略禁用入站远程打印：

运行组策略编辑器（Win+R，输入 gpedit.msc，打开组策略编辑器），依次浏览到：计算机配置/管理模板/打印机：禁用“允许打印后台处理程序接受客户端连接：”策略以阻止远程 攻击。

注：此策略将通过阻止入站远程打印操作来阻止远程攻击。该系统将不再用作打印服务 器，但仍然可以本地打印到直接连接的设备。

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. 攻击者利用Wiper攻击东京奥运会

【概述】

据TheRecord报道，在2021年东京奥运会开幕式之前，日本安全公司研究人员检测到一种以奥运会为主题的恶意软件Wiper，攻击者利用Wiper恶意软件攻击东京奥运会，使用URL应用程序访问XVideos成人视频门户上的内容，专家认为，实施此功能是为了诱使专家相信内容感染是在访问成人网站时发生的。同时删除受感染系统上的文件。该恶意软件仅针对用户文件夹下的数据，恶意软件的目标是使用Ichitaro日语文字处理器创建的文件，这种情况表明它是为日本用户开发的。恶意软件还实现了规避和反分析功能，以防止恶意代码被分析。该恶意软件还能够从受感染的计算机中删除自身及其存在的证据。”

【参考链接】

https://ti.nsfocus.com/security-news/4qYS2

2. 勒索软件团伙利用KaseyaVSA的0day漏洞攻击管理服务商

【概述】

7月2号，勒索软件团伙Revil利用KaseyaVSA远程管理应用的0day漏洞对多个管理服务提供商和企业发动了大规模的攻击，对约60个管理服务提供商和约1500家企业进行了加密，攻击者在完成攻击后，获取通用解密器。之后，勒索软件团伙开出价格：通用解密器需要7000万美元，解密所有受感染的托管服务提供商需要500万，解决一个受害者网络上扩展的加密需要4万美元。随后，REvil勒索软件团伙却神秘消失，也关闭了他们的支付网站和基础设施。当时大部分受害者还没

有支付赎金，勒索软件团伙的消失也使得那些需要购买解密器的公司无法进行购买。7月22日，Kaseya发出声明，他们从一个“受信任的第三方”收到了对应上次勒索攻击的通用解密器，现在也已经分发给了受到影响的顾客。尽管Kaseya并未透露密钥来源，但它们向BleepingComputer表示，被分发的确是攻击的通用解密密钥，能让所有托管服务提供商及其客户免费解密文件。

【参考链接】

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

3. 攻击者利用PlugX变体来攻击MS-ExchangeServer

【概述】

2021年3月，研究人员在监测MicrosoftExchangeServer攻击时，发现了一种PlugX新变体，攻击者利用PlugX新变体攻击MicrosoftExchangeServer。该PlugX变体是作为一个被攻击服务器利用后远程访问工具(RAT)传送到其中一台服务器。PlugX变体独特之处在于对核心源代码的更改。

【参考链接】

https://ti.nsfocus.com/security-news/4qYT9

4. PrayingMantis利用Web应用程序中的漏洞窃取服务器数据

【概述】

一个新发现名为PrayingMantis的威胁组织正通过利用面向互联网的Web应用程序中的漏洞窃取凭据和其他数据。在某些情况下，该组织利用CheckboxSurvey中的零日漏洞攻击用于Web托管的WindowsInternet信息服务器。最新报告显示，在利用漏洞后，该组织部署了一个恶意软件来收集系统信息，并部署额外的JavaScript恶意软件并执行HTTP和SQL流量转发。额外的有效载荷随后会收集凭据并危害更多易受攻击的服务器。“

【参考链接】

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

5. 攻击者利用同性恋色情图片攻击巴布克勒索软件团伙的论坛

【概述】

根据报告称，Babuk勒索软件运营商遭受了勒索软件攻击，攻击者利用他们的论坛同性恋狂欢色情图片对Babuk勒索软件运营商展开大规模攻击，6月底，BabukLocker勒索软件在网上泄露信息，攻击者可以使用它来创建自己的勒索软件版本。

之后，勒索软件团伙闯入华盛顿特区大都会警察局，在华盛顿特区警察局遭到袭击后，攻击者对其文件进行加密并向华盛顿特区警察局索要400万美元的赎金。5月底，Babuk勒索软件运营商将他们的勒索软件泄漏站点更名为Payload.bin，并开始向其他团伙提供使用从受害者那里窃取的数据。

【参考链接】

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

6. 攻击者利用勒索软件攻击南非物流公司

【概述】

南非大型铁路、港口和管道公司TransnetSOCLtd宣布遭到破坏性网络攻击。7月22日，南非物流公司TransnetSOC受到攻击者破坏性网络攻击，因此该公司停止了所有港口码头的运营。Transnet透露：“港口码头在整个系统中运行，但集装箱码头除外，因为卡车运输方面的Navis系统受到了影响。”

针对这次攻击，该公司告诉其员工在另行通知之前，所有员工关闭笔记

本电脑和台式机，并且不得访问他们的电子邮件，以防止威胁蔓延。该公司的一份声明中写道。“正在努力减少停机时间，以确保受影响的系统尽快重新启动并运行，”由于这次攻击，TransnetSOCLtd网站关闭。

【参考链接】

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

7. 攻击者利用发送恶意电子邮件攻击Zimbra服务器

【概述】

攻击者通过发送恶意电子邮件来攻击Zimbra服务器，研究人员表示，Zimbra网络邮件服务器有两个漏洞，攻击者会利用这些漏洞查看所有使用这款协作工具的企业中所有员工的收件箱和发件箱。由于Zimbra处理大量消息的高度敏感性，因此有超过200,000家企业、一千家政府和金融机构以及数亿用户使用在Zimbra网站中的电子邮件和协作工具，每天都在交换电子邮件。报告称，“当攻击者访问员工的电子邮件帐户时，通常会产生严重的安全隐患。”“除了交换的机密信息和文件外，电子邮件帐户通常与其他允许重置密码的敏感帐户相关联。

【参考链接】

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

8. 攻击者利用加密恶意软件LemonDuck攻击Windows、Linux设备

【概述】

根据Microsoft365Defender威胁情报团队的一份新报告，攻击者利用LemonDuck加密挖掘恶意软件攻击Windows和Linux设备。该恶意软件允许攻击者窃取凭据并在受感染的系统上进行一系列恶意活动。该恶意软件通过漏洞利用、网络钓鱼电子邮件、USB设备和暴力攻击在不同国家进行传播。

LemonDuck恶意软件对企业的威胁还在于它是一种跨平台威胁。它是针对Linux系统和Windows设备的僵尸恶意软件家族之一，”恶意软件可以使用新的漏洞，据研究人员称，LemonDuck恶意软件背后的威胁行为者几乎可以立即利用新漏洞并有效地开展诈骗活动。例如，他们在2020年在基于电子邮件的攻击中使用了COVID-19主题诱饵。今年，他们热衷于利用MSExchangeServer漏洞访问未修补的系统。

【参考链接】

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

9. 黑客组织部署恶意软件攻击Android和Windows用户

【概述】

Hack-for-hire组织StrongPity部署了Android恶意软件，以瞄准叙利亚电子政务网站的访问者。在这次最新的活动中，黑客组织使用wateringhole技术入侵叙利亚的电子政务网站，然后用木马版本替换官方应用程序。攻击者随后使用该应用程序从受害者的设备中窃取文件。

除了该恶意软件的Android版本外，攻击者还部署了一款针对Windows用户的应用程序。正在为这两个应用程序版本开发新功能。首先攻击者从MalwareHunterTeamTwitter上共享的一个线程中了解到该样本。根据线程了解到共享样本是叙利亚电子政务Android应用程序的木马化版本，该应用程序会窃取联系人列表并收集具有特定特征的文件，来自受害者设备的文件扩展名。

【参考链接】

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

10. MicrosoftHyper-V中的一个关键漏洞信息

【概述】

SafeBreach的研究人员报告说，有关MicrosoftHyper-V中一个关键缺陷的详细信息，跟踪为CVE-2021-28476，该缺陷可以触发DoS并在其上执行任意代码。该漏洞存在于MicrosoftHyper-V的网络交换机驱动程序中，它影响Windows10和WindowsServer2012到2019。CVE-2021-28476漏洞的严重性评分为9.9，微软已于5月解决了该漏洞。攻击者可以通过从虚拟机向Hyper-V主机发送特制数据包来利用此漏洞。

【参考链接】

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

11. 攻击者利用鱼叉式网络钓鱼技术向用户分发电子邮件攻击企业用户

【概述】

研究人员称，攻击者利用鱼叉式网络钓鱼技术向企业用户传入电子邮件，通过使用域名仿冒等方式攻击企业用户，虽然网络钓鱼攻击一直是网络安全领域的常态，然而，情况正在发生变化，随着攻击者从针对个人转向以企业和组织为目标，今天的网络钓鱼攻击比1996年、2006年甚至2016年的攻击要复杂得多。

最近有报道称，攻击者发起的网络钓鱼活动主要针对全球天然气和石油、能源、媒体、IT和电子行业的企业，攻击者通过给这些企业传入电子邮件，使用了欺骗和域名仿冒等技术，传入的电子邮件看起来像是从真实公司发送的。攻击者还通过精心制作特定文本，按名称引用公司高管并包括真实的公司地址和公司徽标，从而避开了“传统”网络钓鱼消息的散布式泛化方法。

【参考链接】

https://ti.nsfocus.com/security-news/llMJO

12. 攻击者攻击意大利新冠肺炎疫苗预约系统

【概述】

研究人员称，在医疗保健系统的网络攻击中，攻击者攻击意大利拉齐奥地区的新冠疫苗预约系统。目前，该地区的Facebook页面已经不能运行，攻击者已经禁用了该地区卫生保健机构的系统。据报道，意大利除了疫苗接种预约系统外，

还有很多系统都受到了攻击者攻击。

【参考链接】

https://ti.nsfocus.com/security-news/llMJE

13. 攻击者利用勒索软件攻击美国风险投资公司

【概述】

研究人员称，攻击者攻击了美国风险投资公司AdvancedTechnology Ventures（ATV）。以及窃取了公司投资者的数据信息。报道称，攻击者在数据加密之前窃取了美国风险投资公司存储在两台服务器上的财务信息。2021年7月9日，公司从其第三方信息技术提供商处获悉，公司存储财务报告信息的两台相同的ATV服务器出现异常活动。公司很快确定服务器已被攻击者攻击加密。2021年7月26日，公司了解到有证据表明服务器的内容遭到未经授权的访问和泄露。

【参考链接】

https://ti.nsfocus.com/security-news/llMJI

14. 攻击者设立呼叫中心向用户分发恶意软件BazaLoader

【概述】

研究人员称，攻击者通过设立呼叫中心向用户分发恶意软件，3月30日，MalwareTrafficAnalysis发布了对BazaCall号码的通话录音，呼叫中心员工将受害者引导到一个网站，在那里受害者被引导输入订阅号码。Carroll和Hacker写道，订阅号或其他编号可作为执行和跟踪活动的人员的标识符。然后，呼叫中心员工将受害者引导到一个看起来像合法企业的网站。然后指示受害者下载文件，例如Excel电子表格。在音频通话中，显示警告后会引导用户启用宏。最终，受害者被告知他们的订阅已成功取消，但实际上安装了BazaLoader恶意软件。

【参考链接】

https://ti.nsfocus.com/security-news/llMJu

15. 俄罗斯GRU针对美国和全球组织网络暴力攻击

【概述】

最近，俄罗斯军事情报机构GRU对美国和全球组织发起网络暴力攻击。GRU作为俄罗斯的军事情报部门，自2019年以来一直在进行网络暴力攻击。它攻击的

目标是美国和全球的政府和私营部门。研究人员称，攻击者通过提交大量登录信息来侵入网络，登录信息包括电子邮件和其他有效的帐户凭据，当攻击者攻击成功时，他们会访问受保护的数据，数据包括帮助网络攻击者在目标实体内横向移动的凭据。例如，凭证可用于初始访问、权限提升、持久性和防御规避。

【参考链接】

https://ti.nsfocus.com/security-news/IlMJA

16. 攻击者通过分发网络钓鱼电子邮件攻击WeTransfer文件托管系统

【概述】

研究人员称，攻击者利用向系统发送网络钓鱼电子邮件攻击WeTransfer文件托管系统，此攻击的主要目的是检索受害者的Office365电子邮件凭据。经调查，网络钓鱼电子邮件似乎是由WeTransfer发送的，因为它的发件人名称为Wetransfer，标题为“查看通过WeTransfer发送的文件”。这种相似性足以让人联想到真正的WeTransfer电子邮件，并且很容易欺骗用户。电子邮件正文还多次引用目标组织以使其看起来合法。电子邮件正文显示WeTransfer与受害者共享了两个文件，并且有一个链接可以查看它们。当受害者单击“查看文件”时，该链接会将他们引导至一个据称是MicrosoftExcel的网络钓鱼页面。

【参考链接】

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

17. 攻击者利用纯数据泄露模型泄露客户数据

【概述】

俄语组织Conti对爱尔兰卫生服务机构发起勒索软件攻击，同月DarkSide对总部位于美国的ColonialPipeline以及REvil于7月对远程管理软件公司Kaseya发起攻击之后，拜登政府一直在采取行动，更加积极地破坏勒索软件商业模式。白宫还呼吁俄罗斯政府没有对在其境内活动的警察采取更多措施，并威胁要破坏此类行动，除非莫斯科采取行动。

此外，“攻击者一直在瞄准纯数据泄露模型，这是攻击者追捕的一个很好的目标”McArdle说。“另外，'我们会告诉您所有的客户我们即将泄露您的数据。'尤其是在受到严格监管的行业，例如医疗保健或类似行业，如果您遭到破坏，可能会损失一大笔钱。”

【参考链接】

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

18. 攻击者利用MicrosoftExchange服务器攻击亚洲电信公司

【概述】

攻击者利用MicrosoftExchange服务器攻击亚州电信公司，并泄露了亚州电信公司数百GB数据，以收集客户的敏感通信。

Cybereason表示，与其他网络攻击一样，这些APT活动利用了MicrosoftExchange服务器中的缺陷来访问目标网络，然后继续破坏关键资产信息，包括具有敏感呼叫详细记录数据的域控制器和计费系统。

这些攻击主要损害了亚洲电信公司的数据，但这些攻击可能会蔓延到其他地区的电信公司，如果攻击者决定将其目标从间谍活动改为干扰，他们将有能力中断任何受影响电信客户的通信。

【参考链接】

https://ti.nsfocus.com/security-news/IlMJx

19. B2B营销公司泄露了美国人数以百万的数据

【概述】

研究人员表示，B2B营销公司OneMoreLead在配置错误的Elasticsearch服务器上暴露了多达1.26亿美国人的数据。并通知了OneMoreLead供应商，之后供应商对数据进行了保护。OneMoreLead将所有信息存储在一个不安全的数据库中，该公司已将其完全开放。因此，姓名、电子邮件地址和工作场所信息会暴露给任何拥有网络浏览器的人。如果攻击者发现了这个数据库，它将成为各种犯罪活动的金矿，从金融欺诈和身份盗窃，到针对美国公司和政府机构的大规模网络钓鱼攻击。”

【参考链接】

https://ti.nsfocus.com/security-news/llMJN

20. 攻击者利用恶意软件LittleLooter攻击伊朗改革运动的受害者

【概述】

研究人员继续跟踪疑似伊朗威胁组织ITG18的基础设施和活动。自从于2020年5月首次报告该组织以来，发现了一个恶意工具，我们将其命名为Android恶意软件LittleLooter。LittleLooter仅被观察到被ITG18使用。从2020年8月到2021年5月，X-Force研究人员观察到ITG18利用LittleLooter恶意软件攻击了伊朗改革主义运动的多名受害者。

X-Force研究人员发现ITG18从2020年夏末到2021年春季针对伊朗个人公开报告了他们的OPSEC错误，但ITG18继续在开放服务器和开放目录中保留包含泄露的受害者信息的存档文件。X-Force的新分析显示，ITG18从大约20名与伊朗改革运动结盟的人窃取了大约120GB的信息。

【参考链接】

https://ti.nsfocus.com/security-news/llMJJ

21. 攻击者利用Hive病毒勒索软件攻击多家海外企业

【概述】

近日，研究人员发现了一个HIVE病毒勒索软件的样本，该勒索病毒样本会将终端上的文件加密，并留下勒索信息，且攻击者利用HIVE勒索病毒样本在加密文件前进行数据窃取，Hive勒索病毒采用AES+RSA加密算法，在执行后，受害者终端上大部分文件会被加密成*.hive的文件。并且会在每一个目录下留下一个HOWTODECRYPT的文本文档，受害者可根据文档中的账号密码登陆黑客提供的网站后用赎金换取解密密钥。根据海外媒体报道，加拿大商业地产公司AltusGroup正是遭受Hive勒索攻击导致数据泄露。且不到一个月，该勒索团伙已公布了多家企业的数据信息。

【参考链接】

https://ti.nsfocus.com/security-news/llMKy

22. 攻击者利用Glowworm窃听虚拟会议的敏感信息

【概述】

随着越来越多的业务通过MicrosoftTeams、Zoom、Skype等平台，研究人员发现了一种全新的针对电子通信攻击媒介Glowworm，攻击者可利用Glowworm窃听Zoom和其他虚拟会议的敏感对话，它会将设备功耗引起的设备电源指示灯LED强度的变化将其转换为音频。

【参考链接】

https://ti.nsfocus.com/security-news/llMKv

23. 短信网络钓鱼诈骗团伙冒充就业机构窃取用户信息

【概述】

贸易委员会表示，短信网络钓鱼诈骗团伙正在冒充就业和劳工机构，诱使用户点击恶意链接，这些恶意链接称为网络钓鱼文本，被称为重新提交或验证失业救济金的表格链接，短信中的恶意链接将目标受害者引诱类似就业机构的链接。当受害者点击恶意链接时，诈骗团伙会窃取个人信息，甚至救济金。研究人员表示，这些网络钓鱼攻击将在未来几个月内持续存在，阻碍企业工作。因此，组织必须继续就社会工程策略对员工进行培训，并为用户创建及时报告网络钓鱼消息的机制。

【参考链接】

https://ti.nsfocus.com/security-news/llMKt

24. LoakBit勒索软件团伙针对埃森哲公司进行攻击

【概述】

咨询公司埃森哲证实，它受到了勒索软件团伙LockBit的攻击，在其暗网中，LockBit声称已经窃取了超过6TB的数据库，提供了埃森哲数据库出售，并要求支付5000万美元作为赎金。据事务部称，在赎金支付倒计时结束时，泄漏站点显示了一个名为W1的文件夹，其中包含据称从公司窃取的PDF文档集合。并且LockBit声称已经获得埃森哲网络的访问权限，并准备泄漏从埃森哲服务器窃取的文件。

【参考链接】

https://ti.nsfocus.com/security-news/llML0

25. Strongpity利用Android恶意软件攻击叙利亚电子政府网站

【概述】

StrongPity利用Android恶意软件攻击叙利亚电子政务网站，然后用木马版本替换官方应用程序，随后使用该应用程序从受害者的设备中窃取文件。StrongPity通过使用不同的证书对恶意版本的应用程序进行签名，将其重新打包以使其看起来像原始版本。它会调整应用程序以请求对受感染设备的额外权限，添加恶意组件以触发感染。恶意软件继续通过命令控制服务器通信，将加密的有效载荷保存到Android目录中，然后解密文件。StrongPity从受害者的设备收集数

据，例如隐私数据和有关可用Wi-Fi网络的信息。报告指出，在Windows版本中，攻击者使用相同的策略重新打包应用程序的原始版本来感染受害者并窃取数据。

【参考链接】

https://ti.nsfocus.com/security-news/llMLp

26. 攻击者利用WarzoneRAT恶意软件进行鱼叉式网络钓鱼活动

【概述】

研究人员发现，攻击者使用受感染的WordPress网站，利用WarzoneRAT恶意软件进行新的鱼叉式网络钓鱼活动攻击全球制造商，新的鱼叉式网络钓鱼活动始于一家位于英国的在线食品配送服务制造商，攻击者给该制造商传入一封伪装成“FoodHub.co.uk”的自定义电子邮件，看似来自制造商合法客户的虚假电子邮件地址，电子邮件正文包括订单和运输信息，以及一个采购订单PowerPoint文件。威胁行为者通常将全球制造商和其他供应商作为攻击目标，不仅是为了攻击他们，而且是为了窃取到该企业客户的信息。

【参考链接】

https://ti.nsfocus.com/security-news/llMLu

27. 攻击者利用FlyTrap安卓恶意软件攻击Facebook等社交媒体帐户

【概述】

研究人员发现了一种名为FlyTrap的新型Android木马，该木马通过第三方应用商店中被操纵的应用、侧载应用和被劫持的Facebook帐户传播给10,000多名受害者。自3月以来，攻击者利用FlyTrap恶意软件通过GooglePlay商店和第三方应用程序市场分发的恶意应用程序传播到至少144个国家/地区。FlyTrap使用JavaScript注入通过登录原始合法域来劫持Facebook会话，这些被劫持的Facebook会话可用于传播恶意软件，通过木马的链接，以及使用受害者的地理位置详细信息进行宣传或虚假宣传活动，并且经常被攻击者用来将恶意软件从一个受害者传播到另一个受害者。

【参考链接】

https://ti.nsfocus.com/security-news/llMKO

28. 攻击者窃取了100万张信用卡信息

【概述】

攻击者通过多种方式窃取了100万张信用卡的信息，比如销售点刷卡器、以及针对网站的Magecart攻击和信息窃取木马是他们窃取信用卡数据的主要工具。报道称，攻击者在Cybersixgill公司监控的地下信用卡市场上出售了超过4500万张信用卡信息。然后，使用这些信用卡进行网上购物，包括购买礼品卡，但通过这些信用卡信息很难追查到他们的行踪。

【参考链接】

https://ti.nsfocus.com/security-news/llMKP

29. 黑客在加密货币抢劫案中窃取了PolyNetwork公司6亿美元

【概述】

行业领先的中心化金融平台DeFi之一PolyNetwork已成为网络抢劫的受害者，基于区块链的DeFi网络遭受了最大的数字资产盗窃之一，攻击者窃取了该公司价值6.11亿美元的加密货币。据PolyNetwork称，来自BinanceChain、Polygon和Ethereum的资产被盗并转移到三个不同的钱包。此外，PolyNetwork已敦促Binance、OKEx、HuobiGlobal、Uniswap、CirclePay、Tether和BitGo等受影响的区块链和加密货币交易所立即将来自攻击者地址的任何代币列入黑名单。

【参考链接】

https://ti.nsfocus.com/security-news/llML1

30. Exchange服务器受到ProxyShell的主动攻击

【概述】

研究人员发现，Microsoft Exchange服务器受到ProxyShell的主动攻击，Exchange Server长期以来一直是黑客的首要目标，互联网上有超过400,000台Exchange服务器通过端口443受到攻击。通过Shodan扫描发现了30,000多个易受攻击的Exchange服务器，并且考虑到可用信息的数量。这些攻击使任何未经身份验证的攻击者能够发现明文密码，甚至通过端口 443 在Microsoft Exchange 服务器上执行任意代码，该端口由大约 400,000 台 Exchange 服务器暴露在 Internet 上。

【参考链接】

https://ti.nsfocus.com/security-news/llMLv

31. 俄亥俄州纪念卫生系统遭到Hive勒索软件团伙攻击

【概述】

俄亥俄州纪念卫生系统遭到攻击者袭击，这次袭击已经导致卫生系统临床和财务运营暂时中断和紧急手术病例、放射学检查被取消。这次纪念卫生系统攻击事件涉及Hive勒索软件团伙。报道称，攻击者已经窃取了卫生系统数据库200,000名患者的敏感信息，例如社会安全号码、姓名和出生日期等，Hive有一个名为HiveLeaks的泄密网站托管在暗网上，在暗网发布了窃取到患者的数据链接，Hive团伙通过使用一百个不同位大小的RSA密钥来加密文件，在部署加密程序之前，他们通常会花时间在网络上确定最有价值的系统并窃取数据，有更多的手段迫使受害者支付赎金，以换取不共享或泄露被盗数据的承诺并提供解密工具。

【参考链接】

https://ti.nsfocus.com/security-news/llMLK

32. 攻击者窃取了美国管道公司5,800多名客户的身份信息

【概述】

针对美国管道公司ColonialPipeline的勒索软件攻击事件中，攻击者窃取了约100GB的公司数据，包括5,800多名客户身份敏感信息。他们计划在满足赎金要求的情况下发布被盗数据，暴露的数据包括姓名、联系信息、出生日期和社会安全号码，以及政府颁发的身份信息，例如军人和税号以及驾驶执照号码、以及与医疗保健相关的信息。此次攻击，导致殖民管道运营中断，该公司决定关闭其大部分业务，以防止加密锁定恶意软件从IT系统传播到公司的OT系统。

【参考链接】

https://ti.nsfocus.com/security-news/llMLF

33. 攻击者利用Neurevt木马攻击墨西哥用户

【概述】

2021年6月，CiscoTalos发现了间谍软件新版Neurevt木马，攻击者利用Neurevt木马攻击墨西哥金融机构的用户，将Neurevt木马和信息窃取程序结合在一起，首先，通过PowerShell命令下载一个属于Neurevt系列的可执行文件，该木马将可执行文件、脚本放入它在运行时创建的文件夹中，从而窃取墨西哥银行系统的服务令牌来提升访问权限，通过访问操作系统并连接到C2服务器，以窃取用户账号、知识产权、银行网站凭据等私密信息。然后，通过修改系统中的Internet代理设置以逃避检测和阻止分析。因此，一旦被攻击，该木马可能会影响个人用户和组织导致数据泄露或声誉受损，最终导致财务价值损失。

【参考链接】

https://ti.nsfocus.com/security-news/llMLN

34. 巴西国库系统遭到黑客攻击

【概述】

巴西国库内部系统遭到黑客袭击，本次对巴西国库内部网络发起攻击的工具被确定为一种勒索软件，攻击者利用勒索软件通过在受感染系统中插入限制访问的有害代码、程序或软件的方式进行攻击，攻击者利用勒索软件入侵了企业网络并对员工和客户个人数据进行了复制或加密，然后以在网上公布隐私数据为要挟，向受害方索要100万美元赎金，受害者通常采用加密货币支付形式向黑客支付赎金才可重新访问网站。

【参考链接】

https://ti.nsfocus.com/security-news/llMMg

35. Siamesekitten组织冒充HR攻击以色列公司

【概述】

ClearSky的研究人员表示，在2021年5月至7月，近期发现名为Siamesekitten的黑客组织针对以色列的IT和通信公司发起了供应链攻击。Siamesekitten攻击主要针对IT和通信公司，并试图使用供应链攻击破坏以色列企业。首先，攻击者针对潜在的受害者，通过伪装成指定公司的人力资源专员HR，以ChipPc和SoftwareAG公司的“诱人”的工作机会为诱饵。然后，攻击者伪造了两个网站，一个模仿德国企业软件公司SoftwareAG的网站，另一个模仿ChipPc的网站，通过在领英上设置虚假个人资料，详细说明职位信息，引导受害者访问钓鱼网站，诱使用户下载诱饵文件。当用户下载名为Milan的恶意文件后，黑客通过DNS和HTTPS连接到C&C服务器进入公司，

拉取名为DanBot的远控木马，窃取数据并横向平移。

【参考链接】

https://ti.nsfocus.com/security-news/llMMj

36. 诈骗者冒充新冠疫苗制造商针对卫生局销售虚假疫苗

【概述】

国际刑警组织已发出警告，称某组织犯罪集团以政府为目标，伪装成疫苗制造商或指导疫苗分发工作的政府当局的代表，使用COVID-19疫苗的虚假报价，向40个国家的卫生局各地分销虚假疫苗，在新冠病毒的每个阶段，网络犯罪分子都非常活跃，目标人群从普通人到参与疫苗开发、批准和部署过程的各种制药公司和政府组织。诈骗者主要针对医院和卫生部的员工，将他们标记的工作和个人电子邮件帐户作为目标，甚至试图通过电话已出售疫苗为由与他们联系。在过去的一年里，他们部署了一系列与COVID-19相关的骗局，入侵了牛津大学的COVID-19研究实验室以及攻击了欧洲药品管理局，然后泄露了被盗的疫苗文件。

【参考链接】

https://ti.nsfocus.com/security-news/llMMe

37. HAVC黑客针对波士顿地区医院的暖通空调系统发起攻击

【概述】

据报道，针对一家马萨诸塞州供应商的黑客事件，HAVC黑客入侵了一家波士顿儿童医院的暖通空调系统并窃取了其客户的资料， 并且在其网站上泄露了多个医院的众多客户资料，包括波士顿地区的三家哈佛附属医院，分别是波士顿儿童医院、布莱根妇女医院和马萨诸塞州总医院。黑客向 DataBreaches.net 提供了在儿童医院拍摄并从 ENE Systems 内部捕获的原理图和布线方案的屏幕截图。并且勒索供应商支付赎金。

【参考链接】

https://ti.nsfocus.com/security-news/llMM8

38. 日本加密货币交易所Liquid遭遇黑客攻击

【概述】

日本加密货币交易所Liquid宣布遭遇黑客攻击，黑客窃取了价值约9700万美

元的加密货币，该交易所已经停止了所有流动货币存款和取款。攻击者从Liquid的数据库中窃取个人信息，包括姓名、家庭地址、电子邮件和加密密码等用户详细信息。Liquid表示，在跟踪被盗资产动态时，发现3250万美元的以太币以及1290万美元的XRP、480万美元的比特币、20万美元的波场币、920万美元的稳定币和3740万美元的其他代币被盗，并且发现黑客已经通过比特币、能源网络代币的形式将资金转移并且冻结。

【参考链接】

https://ti.nsfocus.com/security-news/llMMD

39. 黑客利用LockBit2.0恶意软件对多个国家的系统发起攻击

【概述】

研究人员发现，黑客利用LockBit2.0恶意软件针对意大利、台湾和英国等多个国家的系统发起了攻击，一旦黑客获得对系统的访问权限并部署LockBit2.0，恶意软件就会使用网络扫描仪来识别网络结构并找到目标域控制器。通过多个批处理文件终止进程和服务。黑客的主要目标通常是ActiveDirectory的域控制器，域控制器能够使黑客以管理员身份操作并将恶意软件推送到任何端点，如果LockBit2.0对系统进行加密锁定，它会将赎金记录放入加密目录并更改桌面壁纸。壁纸不仅包括受害者如何支付赎金的说明，而且还向潜在的附属机构以数百万美元赏金的形式出售。

【参考链接】

https://ti.nsfocus.com/security-news/llMMG

40. 攻击者窃取了美国T-Mobile1亿用户的数据信息

【概述】

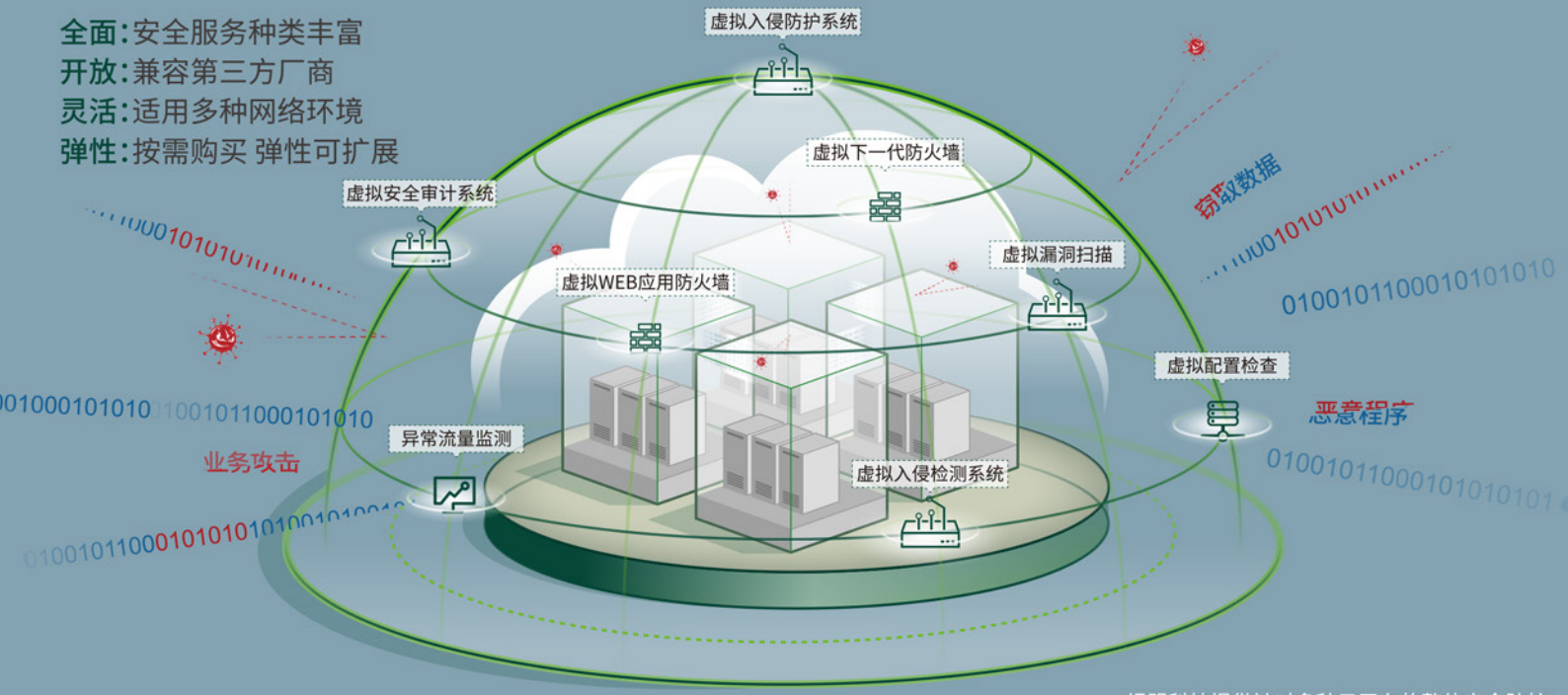
攻击者对美国的多台T-Mobile服务器发起攻击，包括Oracle数据库服务器，并窃取了包含约1亿名客户敏感信息，包括姓名、社会安全号码、地址、出生日期、电话唯一标识每个客户的移动设备的编号、安全PIN和详细信息。表示这一切是为了报复美国，并破坏美国基础设施。8月14日，攻击者在黑客论坛上声称要以6比特币的价格出售一个数据库，其中包含了3000万人的出生日期、驾驶执照号码和社会保险号码。

【参考链接】

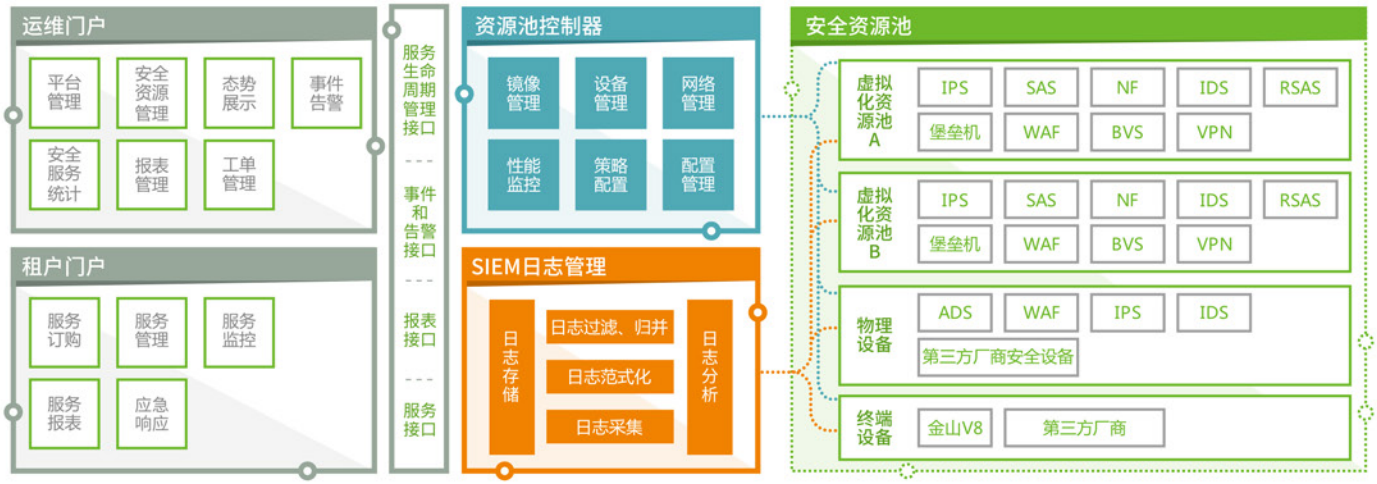
https://ti.nsfocus.com/security-news/llMLC

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

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/