金融行业

4 月报
2021 年

安全月报

攻防论道 | 行业研究 | 漏洞聚焦 | 安全态势

绿盟科技金融事业部出品

攻防论道

攻防论道 | 完备高效的攻防演练，要具备这5个阶段

行业研究

基于网络安全动态防御体系的安全智能运营系统的实践

绿盟安全运营平台全面提升恒泰证券信息安全防护水平

钓鱼短信再次升级，银行金融机构该如何应对

国内某银行存储瘫痪数据缺失6个小时

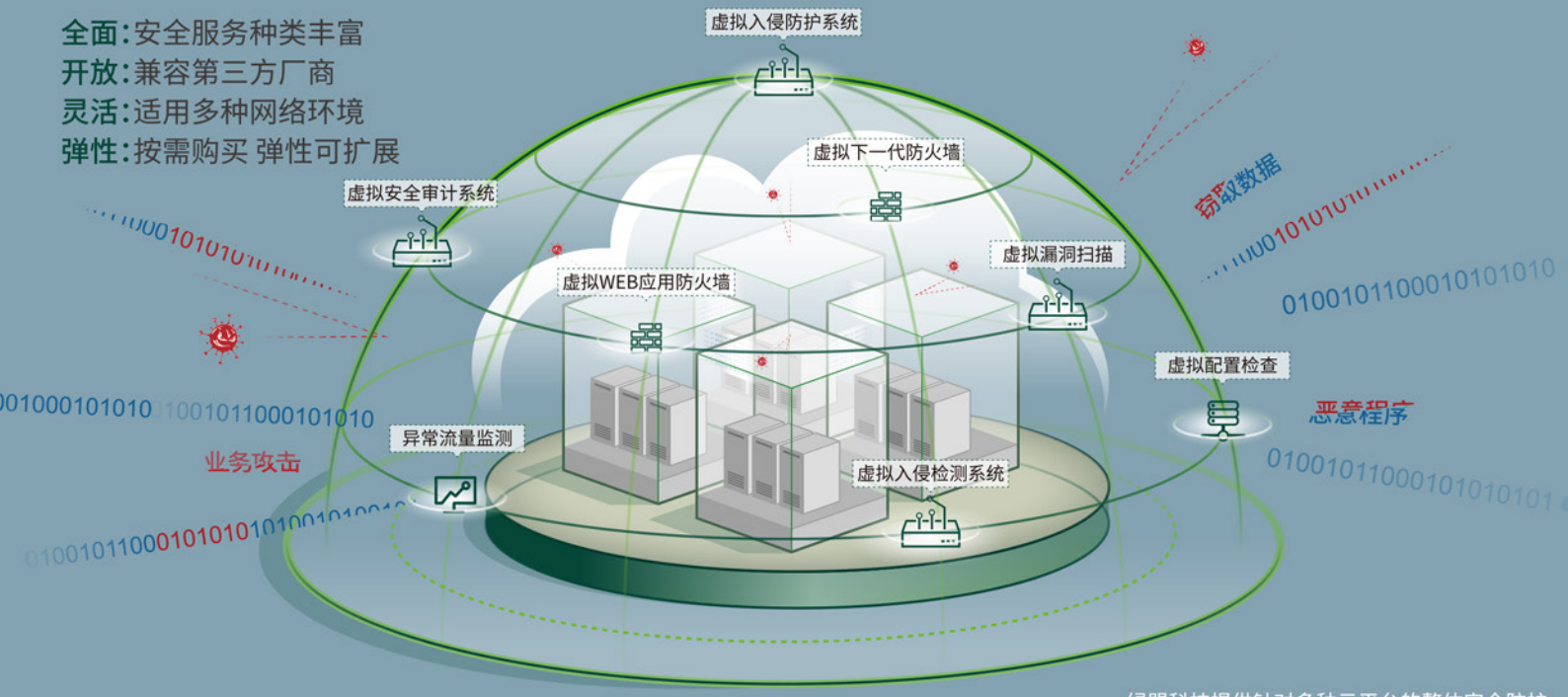
被盗1450万！江西“比特币”盗窃案告破：6名黑客被抓！

一键删好友、修改朋友圈……微信外挂软件主犯被判10年

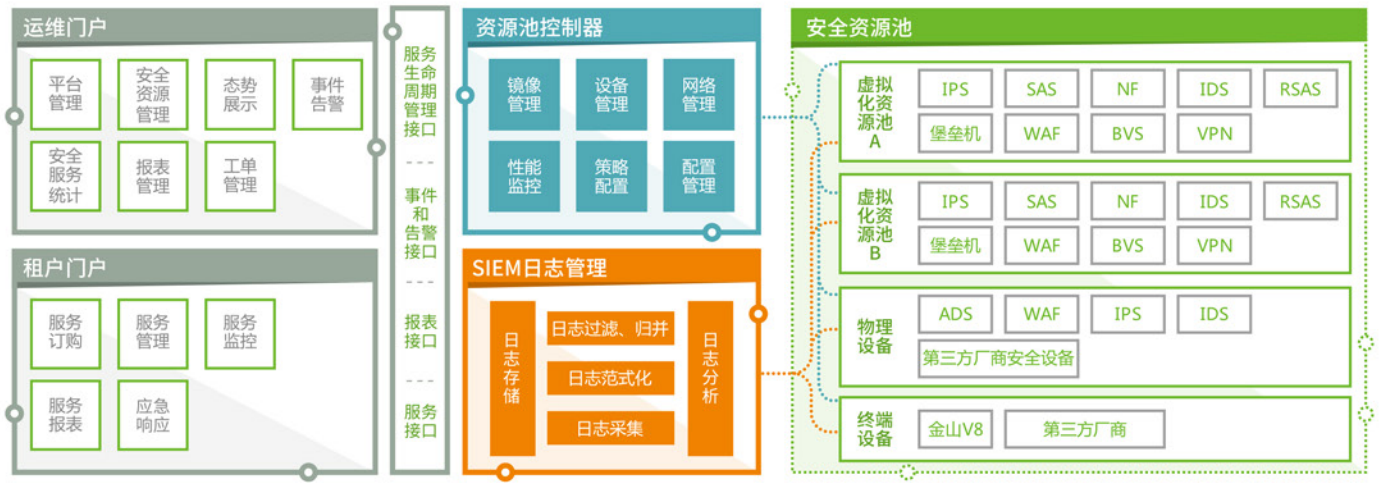
NSFOCUS

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

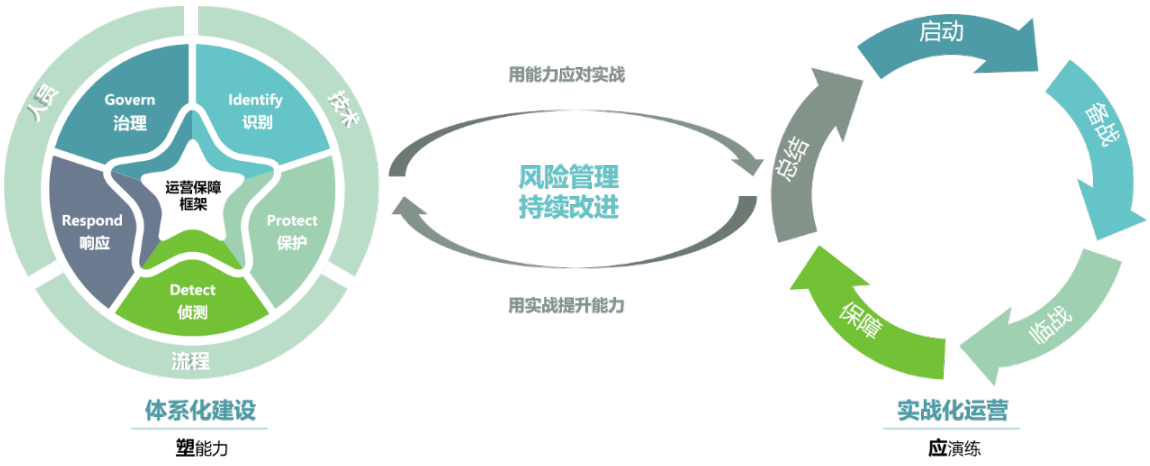
多年以来，绿盟科技致力于安全攻防的研究，为运营商、政府、金融、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。在这些巨人的背后，他们是备受信赖的专家。

客户支持热线：400-818-6868

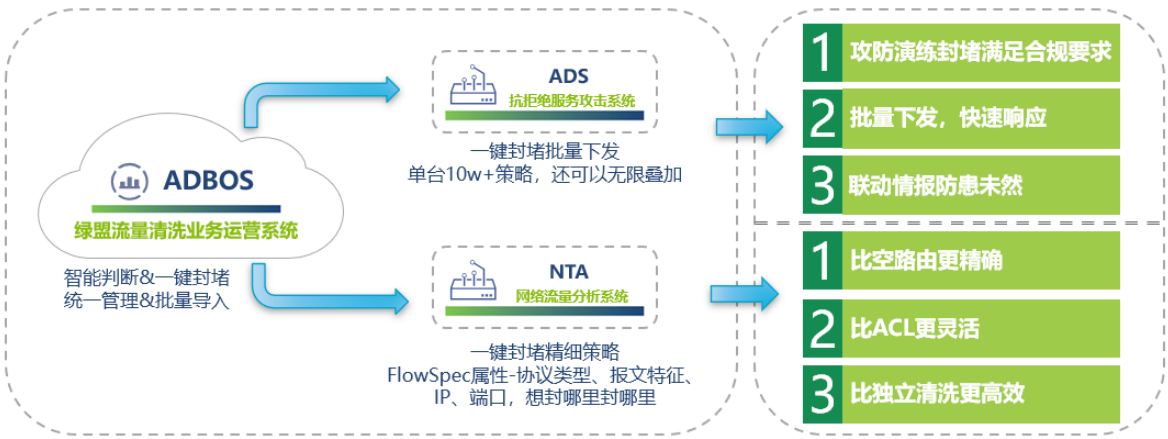
NSFOCUS绿盟科技

本|期|看|点

P4 攻防论道 | 完备高效的攻防演练，要具备这 5 个阶段



P14 攻防论道 | 防守方如何实现一体化异常流量追溯



安全月报

2021年第4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

攻防论道

行业研究

行业最佳实践

安全事件

漏洞聚焦

安全态势

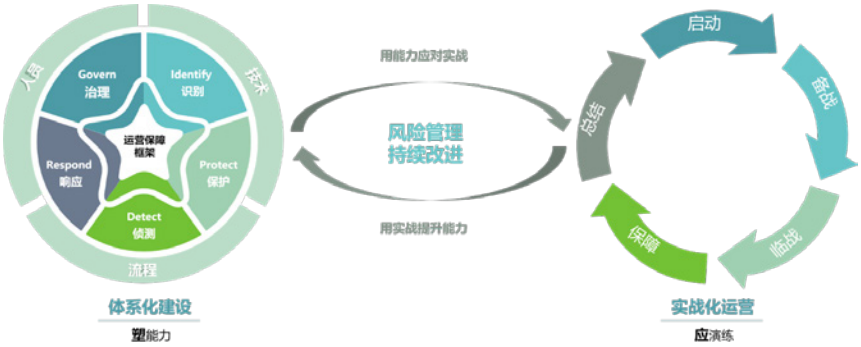
NSFOCUS

攻防论道

攻防论道 | 完备高效的攻防演练，要具备这 5 个阶段

——攻防之间 有备无患

随着网络安全成为国家战略，特别是《网络安全法》的正式颁布实施，网络安全建设正逐步走向实战化、体系化和常态化的新时代。在这一大背景下，攻防演练越来越受到各方重视，成为检验安全体系建设水平，促进安全运营能力提升的常备动作。



如图所示，网络安全能力塑造是在人员、技术和流程的支持下，从治理、识别、保护、侦测和响应等5个方面开展体系化建设的过程。能力塑造到什么程度，需要通过攻防演练进行检验。实战化攻防演练可以发现网络系统中存在的安全问题，识别安全风险，并通过持续改进进一步加强体系化建设成果。

为达到这个目的，攻防演练要从实战出发，按照网络战的思维组织攻击模式。同样，防御方更需要精心组织，充分应用自身安全建设的成果，达到发现攻击、抵御攻击的目的。

网络攻防演练保障工作不是一蹴而就，需要系统化的规划设计、统筹组织和部署执行。对于攻防演练的防御方，应按照以下五个阶段组织实施：

启动阶段：组建网络攻防演练保障团队并明确相关职责，制定工作计划、流程和具体方案。对信息网络架构进行梳理和分析，评估当前网络安全能力现状。对内外网的信息化资产进行梳理。

备战阶段：通过风险评估手段，对内外网信息化资产风险暴露面进行全面评估。制定合理可行的安全整改和建设方案，配合推动网络安全整改与治理工作。开展内部人员的网络安全意识宣贯。

临战阶段：制定应急演练预案，有序组织开展内部红蓝对抗、钓鱼攻击等专项演练工作。对人员进行安全意识专项强化培训。

保障阶段：依托安全保障中台，构建云地一体化联防联控安全保障体系，利用情报协同联动机制，持续有效地进行威胁监控、分析研判、应急响应、溯源反制等网络攻防演练保障工作。

总结阶段：对攻防演练工作进行经验总结和复盘，梳理总结报告，对演练中发现的问题进行优化改进和闭环处理。

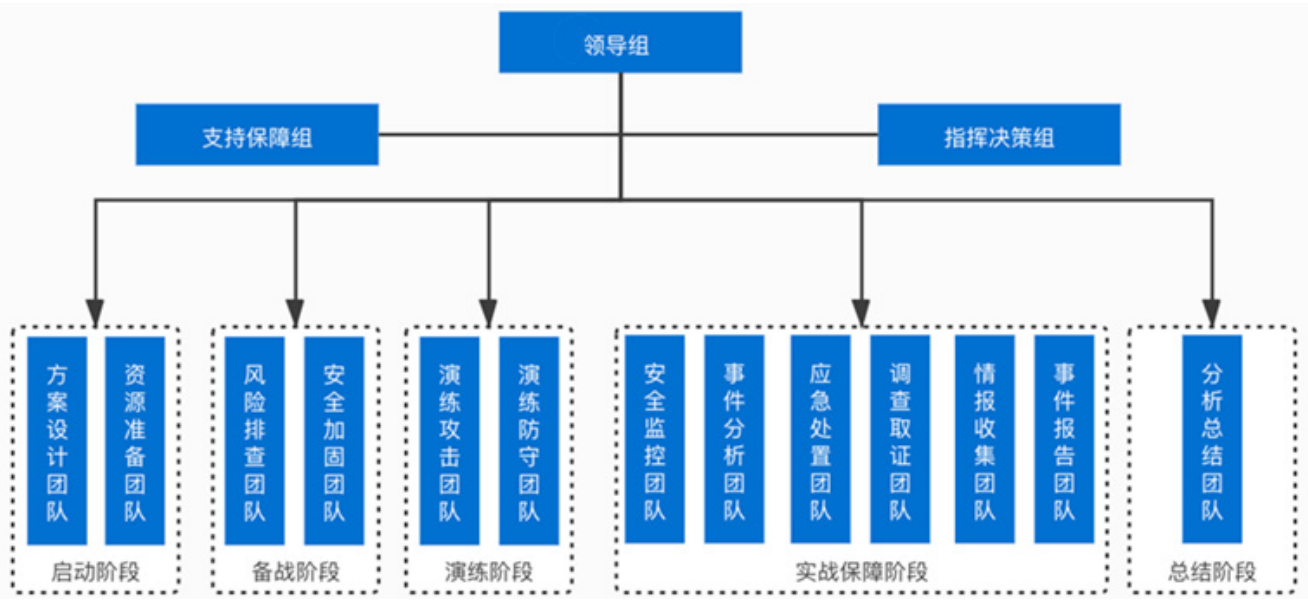
一个完备高效的攻防演练过程，通过启动、备战、临战、保障和总结全流程的精心组织，充分调动内外部资源，在取得好的成绩的同时，达到检验建设成果、锻炼运维团队、提升运营能力的目标。我们将在以后的文章中，为大家进一步深入介绍启动、备战、临战、保障和总结这五个攻防演练关键阶段的具体动作，为企业安全负责人开展攻防演练工作提供参考。

攻防论道 | 做好这三大基础工作，攻防演练方能事半功倍
——打好地基，再起高楼

万丈高楼平地起，要搞好网络安全攻防演练，在演练过程中取得好成绩，必须在演练之初就积极准备，做好整体计划提前部署。我们称这个阶段为网络安全攻防演练的启动阶段。在这个阶段主要有三大工作：建队伍，清家底，做规划。

一、建队伍

在启动阶段，应着手建立一个分工明确的网络安全攻防演练职能团队，以保证安全自查工作得到充分开展，安全防护能力得到有效的验证。因此必须明确安全保障团队的组织架构和职责划分。为做好演练工作，我们建议以如下方式建立安全保障团队的整体架构：



各职能团队分工如下表所示：

分组角色	职责
领导组	负责策略制定、重大事件决策、整体进度把控
指挥决策组	负责安全攻防演习保障工作管理、协调、组织工作
支持保障组	负责后勤保障工作，如准备攻防演习保障期间所需要的场地及物资
方案设计团队	负责制定攻防演习保障的整体方案，包括人员、分工、流程等
资源准备团队	负责准备攻防演习期间所需要的相关网络资源
风险排查团队	负责备战阶段中对保障资产的全面安全检查工作
安全加固团队	负责备战阶段中安全策略加固、优化、重点安全隐患排查工作
演练攻击团队	负责内部演练阶段中攻击方的工作，对资产进行真实模拟攻击，以发现真实存在的相关漏洞
演练防守团队	负责内部演练阶段中防守方的工作，对攻击方的攻击行为作出真实防御操作，以检验防御环节的漏洞
安全监控团队	负责信息安全攻防演习保障阶段安全攻击行为监控分析
事件分析团队	负责对安全设备的告警或上报的安全事件进行完整地分析及判断
应急处置团队	负责对发生的安全事件进行及时研判和应急处置
调查取证团队	负责开展应急处置过程中的调查和证据留存工作
情报收集团队	负责收集保障期间每日的相关安全情报，包括监控反馈、安全预警、厂商安全情报和其他渠道的攻击情报等
事件报告团队	负责对发生的安全事件进行完整的记录并形成文档，及时向分析人员和指挥组人员汇报
分析总结团队	负责对整个保障期间的相关安全工作进行有效总结

二、清家底

清家底是指对当前网络架构进行合理分析和优化，盘点内外网资产，理顺资产与业务系统的关系。摸清、理顺自身家底，充分应用自身安全建设的成果，为后续风险排查、加固优化奠定良好基础。主要包括三方面内容：网络架构分析调优、互联网资产暴露面治理和内网资产发现梳理。

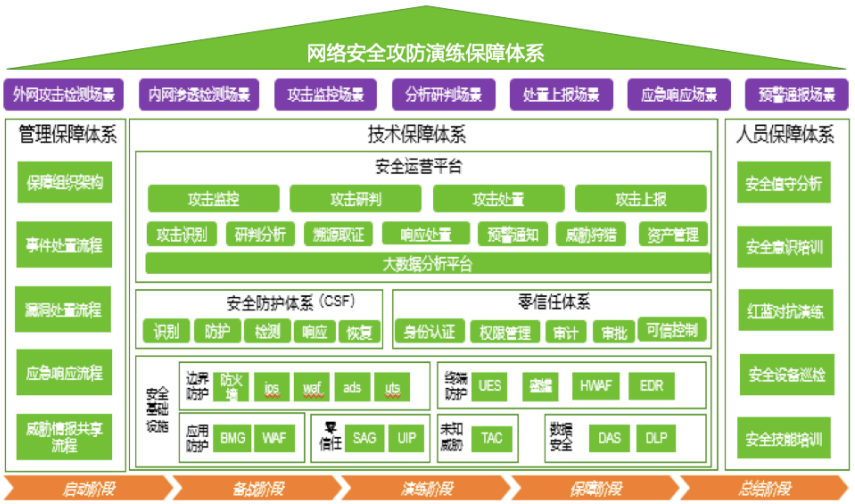
网络架构分析调优分为两大阶段，网络信息收集和安全架构分析。网络信息收集主要是完成对网络安全建设方案、已有网络安全拓扑、网络设备相关配置和流量镜像等方面的初步收集，并在完成初步收集后，同资产拥有方进行相关信息核对，找出存在异常的资产并及时处置。安全架构分析是在现场开展人工访谈和安全测试，以进一步验证前期所收集到的网络信息，并对比收集到的信息和现场调研的结果，综合输出网络安全架构分析报告。

互联网资产暴露面治理是通过专业服务，利用专业测试工具、搜索引擎等多类方式，对用户开放的互联网IP、端口服务、Web站点等进行梳理，并与用户进行归属确认，开放必要性核对，输出互联网暴露资产清单，供后续风险自查及保障使用。

内网资产发现梳理是要理清网络中全部信息资产，主要包括各类业务系统、内部运维系统、测试系统、网络设备、安全设备、接口设备、终端网段等，以便后续对资产进行风险自查、策略优化，同时识别全量资产中的重点保障关键资产，在后续防护和保障中对其进行加固保护。

三、做规划

做规划是指在前期工作的基础上，进一步明确安全保障应用需求，编制《安全运营保障实施计划》与《安全运营保障方案》，制定网络安全攻防演练工作目标，构建网络安全攻防演练保障体系，以全面指导网络安全攻防演练工作。



网络安全攻防演练保障体系如上图所示。体系覆盖攻防演习的五大阶段。对于每个阶段都要建立三位一体的保障体系，包括管理保障、技术保障和人员保障。管理保障是通过梳理组织架构和各类保障流程，从管理层面打通各个环节。技术保障是基于安全基础设施构建纵深防御和零信任机制，并接入安全运营平台实现整体运营。人员保障是通过对演练人员的赋能培训，满足监控、研判、处置、上报等各环节中对人员的能力要求。

因此，网络安全攻防演练的启动阶段，要做好建队伍、清家底、做规划这三项基础性工作，才能为网络安全攻防演练开好头，更好指导攻防演练工作的有序开展，为后续工作打好坚实基础。

攻防论道 | 六大管理策略提升实战演练胜算
——六大方面详论如何发现网络和业务系统的脆弱性

实战对抗中，考验的不仅是双方在对抗过程中的能力与技能，还有各自战前准备工作是否周详完备。只有经过充分的准备，方能在实战演练点内外网资产，理顺资产与业务系统的关系。因此，在前期理清资产的基础上，中掌握主动，并夺取最终的胜利。本需要对信息资产的安全性进行全面评估，主要包括以下7大评估方法：文是攻防论道系列的其中一篇，从资产全面评估，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六个方面，详论如何发现网络和业务系统的脆弱性，评估面临的安全风险，并通过技术和管理两个方面进行增强，实现安全策略的全面优化。

一、资产全面评估

在攻防论道系列文章中，曾讲到要对当前网络架构进行合理分析和优化，盘

- 漏洞扫描：检查系统中是否有中、高危漏洞，并结合人工检查进行确认。
- 配置核查：检查网络架构是否符合隔离要求，设备配置是否最优。
- 弱口令检查：定制弱口令字典，执行自动化扫描，发现资产口令存在的问题。
- 渗透测试：从攻击者视角发现被忽视的威胁路径。
- 入侵痕迹排查：检查资产中是否存在webshell、木马等可被利用进行远控的手段。
- 敏感信息检查：检查桌面敏感文件、开发过程文档等资料中是否存在用户名、密码等企业敏感信息。
- 安全机制校验：检查现有主机、设备、应用、服务等模块的安全监控、安全防护、网络策略、安全策略等机制，检查其是否有效。

二、业务缺陷识别

资产是业务的支撑，业务是资产的聚合。在业务层面，需要对业务系统进行分级，针对重要业务系统，特别是攻防演练确定的靶标系统和重要业务系统，梳理系统关键流程（如登录、认证、查询、申请、审批、交易等）绘制相应时序

图，分析业务流程和数据流转中可能遭遇的攻击和敏感信息泄露等安全隐患，输出相应风险处置措施以降低风险，保障系统安全。

在此基础上，还应该对身份认证系统、VPN、域控系统、网管系统等集权系统和防火墙，入侵防御系统，web安全防护系统，主机防护系统等安全设备进行风险评估，确保其集权管控和安全防护机制能够正常运行，且系统本身不存在中高危安全漏洞。此外，还需要来自供应链，相关业务链，第三方人员链等第三方的安全风险，防止攻击者利用第三方实施入侵。

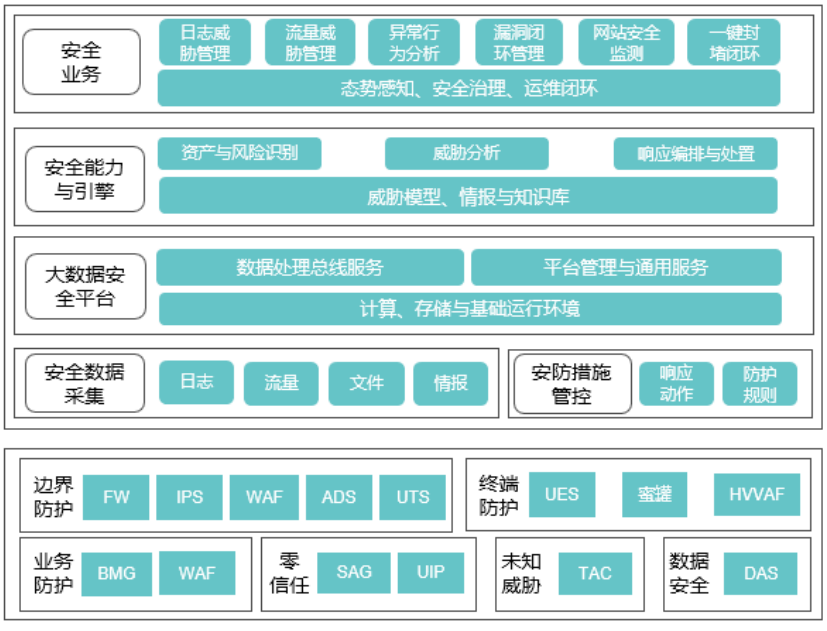
三、风险整改推进

对在资产安全评估和业务缺陷识别中发现的问题，需要制定整改方案，及时进行修复。主要包括：

- 历史发现风险闭环复盘：梳理以往发现的安全风险，对尚未解决的中高风险快速进行全面排查，针对历史上发生的重要安全事件进行复盘，总结教训，提升意识，并确认已无潜在风险。
- 自查发现风险跟进巡查：对自查中发现的风险及问题进行最终汇总整合，形成相应的跟踪表，设立每项风险闭环的责任主体和负责人，明确整改期限，及时跟进直至各项风险排查结束。
- 各类设备风险跟进处置 ：跟进网络设备、安全设备自身的安全风险处置，做好相应的修复规划和策略配置优化等，并及时更新同步。

四、防护能力补差

面对实战攻防演练，需要构建集预警、防护、检测、响应于一体的自适应联动响应体系。攻防演练的防守方，可参考下图展示的网络安全最佳实践技术体系，查漏补缺，消除短板，整体提升安全防护能力。



五、整体策略优化

在构建完成整体防线后，下一步就需要提升攻击检测和防护的效率，对整体策略进行优化，主要包括三方面的优化动作。一是优化日志分析，采用事件分析法，时间分析法，以及流量包样本分析法等方式，在大量日志中捕获关键信息，区分设备关注重点事件。二是处置设备误报，及时拉通业务侧沟通渠道，核实能否够及时对业务代码逻辑进行修改，解决业务误拦问题。三是优化平台和设备策略，根据日志分析及误报处理的结果，对网络设备策略、安全设备策略、主机策略等进行进一步调整和优化。

六、意识能力培训

在安全意识培训方面，需要在三大方向发力。一是要加强安全意识宣传，通过发放张贴安全意识宣传材料，播放安全意识宣传视频等方式加强员工对信息安全的重视和关注。二是要加强内部安全意识培训，通过面向一般人员、技术人员等不同的员工群体，组织针对性的专项培训。三是要面向第三方开发商和服务商人员等开展安全意识宣贯，同时签订安全保密协议、责任界定书，增强其安全敏感度。

在安全能力培训方面，首先要展开威胁分析能力培训，通过告警分析实现对常见攻击行为和结果的识别，包括利用漏洞执行恶意代码，手工尝试弱口令，服务器被攻陷，恶意程序被运行等。其次要对应急响应能力进行培训，通过排查服务器上的木马程序，分析攻击者入侵途径，登录服务器操作以验证事件的准确性等方法实现安全事件的事中和事后取证分析与及时处置。

攻防论道 | 四大制胜锦囊 严守实战演练安全之门
——助您铠甲加身，让攻击无处隐藏

实战攻防演练能够有效验证网络安全体系建设成果。通过实战演练，达到以攻促防的目的，助力企业建立常态化的防御机制。无论是实战演练还是日常工作，网络安全必须要做到持续运营，平战结合。绿盟科技为您奉上四个攻防制胜“锦囊”，助您铠甲加身，让攻击无处隐藏。

锦囊一 安全应急演练

为提升对网络信息安全攻击事件的响应能力和应对突发安全事件的紧急处理能力，切实保障防守方的网络安全，需要根据当前的网络安全现状和面临的安全威胁编制覆盖各类应急场景的重大保障应急预案，并组织开展网络安全专项应急演练，检验网络安全应急体系和工作机制运行情况，及时发现问题，完善应急预案，提高应急处置能力。

锦囊二 钓鱼攻击演练

为模拟防守方在攻防演练期间可能面临的真实攻击，同时对日常的安全意识培训效果进行验证，在实战开展前钓鱼攻击演练可谓是一计良策。

通过相应渠道给防守方员工发送钓鱼测试邮件，统计点击钓鱼链接员工的邮箱及人员信息，并输出统计报表，度量员工安全意识整体状态。在企业邮件办公环境下，还原钓鱼邮件真实场景，通过定制企业办公邮件与企业网站页面，使员工实际感受邮件钓鱼威胁，激发员工邮件办公的警惕心理，弥补员工的安全意识短板，演练结果直接成为后续安全教育的良好素材。

锦囊三 内部红蓝对抗演练

在保证业务正常运转的前提下，建议实战演练双方的攻防演习保障项目组在真实网络环境下开展红蓝对抗，及时发现网络资产的真实隐患，检验安全威胁监测发现能力、应急处置能力和安全防护能力，并通过演练结果进一步改进保障能力。

红蓝对抗演练组织方与参演单位协商基本信息，并提供演练技术支撑，制定对抗规则，提供后期保障，组织红蓝双方在指定时间内开展红蓝对抗。蓝队（攻击方）模拟黑客的动机与行为，探测企业网络存在的薄弱点，加以利用并深入扩展，在授权范围内获得业务数据、服务器控制权限、业务控制权限。红队（防守方）通过设备监测和日志及流量分析等手段，监测攻击行为并响应和处置。

绿盟科技总结多年参加关键信息基础设施网络攻防演习的经验，以及在能源、运营商、金融等20余个关键领域行业常年安全服务经验，结合国际先进的Kill Chain杀伤链战术、ATT&CK攻击对抗战术以及技术知识库，整合公司服务和产品能力，针对我国CII提出了以攻促防的红蓝对抗服务，从攻击者视角验证防护体系建设，实现网络威胁可视化。绿盟科技红队根据不同客户场景定制化网络安全防护体系，按照风险管理方法开展安全评估；蓝队按照攻击技战术验证防护体系的健壮性，建立攻击者生命周期的高级抽象模型，形成TTPs。

锦囊四 实战演练前安全意识专项强化

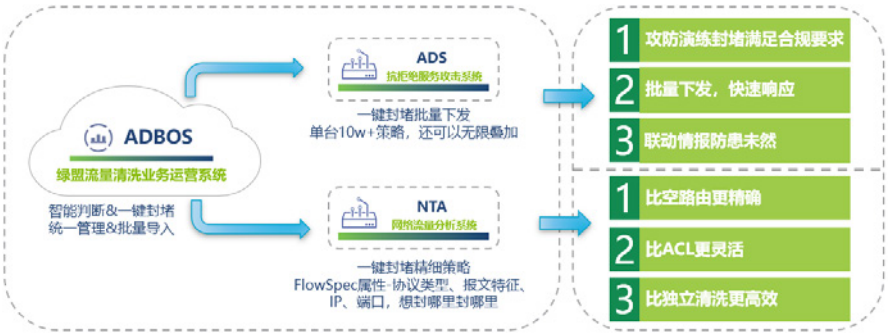
除了开展上述演练活动外，在实战攻防演练前安全意识专项强化工作也必不可少。攻防演练正式开始前，攻防演练保障项目组需要进行战前宣贯，针对前期安全意识培训及钓鱼攻击演练中发现的问题进行同步，重点关注IT技术人员及演练中钓鱼成功人员，对攻击队常用社工手段及防守方法突出强调，通过实战案例的介绍使防守方人员对攻防演习中的社工攻击有更直观的认识，争取最大程度降低人员的隐患。

贴近实战大练兵，磨砺攻防真本领。通过“背靠背”的体系化、实战化攻防演练，攻守双方能够进一步提高自身整体的安全防护能力，为接下来的保障阶段打下坚实基础。

攻防论道 | 防守方如何实现一体化异常流量追溯
——一键封堵 精准溯源

摘要：攻防实战演练是对重点单位和关键网络信息基础设施的安全防护能力、应急处置能力和指挥调度能力的综合检验。实战演练中，不论攻击成功与否，攻击行为的载体只可能是网络流量。因此，网络流量分析，异常流量处置，追踪溯源技术可以说是防守方的一张王牌。本文基于智慧安全3.0理念体系，介绍绿盟科技抗拒绝服务团队基于客户攻防场景需求，利用AI机器学习，大数据关联，威胁情报库碰撞，基线自学习等多重技术，推出的一套集异常流量识别、分析、处置和追踪溯源为一体的解决方案。

一、一键封堵方案



闭环处置，智能管理

ADBOS：实现一键封堵功能从检测到处置的闭环管理。

批量封堵下发，敏捷高效

ADS策略封堵：一键封堵批量下发，单台10w+封堵策略，策略下发简单高效。

ADS黑名单封堵：100w+黑名单，业内领先，满足大、中、小型客户多场景需求。

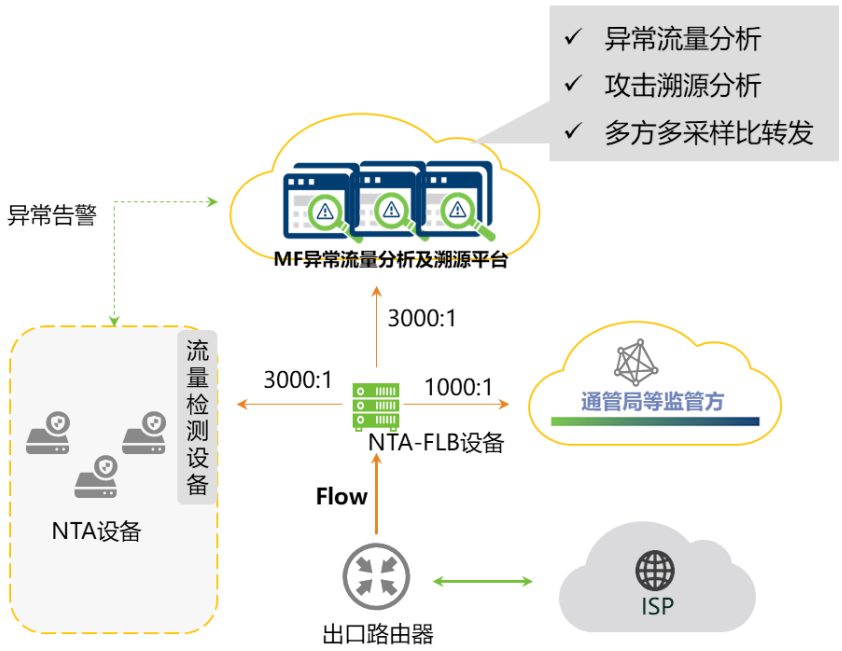
NTA策略封堵：一键封堵批量下发，单台10w+封堵策略，封堵方案灵活，全面适配客户业务场景。

封堵精细化，DDoS防护最大化

ADS精细化封堵：ADS URL-ACL，基于源地址、目标地址、源端口、目标端口、协议信息对数据包进出过滤控制，使用成本低。

NTA精细化封堵：NTA Flowspec，基于源地址、目的地址、IP协议、源端口、目的端口、ICMP代码、TCP标志、流量速率（丢弃/巡视）、下一跳重定向、VRF重定向、DSCP标记进行过滤、限速，实现精细化防护。

二、异常流量检测及溯源方案



多方采样，高性能转发Flow

NTA-FLB设备可复制多份Flow数据，往不同目标发送，同时支持按自定义的采样比转发，不仅能满足监管方的监管需求，还能满足后端各类流量检测设备的分析需求。

500万Flow/s的高收发性能，完美适配骨干网级的大流量环境。

Flow去重技术，让流量分析更加准确可靠。

异常流量分析检测

NTA设备基于机器学习的数据包异常行为检测能力，可从端口、协议、源IP、地域、访问时间等多种维度抓取特征，可秒级自动识别20余种异常攻击。

动态调整阈值基线，保证数据检测结论的准确性和可靠性。

丰富的告警策略以及10万+的封堵策略，可帮助用户快速发现和处置异常流量。

具备超强适应能力的NTA不仅支持DPI和DFI两种检测模式，还支持VM、KVM等虚拟化环境部署，最高可达30万Flow/s的分析能力。

具备精准完整的溯源能力

MagicFlow平台统一集中管理分散的NTA设备，汇总各NTA异常检测数据，利用大数据技术，为客户分析和发现威胁，追踪攻击源。

平台不仅支持快速秒级溯源，还能长期存储原始Flow，以便用户溯源取证。

多级深度溯源功能可还原攻击链，帮助用户快速提取攻击路径，便于进一步处置。

平台级的挖矿识别、虚假源IP识别、隐蔽信道、暴力破解、蠕虫病毒识别等能力，进一步帮助客户构筑安全防线。

NSFOCUS

行业研究

基于网络安全动态防御体系的安全智能运营系统的实践　绿盟安全运营平台全面提升恒泰证券信息安全防护水平

信息化的不断发展，信息化资产数量日趋增多、系统的关联性和复杂度不断增强，然而当前信息安全形势日益严峻，信息安全防护工作面临前所未有的困难和挑战。恒泰证券为了更好监控和保障信息系统安全稳定运行，及时识别和防范安全风险，同时满足国家和行业监管要求，保证信息安全管理工作的依法合规，建立了一个全数据、集中管理的安全运营管理平台，做到事前预警、事中监控、事后分析，全面提升恒泰证券信息安全管理与防护水平。

一、智能安全平台概述

智能安全运营平台以大数据框架为基础，结合威胁情报系统，通过对攻防场景的机器学习、威胁建模、场景关联分析、异常行为分析以及安全编排自动化、可视化呈现等技术，助力建设和完善安全态势全面监控、安全威胁实时预警、资产及漏洞全生命周期管理、安全事故紧急响应的能力，并为安全运营提供可靠的信息数据支撑，协助运维人员快速发现和分析安全问题，且能通过运维手段实现安全闭环管理。

二、企业面临的痛点

恒泰证券股份有限公司希望通过建立一套由资产管理、威胁情报以及日志、流量分析系统为支撑的态势感知平台，将各单点防护设备(WAF、IPS、流量探针UTS)进行整合，实现公司信息系统整体的安全态势感知，及时发现并阻止正在进行或将要出现的来自内外部的信息安全问题，并在事件挖掘、调查时提供分析途径。

通过部署绿盟安全运营平台建设，利用大数据采集、分析技术。收集各种安全设备（IPS、WAF、UTS等）的数据，并将各类安全数据进行关联分析，再利用可视化技术，将

各种攻击行为进行可视化展示。实现对系统安全的整体展示、态势感知、攻击事件溯源及对潜在威胁的预警功能。

三、立体安全威胁防御体系

3.1 管理层面

恒泰证券公司领导高度重视信息安全，建立健全信息安全防御体系。设立IT战略发展和治理委员会，承担公司信息安全工作领导小组工作。另设立信息安全联络联动机制，由公司系统运行总部信息安全部牵头，在各部门、各子公司设立信息安全联络专员，用于及时通报信息安全预警和事件。

3.2 技术层面

目前分别在呼和浩特机房和深圳机房部署UTS流量探针，收集全网流量信息，并上传至安全运营平台，对攻击进行分析、溯源、展示、研判、处置。

基于区域 / 资产的数据降噪措施

主要措施：

- 结合用户业务进行事件规则调优，将误报量降低。
- 分区域进行展示，快速将风险定位至内网有问题的区域。
- 重新定义事件标准，对高危事件进行外发；专注于高保真安全事件。
- 结合资产重要性及用途对关键事件进行二次筛选，发现真实攻击的事件。
- 集合内网区域边界的设备进行再筛选，可以发现突破边界的攻击。

通过上述措施，每日真正的高危告警数量可以收敛到5-6条，极大提高了运维效率。

业务系统及规则降噪调优

- 通过运维工作台发现攻击事件；
- 通过攻击详情展开查看流量上下文信息；
- 联系相关业务部门进行确认识别。

按区域进行重点监控展示

将区域与设备进行绑定，以便生成每个区域的告警：

基于现网区域拓扑进行大屏展示，对网内所有区域安全情况进行展示。通过比对，可以快速了解某区域存在安全问题：

图 1.1 区域大屏展示

事件级别定义与重点告警展示

- 自定义中高危及需要关注的事件级别

内部映射，将特别重大/重大映射为高；较大/一般映射为中；轻度与未知映射为低；同时在高中、低基础上，筛选出不同级别中用户需要关注的：

- 重点展示与告警

对中高危事件重点展示并进行邮件告警

图 1.2 中高危展示

基于资产特性与告警进行整合筛选

- 定义重要资产类别

重要资产定义：如可以SSH登录，或者可获取高权限的资产。

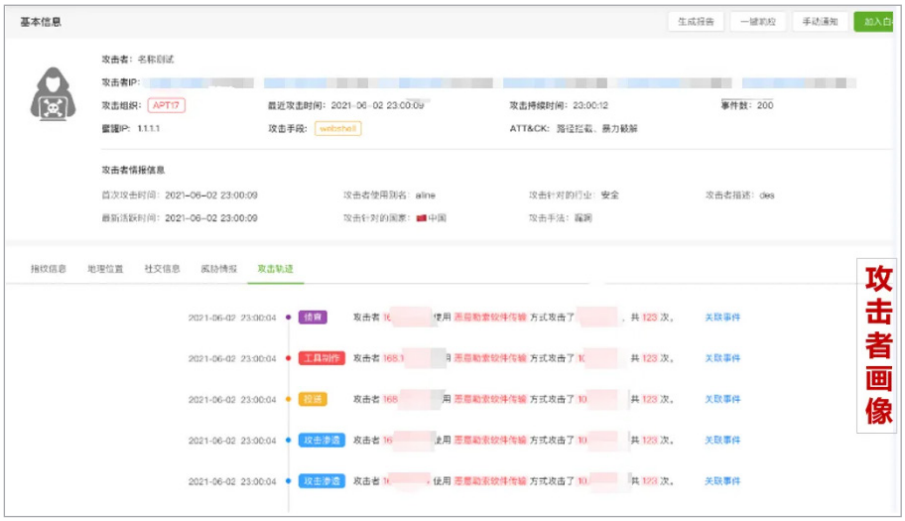
- 基于资产视角的威胁定位
  - 资产管理、威胁情报、事件分析结合提高了我们的分析处置、响应处置速度。
  - 终端、服务器、应用的标识可快速定位到受害主机负责人、团队及其联系方式。
  - 因此可快速定位是从哪个区域发起的攻击及攻击影响范围（因接入所有安全设备事件可集中搜索）。
- 基于内网区域边界设备进行筛选出实锤事件

基于内网安全设备IP，重点监控及快速查看突破内网进来的攻击，根据其监测设备告警特征对外网安全设备进行规则防护完善与自定义添加新规则，这些告警都是需要深入关注的。

四、实战案例

日常安全运营中，攻击溯源作为安全事故中事后响应的重要组成部分，通过对受害资产、内网流量、日志等进行分析一定程度上还原攻击者的攻击路径与攻

击手法，有助于修复漏洞与风险避免二次事件的发生。攻击知识可转换成防御优势,能够做到积极主动且有预见性，更好地控制后果。



五、成果展示

安全智能运营平台的建设为恒泰证券信息安全取得了如下成果：

建立纵深化安全防御体系

通过智能安全运营整体解决方案的建设，实现对网络安全的分析研判、跟踪和分析，全面掌握网络安全态势、威胁、风险和隐患；实现实时监测漏洞、网络攻击情况；及时通报预警重大网络安全威胁；实时分析研判、准确安全监测、及时应急处置。经过多重纵深安全防护体系建设，能够实现安全区域边界、安全网络通信和安全计算环境三重防护，并建立安全管理中心，通过技术手段实现集中管理，系统管理、审计管理、安全管理。融合事前监测预警、事中实时防御、事后检测响应的全过程安全防护能力。满足《中华人民共和国网络安全法》以及证券行业相关主管部门对于信息系统安全防护建设要求的有关规定。

安全态势可视化展示：

分区域直观展示当前面临的各种网络攻击，实现重点安全监控指标的展现，在出现高威胁攻击时可通过实时攻击地图进行展示，同时结合历史数据分析，展

示数据中心安全态势及发展趋势，为运维处置人员作出预警及处置研判的决策依据。

攻击路径可视化提供决策支撑：

利用攻击链模型和机器学习算法，结合威胁情报，及时通报预警重大网络安全威胁；提前感知攻击者的下一步攻击计划，提供决策数据，指导进行安全防御体系的敏捷调整、持续运营，使安全防御体系变得更有智慧。

安全防护/运维效果量化分析：

利用平台资产管理能力，定义资产的安全价值。结合资产安全价值、资产威胁情况从资产视角及时发现重点攻击。

建立7*24小时全天候多方式安全监控告警体系：

通过平台告警推送接口与恒泰证券信息技术中心集中告警平台的对接，提高安全告警的时效性，实现7*24小时的安全监控告警。告警信息通过企业微信、短信、邮件以及声音等多种方式向安全管理相关人员推送。其次，通过不断的对系统过滤规则调优提高每条告警的有效性，降低误报，为安全事件处置人员提供更具价值信息，有效提高事件处置效率。

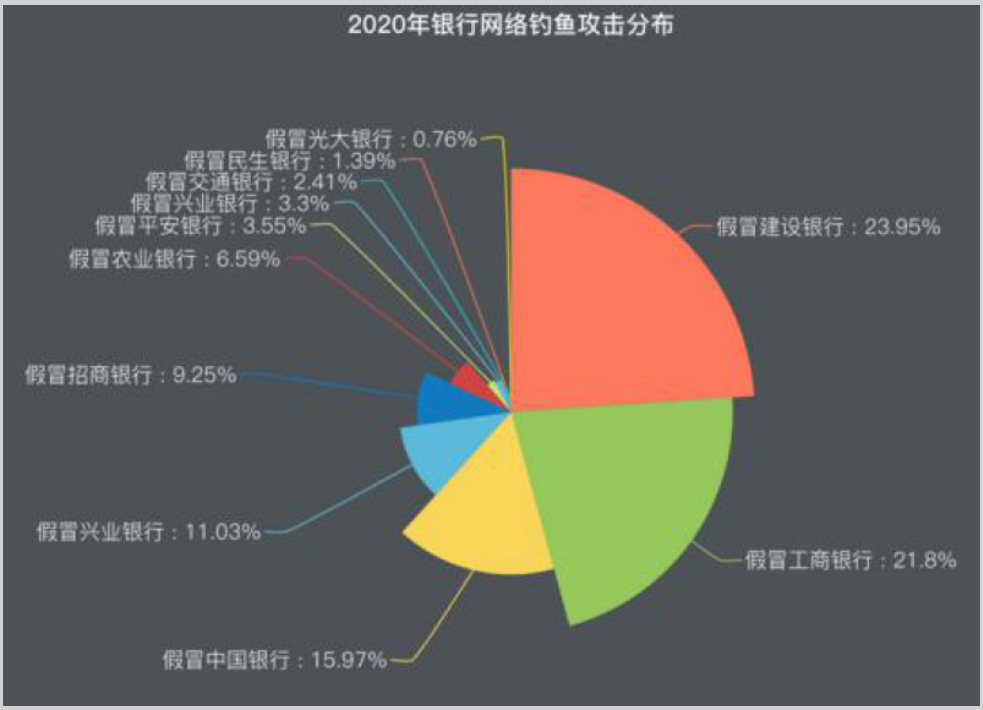
六、规划展望

随着黑色产业链的萌生和壮大，日益频繁的APT等网络攻击，正在导致政企行业机密情报被窃取、工业系统被破坏、金融系统遭受经济损失，2014年曝光的专门针对我国海事部门的“海莲花”APT攻击事件、2015年乌克兰“电力门事件”、2016年沙特阿拉伯Shamoon2.0的攻击，2017年全球范围爆发的永恒之蓝漏洞攻击等等，众多有针对性的安全事件，将未知威胁防御话题提到了空前的高度。恒泰证券将在全流量三期中通过绿盟安全运营平台与终端检测与响应系统对接，以端点检测与响应技术为核心，通过可信特征管理、综合行为检测、基线横向分析和安全沙箱等方式对用户的行为进行分析，有效发现已知和未知的威胁，提升防护精准度，降低企业终端安全风险。

钓鱼短信再次升级，银行金融机构该如何应对

摘　要：据美国网络安全公司proofpoint《2020 State of the Phish Report》数据显示，受疫情全球大流行影响，2020 年全球钓鱼短信攻击的增长率超过300%。而其中，针对金融机构的网络钓鱼攻击占比最大，占所有攻击的22.5%。而在国内，这一比例更是高达26.88%。

关键词：标签（proofpoint、钓鱼短信、金融机构），技术问题（安全事件）。



数据来源：12321 网络不良与垃圾信息举报受理中心

内　容：

一、钓鱼短信盯上银行用户

近期「假冒银行短信钓鱼」案件频发，中国银保监会也紧急发文，就近期假冒多家银行名义发送服务信息的短信钓鱼诈骗行为进行风险提示：

图片来源：中国银行保险监督管理委员会网站

种种迹象表明，黑产团伙已经盯上各家银行的用户，这将严重威胁到用户的财产安全，并对各大银行的品牌形象造成极为恶劣的影响。

二、短信如何成为黑产敲门砖

早在2012 年，全球每天有将近19 亿条文字讯息通过WhatsApp 等实时通讯软件传送，而传统短信则仅有17.6 亿条。从那时起，每年都会有人喊出「短信已死」，结果人家非但没死，每天还变着花样，轮番轰炸你的手机。

紧迫感下的新商机

营销泛滥的当下，流量转化成本越来越高，以槽点最多的开屏广告为例：

这种误点率极高的设计，就是为了让点击率能突破行业12%的上限。而短信则不同：

Mobile Squared 的数据称，在所有营销渠道中，近九成的短信会在被收到后的三分钟之内被打开阅读，这一点是其他任何直接营销渠道所无法比拟的。

在独有的紧迫感下，短信催生了新的商机。除常规的短信验证码、服务类短信通知外，越来越多的银行使用文本消息进行新客营销，老客促活。越来越多的银行用户开始习惯，以短信文本消息与银行进行交互。而在不经意间，银行也帮助黑产团伙培养了用户习惯：

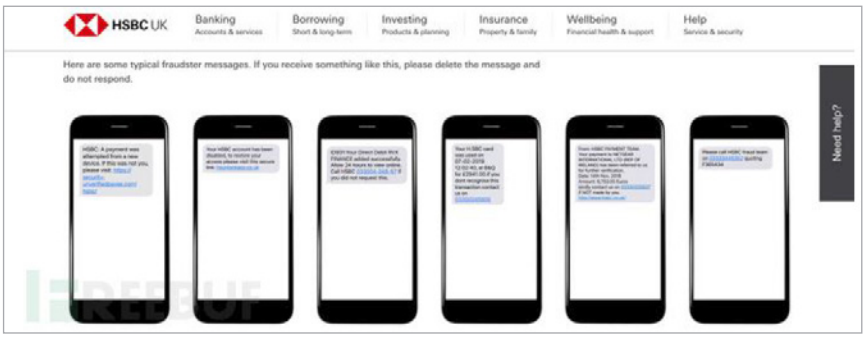
「在紧迫感下，银行用户参与度高，并较大概率会对短信内容迅速采取行动」

完美的钓鱼攻击环境，黑产团伙只需要模仿各大银行定期通过短信与用户互动，便可实施钓鱼短信诈骗。

千亿规模的黑产市场

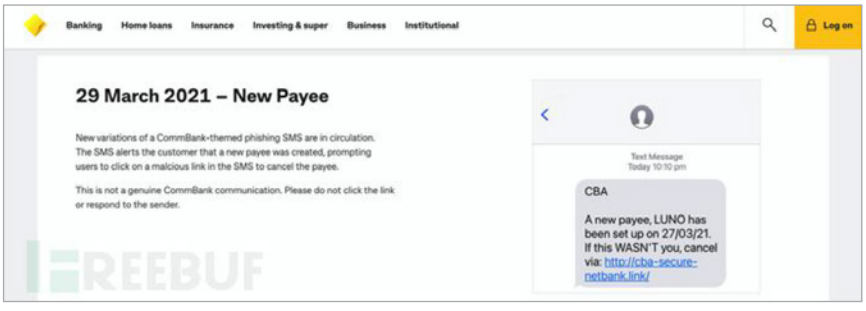
根据FBI 旗下互联网犯罪投诉中心（IC 3）的一份调查报告显示，在过去的三年里，全美因钓鱼攻击所造成的损失，超过260 亿美元。而在我国，2020 年以来，仅凭拦截下来的钓鱼诈骗信息，就为群众直接避免了将近1200 亿元的经济损失。

在美国，摩根大通银行作为金融领域代表，与Netflix、苹果公司入选最受「钓鱼短信」模仿的热门品牌。而「假冒银行钓鱼短信」威胁，早已蔓延全球：

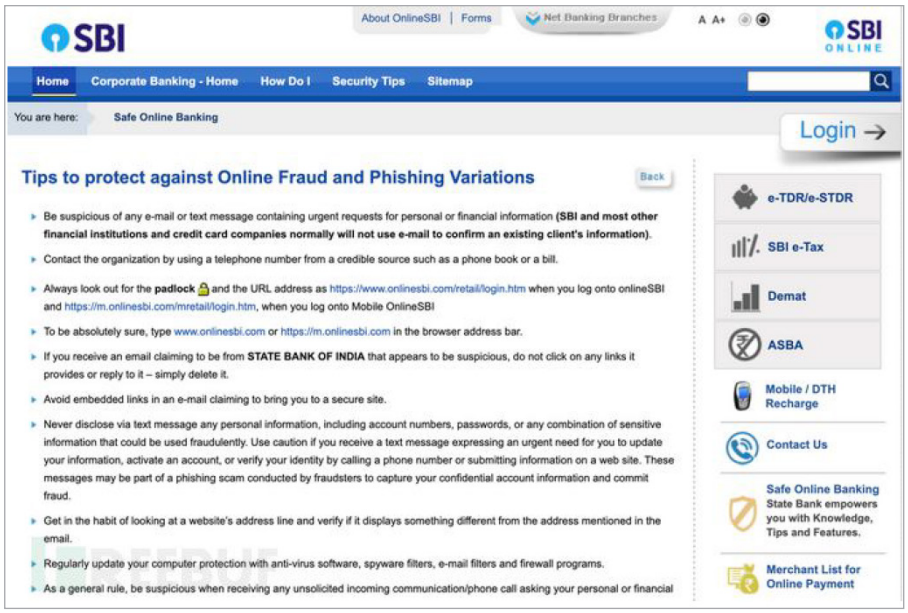


汇丰银行官网向用户展示钓鱼短信

花旗银行用户反钓鱼欺诈公告



澳大利亚联邦银行向用户展示钓鱼短信



印度国家银行有关在线欺诈和网络钓鱼应对说明

在国内，包括：民生银行、华夏银行、招商银行、众邦银行、贵州银行、嘉兴银行、湖州银行、昆仑银行、郑州银行等在内的多家银行纷纷通过官方渠道向用户推送风险提示，对冒充银行短信的新型诈骗手法进行预警：

三、钓鱼攻击背后的黑灰产

网络钓鱼发展历程

钓鱼式攻击（Phishing）作为最早的网络攻击类型之一，其历史可以追溯到上个世纪90 年代。随着移动互联网的发展，传统钓鱼攻击下又演变出移动钓鱼攻击，其中短信钓鱼攻击（Smishing）就是传统钓鱼式攻击（Phishing）的变种：

网络钓鱼技术最早出现于1987 年；

首次使用「网钓」（phishing）这个术语是在1996 年，该词是英文单词钓鱼（fishing）的变种之一，大概是受到「飞客」（phreaking）一词的影响，意味着放钱钓鱼以“钓”取受害人财务数据和密码；

2000 年，通讯信息诈骗由台湾从沿海逐渐向内地发展，并迅速在国内发展蔓延；

2002 年，著名黑客凯文·米特尼克推出一本关于社会工程学的畅销书，名为《欺骗的艺术》（The Art of Deception）；

2004 年，美国联邦贸易委员会提交了涉嫌网钓者的第一次起诉；

2012 年，中国首例入刑的「伪-基站」案件出现；

2013 年，短信拦截木马利用伪-基站传播开始在全国范围内爆发；

2016 年，罗庄徐玉玉通讯信息诈骗猝死案发生，引发社会关注；

2016 年，美国总统大选期间，希拉里团队遭遇钓鱼攻击，邮件信息泄露成为关键转折点；

2018 年，约96%的新加坡企业遭遇过网络钓鱼攻击；

2020 年，受疫情影响，网络钓鱼攻击激增600%

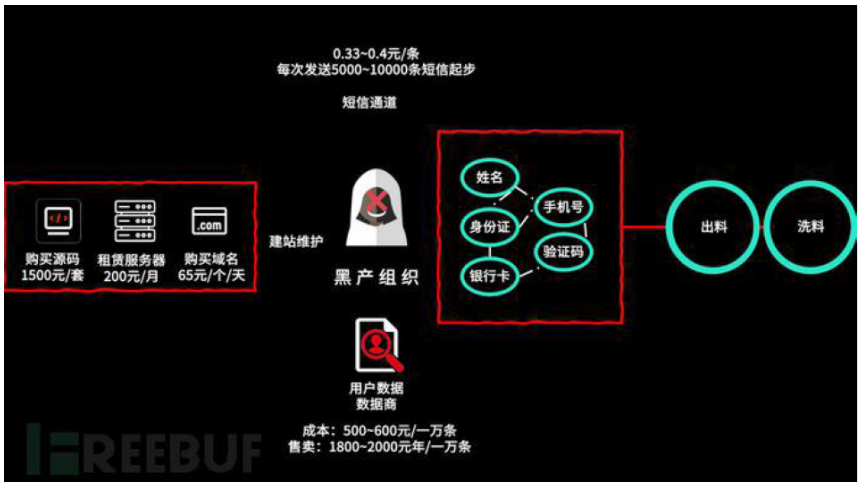
作为移动威胁的一部分，「钓鱼短信」攻击已成为当下互联网的重要威胁。而随着各类信息及数据泄露事件的不断发生，包括：姓名、手机号、银行卡号与身-份证信息等一套完整的公民隐私信息，对黑产而言，已触手可得。

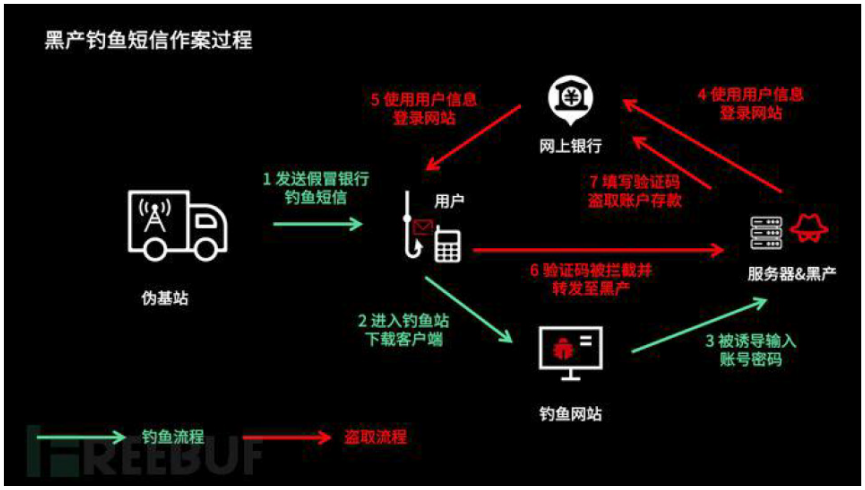
BAAS 模式下的新型钓鱼攻击

随着社会对钓鱼攻击的关注，传统的攻击手段逐渐为用户所熟识，简单的信息诱骗和相似网站内容的欺骗已经很难成功实现钓鱼攻击：

图片来源网络

成本低，风险小，广撒网，多敛鱼的模式已不具备优势，黑产转而向专业化、组织化以及分工细致化发展。一条由包网服务、短信通道、盗刷通道、游戏代充等多个黑灰产业链共同参与的钓鱼短信诈骗组织逐渐兴起。

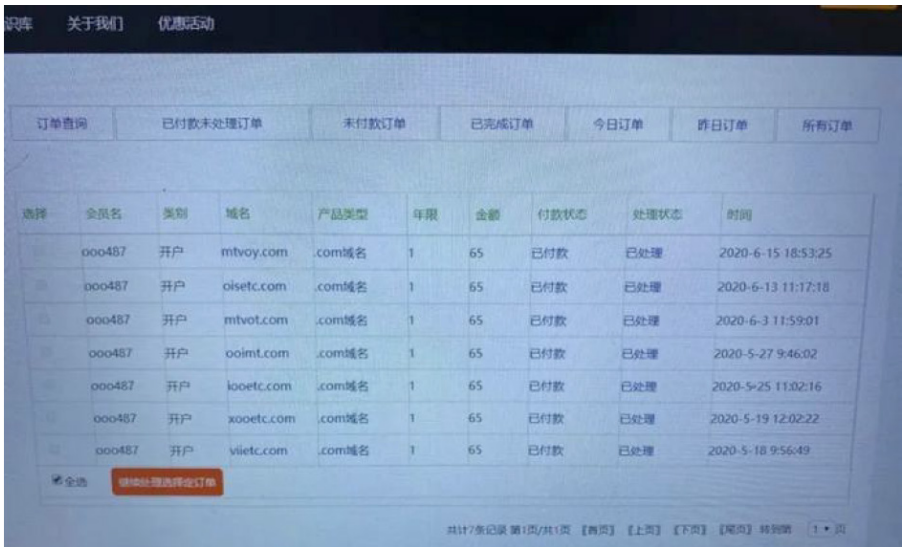




1. 钓鱼网站：

作为诈骗的关键环节，这块基本也是除了数据外，黑产另一项硬支出。包括：仿冒银行域名抢注、各大银行官网的模仿、到大量的适配手机界面的钓鱼网站以及购买美国或者香港免备案服务器进行搭建后制作拦截程序。搭建一个完整的钓鱼网站下来，五年前的价格大概在上千元。

随着分工越来越细，包网服务商出现，他们为黑产提供包括：搭建钓鱼网站、购买域名、服务器租赁甚至网站维护在内的全套服务。为提升竞争力，服务商还开通了各类后台管理系统，为黑产组织提供「一站式钓鱼攻击服务」：



图片来源于网络

2. 精准数据采购

为了提升钓鱼短信转化率，降低运营成本，黑产会向「数据贩子」购买数据。而数据商通过各种渠道，能够拿到各种行业的用户数据，其中以金融行业数据最为热销。

通过黑市、暗网论坛以及社交媒体进行交易，优质的一手数据，按照1 万条算，单价一般能到上千元。一旦黑产掌握了银行用户的真实信息，如姓名、手机号、身份证、银行卡等重要隐私信息后，钓鱼短信的破坏性将得到质的提升。

3. 伪基站发送钓鱼短信：

为了提升反侦察能力以及机动性，伪基站设备也在不断更新，由固定式变为移动式，由大功率变为小功率，由大体积变为小体积，使得违法犯罪分子携带更加轻便并实现移动攻击模式，比如，以每小时500 元左右为酬劳或以合作分成的方式，让人带着设备穿梭于闹市区以及大型社区，「打一qiang 换一个地方」。

现在，国内各大运营商和短信平台的风控机制越来越严格，发送这些钓鱼网站被拦截的概率越来越大，于是有些黑产开始用国际短信通道来发送信息，规避审核。这些国际短信通道也有专门的公司提供，一般5000 条起发，每条3-4 毛钱。

4. 出料

当用户上钩后，黑场会将钓鱼网站后台所收到的数据进行筛选整理，利用各

个银行的在线快捷支付功能查询余额。然后，直接消费、进行转账或第三方支付消费，而针对无法将余额消费的，将会以余额的额度以不同的价格出售（大部分会打包起来以每条1 元的价格进行多次叫卖），余额巨大的有时还会找人合作进行「洗料」。

5. 洗料：

黑产通过多种方式将「料」进行变现，一般开通快捷支付充值水电、话费、游戏币或者利用其他存在第三方支付转账接口和银行快捷支付漏洞等，将「四大件」变成现金后，通过各种规避追查的手段与合伙人按比例进行分账，日均收入都在6 位数以上。

网络钓鱼威胁趋势

与此同时，钓鱼短信仍保持着快速的技术迭代与策略更新：

钓鱼短信形式更加丰富

利用移动通信、短视频平台、富媒体类等营销场景，钓鱼短信所承载的内容也将愈发丰富。这些消息，用于诱使用户下载欺诈性应用程序或打开指向密码窃取或欺诈性移动站点的链接；

内容更加隐蔽

更具欺骗性的文本使用以及短链，向银行用户隐藏实际的欺诈目的。黑产利用合法URL+字符形式+高防域名，让假冒域名在移动设备的小地址栏中仅显示该域的合法部分；

利用紧迫感

配合强调消息的紧迫性以及很难抗拒的诱惑，进一步提升钓鱼短信转化率；

频繁发生的钓鱼攻击案件，正在造成各大银行线上用户的流失。赛门铁克的一项研究表明，将近三分之一的银行用户表示，由于担心遭遇钓鱼攻击，而被迫放弃对网上银行的使用。

四、应对建议

随着钓鱼短信攻击的手段日益复杂，事件持续高发，让银行以及用户蒙受巨大损失，严重影响用户财产安全，并逐渐失去对银行的信心。作为交互安全领域服务商，将从企业与用户的交互视角，审视钓鱼短信攻击：

银行金融机构

早在5 年前的KCon 黑客大会上，网络安全专家Seeker 在《伪基站高级利用技术——彻底攻破短信验证码》中曾明确表示，短信验证码这种安全认证机制可被轻易突破，理应尽快放弃并使用更安全的认证机制。

GSM 伪-基站的搭建：硬件：普通PC、USRP B2X0 + 天线（或Motorola C118／C139 + CP2102）。软件：Ubuntu Linux、OpenBSC。OpenBSC：由Osmocom 发起并维护的一套高性能、接口开放的开源GSM／GPRS 基站系统。

针对短信验证码存在的缺陷与安全隐患，具体表现为：

基于2G 网络的短信安全验证「短信验证码」本身存在缺陷：使用单向鉴权技术，且短信内容以明文形式传输；

目前银行App 在登录、支付甚至是修改密码等关键业务环节，过于依赖「短信验证码」这一安全短板；

当手机短信被拦截，这套身份认证体系将变得格外脆弱；

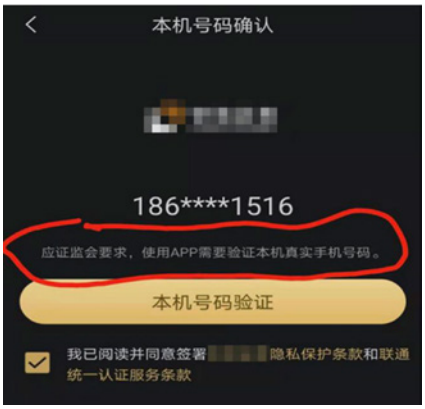
显然，如果仅仅是依靠短信验证码来确认用户身份，具有一定的安

全隐患。对于平台而言，除了短信验证之外，在涉及大额支付及修改用户交易密码等业务场景，增加新的验证手段刻不容缓。

替代方案：脱敏手机号+免短信登录

仔细研究黑产整个钓鱼短信攻击环节，短信是黑产突破银行防线的重要突破口。

而在银行金融机构的关键业务关节，「无感本机认证」正在替代传统短信验证码：



无感本机认证

作为身份校验的升级方案，全国三大运营商推出「无感本机认证」。由运营商网关直接验证用户SIM 卡中的手机号码，全程加密，替代短信验证码。从而让不法分子无短信可嗅探，从根源解决短信嗅探的风险。同时，也大大简化用户操作流程，用户体验更加顺畅，有效提高转化率，帮助银行金融机构优化认证流程，助力拉新、留存、促活。

银行用户

而对于银行用户，提升隐私安全意识，就能抵御超过一半的安全风险：《2019年数据泄露成本报告》中有一组数据，49%的数据泄露是人为错误和系统故障造成的，而这都让他们成为网络钓鱼攻击的牺牲品。

幸运的是，短信网络钓鱼攻击相对容易防御。你会发现，只要什么都不做，通常可以确保自己的安全。所以当遭遇疑似钓鱼短信的时候，不妨冷静下来思考三个问题：

消息来自谁?

他们要我做什么?

哪些证据支持该信息?

当然，如果遭遇短信嗅探，则要迅速做出响应，例如：

发现手机短信验证码发送频繁的情况；

如遇到手机信号较差、无4G 仅有2G 的情况；

发现手机突然变回2G；

作为银行用户，提高对移动安全事件的关注度和敏感度，对与个人关联的事件进行紧急响应，做好事后止损的工作。一旦遭遇以上情况，提高警惕，必要时可采取关机、启动飞行模式等应对措施应对。

可以预见，在之后数年，移动网络安全依然不容乐观。隐私泄露和移动攻击的泛滥和融合还会进一步加深，并导致网络攻击威胁泛滥进一步加深。对抗还将继续，不论是企业还是消费者，唯有不断强化安全意识，提升自身对抗风险能力，并做到及时排除风险隐患，才是不变的真理，从而让自己远离风险。

信息来源：https://www.freebuf.com/news/268370.html

国内某银行存储瘫痪数据缺失 6 个小时

摘　要：《云头条》消息：国内某银行生产中心存储设备发生故障，导致包括核心业务系统在内的多个系统长时间中断，柜面及各电子渠道业务均受到较大影响。

关键词：标签（银行故障、系统中断、数据缺失），技术问题（安全事件）。

内　容：《云头条》消息：国内某银行生产中心存储设备发生故障，导致包括核心业务系统在内的多个系统长时间中断，柜面及各电子渠道业务均受到较大影响。

该行生产中心存储设备（系某国外品牌）因容量扩容操作触发光纤桥接器固件程序缺陷，造成大量磁盘在短时间内出现故障，两个互为备份的控制器同时工作紊乱，数据无法读写，核心、柜面等系统停止运行。

该存储设备还承载了该行虚拟化平台中的数十个信息系统的数据。造成6个多小时业务缺失。

该行未建立同城灾备中心，异地灾备中心仅实现数据级灾备而未实现应用级灾备，异地仅存储了本地备份数据的远程副本，同样与生产系统数据存在较大差距，而且不具备业务所需要的基本软硬件环境，导致核心、柜面、电子渠道等重要信息的灾难恢复能力严重不足。

因故障存储设备无法完全修复，该行紧急调配服务器和存储资源，在本地搭建生产系统，导入备份数据，并通过人工补录方式，逐步恢复缺失业务数据，才得以恢复业务运营。

对数字世界及时有效的灾难管控对于维持现实世界的正常运转至关重要。数字经济时代，数据之于企业、社会的重要性不言而喻，如今“数据保护”作为一项产业已引发业界广泛热议。一个加强数据容灾备份的时代呼之欲出。

回顾历史进程中生产要素的变化，从农业经济时代的土地和劳动力，到工业革命后的资本和技术，再到数字经济时代，数据作为经济发展的新引擎，牢牢抓住时代精神内核，成为最重要的战略资源和新的生产要素。而在今天，数据野蛮生长的时代不再，灾备诉求已成为企业刚需，而数据保护市场也成为了全球主流存储厂商和数据保护厂商觊觎的主战场。可以说，这不单单是数据的时代，更是属于数据保护产业的新时代。

信息来源：http://finance.sina.com.cn/money/bank/bank_hydt/2021-03-25/doc-ikkntiam7991491.shtml

被盗 1450 万！江西“比特币”盗窃案告破：6 名黑客被抓！

摘　要：近期，南昌市公安局青云谱分局成功侦破了一起利用黑客网络技术盗取区块链货币的价值新型网络犯罪案件，实现了对案件上下游犯罪“全链条”的有力打击。

关键词：标签（长风1 号、比特币、网络犯罪），技术问题（安全事件）。

内　容：大江网/大江新闻客户端讯报道：“长风1 号”集中打击收网行动开展以来，南昌市公安局青云谱分局全面动员、全警发动，迅速掀起集中打击收网行动高潮。

近期，该分局成功侦破了一起利用黑客网络技术盗取区块链货币的价值新型网络犯罪案件，实现了对案件上下游犯罪“全链条”的有力打击。截止目前，该案已抓获6名涉案犯罪嫌疑人。

虚拟货币不翼而飞受害者事前无操作

2021 年2 月26 日，辖区群众黄某到分局报案：其称2 月23 日18 时许，突然发现手机号码被他人莫名挂失，继而发现与手机号码捆绑登录的“雷达网”账户中的区块链货币(雷达币和比特币)被人转走，被盗虚拟货币折合人民币价值近1450 万元。接警后民警迅速立案侦查，办案民警在侦查中初步发现——该案中涉及的“雷达网”，属于国外一雷达实验室开办，国内未发现有相应的公司或机构。受害人损失的是虚拟货币，且犯罪嫌疑人未与受害人发生任何实质性接触，也未留下电话、微信等任何联系方式。犯罪嫌疑人在受害人没有任何操作的情况下，盗取安全性较高的虚拟货币账户，而且几乎没有留下作案痕迹。

12 小时内锁定嫌疑人

专案组反诈民警通过摸排走访调查发现，案发前曾有5 名江苏连云港籍男女开车流窜至南昌，持有伪造的受害人身份证件挂失、补办受害人手机卡的犯罪踪迹。获取初步线索后，专案组加班加点、连续攻坚，图侦、情报等警种联合作战，成功锁定涉案嫌疑人基本信息。经过办案民警不到12 个小时的加班加点，案件侦查工作取得重大突破。

转战连云港抓获黑客犯罪嫌疑人家中发现140 余万现金

根据研判线索，专案组连夜奔袭上千公里到达江苏连云港，在当地转战10 天，将嫌疑人轨迹逐一追踪到位。

直到3 月8 日，专案组在连云港市区、灌云县等地陆续抓获该4 名嫌疑人——邓某（女，1991 年2 月出生）、张某1（男，1994 年10 月出生）、王某苗（女，1981 年4月出生）、张某2（女，1991 年1 月出生），并从邓某家中缴获了140 余万现金，以及大量作案用手机、电脑以及各种伪造证件。

3 月15 日，专案组民警又赴广东中山、东莞分别抓获犯罪嫌疑人曾某(男，1997年12 月出生，湖南省耒阳市人)，张某某(男，1992 年11 月出生，安徽省阜南县人)。

经查，犯罪嫌疑人邓某利用购买的黑客技术盗取虚拟货币交易平台“雷达网”后台用户信息，再雇佣犯罪嫌疑人王某、张某等伪造证件冒充受害人补办“雷达网”账户所捆绑手机号码，又通过补办的手机号由犯罪嫌疑人张某接受平台登录验证码，最后登陆受害人存有虚拟币的账户盗取账户内的虚拟货币。张某某负责查询相关信息，确认机主身份后发给曾某。曾某负责制作虚假证件和联系营业厅办理业务。专案组在前期侦查的基础上，逐步挖掘、固定该网络犯罪团伙的证据链条，斩断了该犯罪团伙盗取后台数据、制作假证、冒充受害人补办手机卡，利用手机验证码登录平台进行盗窃的犯罪链条。至此，利用黑客技术盗取虚拟货币的、江西首起特大新型网络犯罪案件实现全链条破案。

目前， 6 名犯罪嫌疑人已依法刑事拘留，此案在进一步审理中。

信息来源：https://www.youxia.org/2021/03/55191.html

一键删好友、修改朋友圈……微信外挂软件主犯被判 10 年

摘　要：近日，广州市南沙区人民法院公开宣判被告人陈某展等38 人提供侵入、非法控制计算机信息系统程序、工具、非法获取计算机信息系统数据、非法控制计算机信息系统、侵犯公民个人信息、掩饰、隐瞒犯罪所得一案。

关键词：标签（微信外挂、非法入侵），技术问题（安全事件）。

内　容：被告人梁某伦、陈某展犯提供侵入、非法控制计算机信息系统程序、工具罪、非法获取计算机信息系统数据、非法控制计算机信息系统罪、侵犯公民个人信息罪，数罪并罚，分别被判处有期徒刑十年、八年六个月，并处罚金人民币十一万六千元、十三万二千元，其余36名被告人犯提供侵入、非法控制计算机信息系统程序、工具罪、非法获取计算机信息系统数据、非法控制计算机信息系统罪、侵犯公民个人信息罪、掩饰、隐瞒犯罪所得罪，分别被判处有期徒刑八年至六个月不等，并处罚金人民币十四万九千元至二千元不等。

2019 年5 月，广州市公安局南沙区分局在侦办一宗以婚恋交友诱骗投资的网络诈骗案中，发现了该以犯罪嫌疑人陈某展为首的制作、售卖以及使用“海贼王”系列软件的犯罪团伙。该局遂立案侦查，并于2019 年8 月抓获犯罪嫌疑人陈某展等人。

法院经审理查明，2018 年3 月，被告人陈某展为更加便捷地销售微信账号，遂让被告人陈某巍、王某帮其开发操作软件。被告人王某在被告人陈某巍提供的微信底层接口协议基础上，先后编写了“黑客数据助手”、“黑客检测助手”、“黑客销售助手”等系列软件。

2018 年年底，被告人陈某展等人为牟取非法利益，将上述软件放在互联网

上公开出售。2019 年春节后,被告人陈某展为进一步扩大微信账号销售规模,将上述软件重新包装后更名为“海贼王”，由被告人王某制作官方下载网站，被告人杜某然制作广告图片、功能介绍视频后进行推广，并先后发展杜某然、梁某伦等人为代理进行销售。

经鉴定，“海贼王”系列软件具有挂机模式、一键删除好友、添加好友、修改朋友圈、一键洗白、检测账户封号、批量实名认证等功能，上述功能均是通过获取计算机信息系统中对应的数据实现。“海贼王”系列软件能够代替人工在微信界面的操作，实现对微信计算机信息系统的控制。

被告人陈某展、梁某伦等人为牟取非法利益，使用“海贼王”系列软件侵入并控制深圳腾讯计算机系统有限公司的计算机系统，批量登入他人微信账号，并进行检测、修改密码、实名认证等操作，非法获取微信账号数据，并向他人销售经“海贼王”软件处理的微信账号获利。

经司法审计，被告人陈某展销售“海贼王”系列软件共计2284 个，销售金额共计人民币456905 元，获利人民币427940 元，其他14 名被告人亦通过销售“海贼王”系列软件获利不等。

南沙法院审理认为，根据审理查明的事实和证据，被告人陈某展、梁某伦等人无视国家法律，违反国家规定,提供专门用于侵入、非法控制计算机信息系统的程序、工具，侵入深圳腾讯计算机信息系统，获取计算机信息系统中的数据、且对腾讯计算机信息系统进行非法控制，向他人出售或非法获取公民个人信息，其行为均已触犯刑律，犯提供侵入、非法控制计算机信息系统程序、工具罪，非法获取计算机信息系统数据、非法控制计算机信息系统罪，侵犯公民个人信息罪，遂依法作出上述判决。

法官提示，类似本案中的微信外挂软件是黑产人员养号、卖号的重要工具，可以为实施网络诈骗等犯罪行为提供大量账号资源，这些外挂功能的出现是对恶意营销行为的纵容，对正常微信用户会造成骚扰和损失，危害严重。法院对于开发、销售非法软件的行为将依法予以惩处，从源头上遏制网络黑产的发展，守护网络安全，营造良好的网络环境。

信息来源：https://www.cnbeta.com/articles/tech/1110349.htm

NSFOCUS

漏洞聚焦

Adobe ColdFusion 远程代码执行漏洞（CVE-2021-21087）通告

发布日期：2021-03-24

一、漏洞概述

3月23日，绿盟科技监测到Adobe官方发布安全公告，修复了代码执行漏洞（CVE-2021-21087），由于对用户输入过滤不严，未授权的攻击者通过向ColdFusion服务器发送精心构造的恶意请求，可在目标服务器上执行任意代码。

Adobe ColdFusion是一个快速应用程序开发平台，ColdFusion经常用在数据驱动的网站及内部网的开发上，但也可以用来生成包括SOAP Web服务及Flash远程服务在内的远程服务。还可以作为Adobe Flex应用的后台服务器。

参考链接：https://helpx.adobe.com/security/products/coldfusion/apsb21-16.html

二、影响范围

受影响版本

☐ Adobe ColdFusion 2021 <= 2021.0.0.323925

☐ Adobe ColdFusion 2018 <= 2018 Update 10

☐ Adobe ColdFusion 2016 <= 2016 Update 16

不受影响版本

☐ Adobe ColdFusion 2021 Update 1

☐ Adobe ColdFusion 2018 Update 11

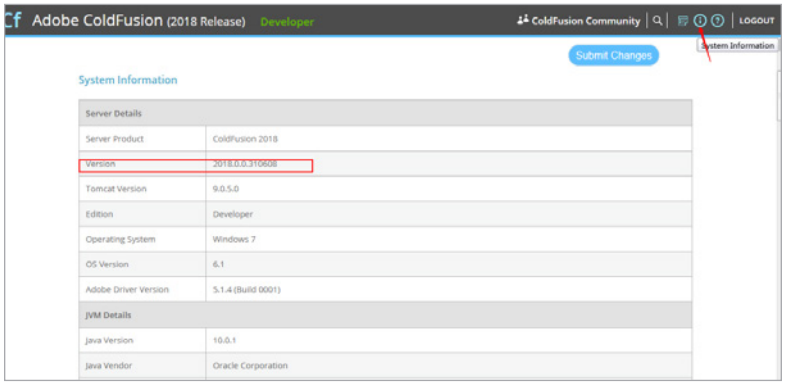
☐ Adobe ColdFusion 2016 Update 17

三、漏洞检测

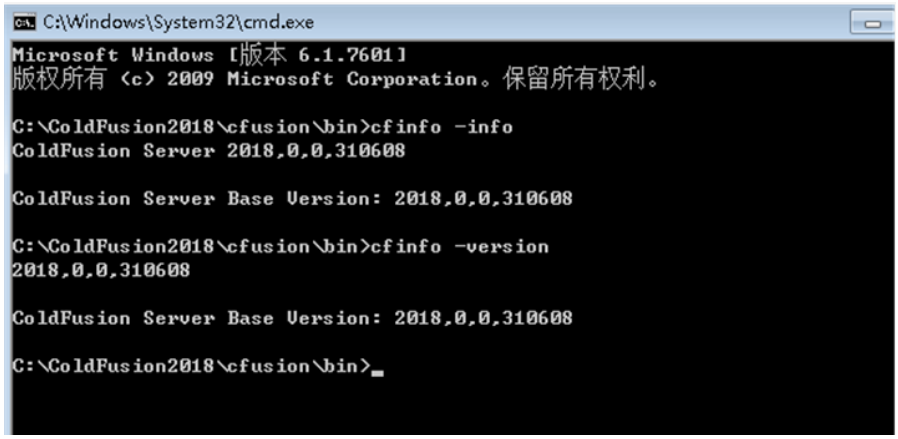
3.1 版本检测

相关用户可通过版本检测的方法判断当前应用是否存在风险。

1. 登陆系统后访问/CFIDE/administrator/index.cfm，查看system inforamtion中的版本



2. 在Adobe ColdFusion安装目录的bin下执行cfinfo -version(info)命令查看版本



若当前版本在受影响范围内，则可能存在安全风险。

四、漏洞防护

4.1 官方升级

目前官方已在最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，对应版本的补丁下载链接如下：

Adobe ColdFusion 2021：

https://cfdownload.adobe.com/pub/adobe/coldfusion/2021/updates/hotfix-001-325996.jar

Adobe ColdFusion 2018：

https://cfdownload.adobe.com/pub/adobe/coldfusion/2018/updates/hotfix-011-326016.jar

Adobe ColdFusion 2016：

https://cfdownload.adobe.com/pub/adobe/coldfusion/2016/updates/hotfix-017-325979.jar

注：Adobe ColdFusion在2016 HF7及之前的版本，需要先将ColdFusion的JDK/JRE更新到8u121或更高版本再进行升级。

根据下载的补丁文件执行以下相应命令（必须具有启动或停止ColdFusion服务以及对ColdFusion根目录有完全访问权限。）

Windows下执行：

```
<cf_root>/jre/bin/java.exe -jar <jar-file-dir>/hotfix-*.jar
```

Linux下执行：

```
<cf_root>/jre/bin/java -jar <jar-file-dir>/hotfix-*.jar
```

确保与ColdFusion捆绑在一起的JRE用于执行下载的JAR。对于独立的ColdFusion，必须位于<cf_root>/jre/bin。

更多信息请参考官方教程：

https://helpx.adobe.com/coldfusion/configuring-administering/using-the-coldfusion-administrator.html#serverupdate

Apache Solr 任意文件读取与 SSRF 漏洞通告

发布日期：2021-03-18

一、漏洞概述

近日，绿盟科技监测到网上披露了Apache Solr的文件读取与SSRF漏洞，由于Apache Solr默认安装时未开启身份验证，导致未经身份验证的攻击者可利用Config API打开requestDispatcher.requestParsers.enableRemoteStreaming开关，从而利用漏洞进行文件读取。目前漏洞PoC已公开，请相关用户采取措施进行防护。

Apache Solr是 Apache Lucene项目的开源企业搜索平台，由Java开发，运行于Servlet容器（如Apache Tomcat或Jetty）的一个独立的全文搜索服务器，主要功能包括全文检索、命中标示、分面搜索、动态聚类、数据库集成，以及富文本的处理。

参考链接：

https://issues.apache.org/jira/browse/SOLR?spm=a2c4g.11174386.n2.4.4fda1051uA9TBw

二、影响范围

受影响版本

☐ Apache Solr <= 8.8.1（全版本）

三、漏洞防护

由于目前官方不予修复该漏洞，暂无安全版本。

3.1 防护措施

1. 开启身份验证/授权，参考官方文档：https://lucene.apache.org/solr/guide/8_6/authentication-and-authorization-plugins.html

2. 配置防火墙策略，确保Solr API（包括Admin UI）只有受信任的IP和用户才能访问。

GitLab 远程代码执行漏洞通告

发布日期：2021-03-18

一、漏洞概述

3月18日，绿盟科技监测到GitLab官方发布安全通告修复了存在社区版(CE)和企业版(EE)中的GitLab 代码执行漏洞，CVSS评分为9.9。未授权但经过身份验证的攻击者通过利用可控的markdown渲染选项，构造恶意请求从而在服务器上执行任意代码。

GitLab 是一个用于仓库管理系统的开源项目，使用Git作为代码管理工具，可通过Web界面访问公开或私人项目。

参考链接：

https://about.gitlab.com/releases/2021/03/17/security-release-gitlab-13-9-4-released/

二、影响范围

受影响版本

- ☐ Gitlab CE/EE < 13.9.4
- ☐ Gitlab CE/EE < 13.8.6
- ☐ Gitlab CE/EE < 13.7.9

不受影响版本

- ☐ Gitlab CE/EE 13.9.4
- ☐ Gitlab CE/EE 13.8.6
- ☐ Gitlab CE/EE 13.7.9

三、漏洞检测

3.1 版本检测

相关用户可通过版本检测的方法判断当前应用是否存在风险。

使用如下命令可查看当前GitLab的版本：

```
cat /opt/gitlab/embedded/service/gitlab-rails/VERSION
```

```
[root@localhost gitlab-rails]# cat /opt/gitlab/embedded/service/gitlab-rails/VERSION
11.0.6
```

若当前版本在受影响范围内，则可能存在安全风险。

四、漏洞防护

4.1 官方升级

目前官方已在最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://about.gitlab.com/update/

4.2 临时防护措施

若相关用户暂时无法进行升级操作，可使用白名单限制对Web端口的访问。

OpenSSL 拒绝服务与证书绕过漏洞（CVE-2021-3449/CVE-2021-3450）通告

发布日期：2021-03-26

一、漏洞概述

3月26日，绿盟科技监测发现OpenSSL发布安全通告，修复了OpenSSL产品中的一个拒绝服务漏洞和一个证书验证绕过漏洞（CVE-2021-3449/CVE-2021-3450）。目前已有PoC披露，请相关用户采取措施进行防护。

CVE-2021-3449：OpenSSL TLSv1.2 默认开启的重协商中存在一处空指针解引用，攻击者通过从客户端发送恶意的重协商ClientHello消息可导致服务器崩溃和拒绝服务。

CVE-2021-3450：在开启了 X509_V_FLAG_X509_STRICT 的 OpenSSL服务器上，由于OpenSSL对X.509证书链的验证逻辑中存在问题，导致受影响的系统接受由非CA证书或证书链签名的有效证书，攻击者可以进行中间人（MiTM）攻击并获取敏感信息。

OpenSSL是一个开源的软件库包，应用程序可以使用这个包来进行安全通信，避免窃听，同时确认另一端连接者的身份，它被广泛应用在互联网的网页服务器上。

参考链接：

https://www.openssl.org/source/

二、影响范围

CVE-2021-3449：

受影响版本

☐ OpenSSL 1.1.1-1.1.1j

CVE-2021-3450：

受影响版本

☐ OpenSSL 1.1.1h-1.1.1j

三、漏洞检测

3.1 人工检测

OpenSSL 拒绝服务漏洞（CVE-2021-3449 ）可通过以下方式检测是否受影响：

```
openssl s_client -tls1_2 -connect your_domain:443
[按 R键]
```

查看RENEGOTIATING下方的内容，如果包含verify关键词则可能存在风险，若出现write:errno=0则不受此漏洞影响。

四、漏洞防护

4.1 官方升级

目前官方已在最新版本中修复了以上漏洞，请受影响的用户尽快升级至1.1.1k版本进行防护，下载链接：https://openssl.en.softonic.com/

XStream 多个高危漏洞通告

发布日期：2021-03-15

一、漏洞概述

近日，绿盟科技监测到XStream官方发布安全公告，公开了XStream中的11个安全漏洞，攻击者可以利用这些漏洞造成拒绝服务、SSRF、删除任意文件、远程执行任意代码。

XStream是一个Java对象和XML相互转换的工具，在将JavaBean序列化、或将XML文件反序列化时，它不需要其它辅助类和映射文件，这使得XML序列化不再繁琐。

CVE-2021-21341:

攻击者可以操纵已处理的输入流，并替换或注入一个ByteArrayInputStream（或其子类），这可能导致一个无休止的循环，从而造成拒绝服务攻击。

CVE-2021-21342:

攻击者可以操纵已处理的输入流并替换或注入对象，导致服务端请求伪造。

CVE-2021-21343:

攻击者可以操纵已处理的输入流并替换或注入对象，从而可以删除本地主机上的任意文件。

CVE-2021-21344:

攻击者可以操纵已处理的输入流并替换或注入对象，从而执行从远程服务器加载的任意代码。

CVE-2021-21345:

攻击者可以操作已处理的输入流并替换或注入对象，从而在服务器上本地执行命令。

CVE-2021-21346:

攻击者可以操纵已处理的输入流并替换或注入对象，从而执行从远程服务器加载的任意代码。

CVE-2021-21347:

攻击者可以操纵已处理的输入流并替换或注入对象，从而执行从远程服务器加载的任意代码。

CVE-2021-21348:

攻击者可以操纵已处理的输入流并替换或注入对象，导致执行恶意正则表达式的计算，从而造成拒绝服务攻击。

CVE-2021-21349:

攻击者可以操纵已处理的输入流并替换或注入对象，从而导致服务端请求伪造。

CVE-2021-21350:

攻击者可以操纵处理后的输入流并替换或注入对象，从而导致任意代码执行。

CVE-2021-21351:

攻击者可以操纵已处理的输入流并替换或注入对象，从而执行从远

程服务器加载的任意代码。

参考链接：

https://x-stream.github.io/security.html#workaround

二、影响范围

受影响版本

☐ Xstream <= 1.4.15

不受影响版本

☐ Xstream = 1.4.16

三、漏洞防护

3.1 官方升级

目前官方已在最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://x-stream.github.io/download.html

3.2 临时防护措施

若相关用户暂时无法进行升级操作，也可使用官方提供的方案进行临时缓解：

https://x-stream.github.io/security.html#workaround

NSFOCUS

安全态势

互联网安全威胁态势

行业动态回顾

1. OpenSSL拒绝服务与证书绕过漏洞（CVE-2021-3449、CVE-2021-3450）

【概述】

2021年3月26日，绿盟科技监测发现OpenSSL发布安全通告，修复了OpenSSL产品中的一个拒绝服务漏洞和一个证书验证绕过漏洞（CVE-2021-3449/CVE-2021-3450）。CVE-2021-3449：OpenSSL TLSv1.2 默认开启的重协商中存在一处空指针解引用，攻击者通过从客户端发送恶意的重协商ClientHello消息可导致服务器崩溃和拒绝服务。CVE-2021-3450：在开启了X509_V_FLAG_X509_STRICT 的 OpenSSL服务器上，由于OpenSSL对X.509证书链的验证逻辑中存在问题，导致受影响的系统接受由非CA证书或证书链签名的有效证书，攻击者可以进行中间人（MiTM）攻击并获取敏感信息。

【链接】

https://nti.nsfocus.com/threatWarning

2. GitLab多个高危漏洞

【发布时间】

2021-04-02 15:00:00 GMT

【概述】

2021年4月1日，绿盟科技监测到GitLab官方发布安全通告，修复了存在于社区版(CE)和企业版(EE)中的多个高危漏洞。Project Import文件读取漏洞：从13.9开始的GitLab版本，攻击者可以通过导入特定的文件读取服务器上的任意文件。

Wiki page文件读取漏洞：攻击者通过特制的 Wiki 页面在服务器上读取任意文件。文件读取漏洞：从12.6开始的GitLab版本，攻击者可以用匿名用户的身份通过公共项目fork访问内部存储库的数据。文件删除漏洞：从13.8开始的GitLab版本，经过验证的攻击者可以删除公共项目的图像。跨站脚本攻击漏洞：从13.4开始的GitLab版本，攻击者通过制作特定的分支名称在合并请求中触发跨站脚本攻击。

【链接】

https://nti.nsfocus.com/threatWarning

3. 台湾计算机制造商宏碁遭勒索软件攻击

【概述】

台湾计算机制造商宏碁遭REvil勒索软件组织攻击，攻击者要求在3月28日之前支付支付5000万美元的巨额资金，否则将泄露其机密数据。攻击者可能通过微软Exchange漏洞入侵宏碁网络。

【参考链接】

https://www.forbes.com/sites/leemathews/2021/03/21/acer-faced-with-ransom-up-to-100-million-after-hackers-breach-network/?sh=49d011ad750f

4. SilverFish网络间谍组织

【概述】

SilverFish是一个高度复杂的网络间谍组织，针对世界各地的大公司和公共机构，重点目的为欧盟和美国。SilverFish组织与SolarWinds攻击、EvilCorp组织以及其他一些知名的恶意软件活动有着密切的关系。

【参考链接】

https://www.prodaft.com/m/uploads/SilverFish_TLPWHITE.pdf

5. 5G核心网络切片因存在安全漏洞易遭受DoS攻击

【概述】

安全研究人员发现了5G网络切片和虚拟网络功能架构中的一个主要漏洞，已发现此漏洞潜在地允许移动运营商上不同网络切片之间的数据访问和拒绝服务（DoS）攻击，从而使企业客户容易受到恶意网络攻击。受此漏洞影响最大的国家和地区，包括韩国、英国、德国和美国。

【参考链接】

https://www.hackread.com/5g-vulnerability-core-network-slicing-dos-attacks/

6. Purple Fox通过蠕虫攻击Windows服务器

【概述】

2021年3月23日，安全研究人员发现Purple Fox增加了蠕虫传播模块，通过扫描、攻击联网的 Windows 系统进行感染传播。与此同时，更新的Purple Fox还带有Rootkit和后门功能。Purple Fox针对Windows系统进行漏洞利用套件的开发，在利用内存破坏和权限提升漏洞后，通过Web浏览器感染Windows用户。2018年，Purple Fox（紫狐）在野感染超过 30000 台计算机后被首次发现。Purple Fox通过漏洞利用和钓鱼邮件进行传播分发，自身还充当其他恶意软件的 Downloader。

【参考链接】

https://www.guardicore.com/labs/purple-fox-rootkit-now-propagates-as-a-worm/

7. Facebook跟踪针对维吾尔族人的攻击组织

【概述】

Facebook对与中国有联系的网络间谍组织使用的一系列帐户进行了跟踪，该组织被称为Earth Empusa 或Evil Eye，以在居住在中国境外的维吾尔族活动家、记者和持不同政见者使用的设备上部署监视恶意软件，攻击者使用PoisonCarp或INSOMNIA等间谍软件将属于维吾尔族目标的iOS设备作为攻击目标。

【参考链接】

https://securityaffairs.co/wordpress/115956/apt/facebook-china-apt-uyghur.html

8. Black Kingdom勒索软件攻击未修补的Exchange服务器

【概述】

近期安全研究专家发现一种新勒索软件Black Kingdom针对xchange电子邮件服务器发起攻击活动。上周，安全公司RiskIQ统计仍有未修补超过45万台本地Exchange服务器，并且大多数位于美国。

【参考链接】

https://www.inforisktoday.com/black-kingdom-ransomware-hits-unpatched-exchange-servers-a-16258

9. Sierra Wireless物联网公司遭勒索软件攻击

【概述】

上周，物联网公司Sierra Wireless披露了勒索软件攻击，该攻击于2021年3月20日袭击了其内部IT系统，并中断了其生产。Sierra Wireless是加拿大跨国无线通信设备设计人员和制造商，总部位于加拿大不列颠哥伦比亚省里士满。

【参考链接】

https://securityaffairs.co/wordpress/115897/malware/sierra-wireless-ransomware.html

10. Hobby Lobby零售商138GB敏感信息遭泄露

【概述】

工艺品零售商Hobby Lobby遭受了云存储桶的错误配置，暴露了138GB敏感信息，其中包括客户姓名、部分支付卡详细信息、电话号码、通讯地址和电子邮件地址等客户详细信息，还包括公司应用程序的源代码、员工姓名和电子邮件地址。

【参考链接】

https://threatpost.com/hobby-lobby-customer-data-cloud-misconfiguration/164980/

11. BlackRock恶意软件伪装成Clubhouse应用窃取信息

【概述】

BlackRock恶意软件伪装成音频聊天应用程序Clubhouse的Android版本，旨在窃取受害者的登录凭证。

【参考链接】

https://www.hackread.com/trojan-malware-blackrock-android-clubhouse-app/

12. 加利福尼亚州控制局(SCO)遭网络钓鱼攻击

【概述】

上周的网络钓鱼攻击使攻击者可以访问加利福尼亚州控制局

（SCO）的电子邮件和文件，入侵者窃取了成千上万名州工作人员的社会安全号码和敏感文件，并向至少9,000名其他工人及其联系人发送了针对性的网络钓鱼消息。

【参考链接】

https://krebsonsecurity.com/2021/03/phish-leads-to-breach-at-calif-state-controller/

13. 2020年全球数据泄露超过去15年总和

【概述】

Canalys的最新报告称，2020年数据泄露危机升级，在短短12个月中泄露的记录比过去15年的总和还多。同时勒索软件攻击激增，与2019年相比增长60%。这种前所未有的攻击热潮可部分归因于新冠疫情影响。

【参考链接】

https://canalys.com/newsroom/cybersecurity-investment-2020

14. 黑客声称窃取了8.2TB的MobiKwik数据

【概述】

印度支付应用程序公司MobiKwik因隐瞒泄露了近8.2TB数据而受到批评，其中包括敏感记录，例如KYC详细信息、电话号码、地址、Adhaar卡和其他敏感数据。这些数据已被放在暗网上以1.5比特币的价格出售，约86000美元。

【参考链接】

https://www.hackread.com/hacker-steal-mobikwik-data-leaks-online/

15. WordPress搜索插件中XSS漏洞影响6万多个站点

【概述】

2021年3月28日，安全研究人员披露了Ivory Search中的一个漏洞，Ivory Search是一个安装在60,000多个站点上的WordPress搜索插件。攻击者可以利用此安全漏洞在受害者的网站上执行恶意操作，该漏洞是XSS漏洞，影响Ivory Search插件版本4.6.0及更低版本。

【参考链接】

https://securityaffairs.co/wordpress/116140/hacking/reflected-xss-ivory-

search-wp-plugin.html

16.《智慧城市白皮书（2021年）》发布

【概述】

近日，由国家工业信息安全发展研究中心、联想集团、中国产业互联网发展联盟、工业大数据分析与集成应用实验室共同编制的《依托智慧服务，共创新型智慧城市——智慧城市白皮书（2021年）》（以下简称“白皮书”）正式发布。该白皮书采用案例分析、实证分析、调研分析等研究方法，深入剖析我国智慧城市发展历程与内在规律，针对智慧城市当前的发展情况，提出一系列智慧城市建设的新理念、新架构、新建议，旨在为建设应用技术先进、社会效益良好、生态环境友好的新型智慧城市提供参考。

【参考链接】

https://mp.weixin.qq.com/s/BcRKpzbYGzd5JH-TPu6FxA?scene=25#wechat_redirect

17. Cl0p勒索软件集团泄露了美国六所大学的学生信息

【概述】

Cl0p勒索软件组织泄露美国六所顶尖大学的学生详细信息，其中包括在校学生的照片、出生年月、家庭住址、护照号码、移民身份、个人姓名和社会安全号码。

【参考链接】

https://seguranca-informatica.pt/cl0p-ransomware-group-compromised-and-leaked-data-from-6-us-universities-including-students-details/

18. 制造业成为黑客头号目标

【概述】

网络安全公司趋势科技最新发布的报告称，制造业企业已经成为网络犯罪分子、勒索软件和国家黑客的首要目标， 61%的企业工厂发生过网络安全事件，其中四分之三导致生产线下停摆。

【参考链接】

https://resources.trendmicro.com/Industrial-Cybersecurity-WP.html

19. 2020年无文件恶意软件数量飙升900%

【概述】

根据Watchguard Technologies的最新数据，由于攻击者不断提高隐蔽性绕过传统安全控制，2020年，无文件恶意软件的检测量同比增长了近900%。由于攻击者试图通过在不安装恶意代码的情况下进行攻击，从而试图逃避许多端点保护产品的监视，因此无文件恶意软件比率在过去一年中迅猛增长。

【参考链接】

https://www.watchguard.com/wgrd-resource-center/security-report-q4-2020

20. 针对视频游戏玩家和PC改装者的攻击活动

【概述】

近期攻击者利用游戏中后门专门针对游戏玩家和PC改装者，这些游戏调整隐藏了能够通过获取麦克风和网络摄像头访问权而从其系统中窃取信息的恶意软件XtremeRAT，该恶意软件是一种商业可用的远程访问木马。

【参考链接】

https://www.hackread.com/gamers-malware-attack-games-cheat-codes/

21. Boggi Milano服装公司遭受Ragnarok勒索软件攻击

【概述】

Boggi Milano服装公司遭受Ragnarok勒索软件攻击，此次攻击活动窃取了40 GB的敏感数据，其中包括工资单文件、付款PDF、凭证、税务文件等。Boggi Milano的总部位于意大利，据该公司称，在全球38个以上的国家/地区拥有190家商店，为男士提供高端时尚装扮。

【参考链接】

https://threatpost.com/ragnarok-ransomware-boggi-milano-menswear/165161/

22. Hades勒索软件瞄准三家美国公司的攻击活动

【概述】

近期未知的威胁组织正在部署Hades勒索软件针对美国运输、消费品和制造业的三家公司进行网络攻击活动。

【参考链接】

https://www.inforisktoday.com/hades-ransomware-targets-3-us-companies-a-16268

23. 工信部通报下架60款侵害用户权益APP

【概述】

2021年3月11日，工信部向社会通报了136家存在侵害用户权益行为APP企业的名单。截至目前，经第三方检测机构核查复检，尚有53款APP未按照要求完成整改。依据《网络安全法》和《移动智能终端应用软件预置和分发管理暂行规定》（工信部信管〔2016〕407号）等法律和规范性文件要求，工信部组织对60款APP进行下架。

【参考链接】

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

24. Cycldek组织针对越南政府和军队的攻击活动

【概述】

Cycldek（又名 Lucky Mouse、APT27、Goblin Panda和Conimes）是一

个自2013年以来一直很活跃、并与中国有关的威胁组织。Cycldek组织正在利用FoundCore 恶意软件监视越南政府和军队，FoundCore使攻击者能够执行文件系统操纵、捕获屏幕截图、处理操纵以及执行任意命令。

【参考链接】

https://securelist.com/the-leap-of-a-cycldek-related-threat-actor/101243/

25. WatchDog实施加密劫持活动已有两年

【概述】

WatchDog挖矿劫持自2019年1月27日以来一直在运行，目前已收集至少209个门罗币（门罗币），价值约32056美元，已知存在的最大、持续时间最长的门罗币加密劫持活动。同时，至少有476个主要由Windows和NIX云实例组成的被破坏的系统在任何时间都在进行挖掘操作，时间超过了两年。

【参考链接】

https://unit42.paloaltonetworks.com/watchdog-cryptojacking/

26. 针对巴西的银行木马Janeleiro

【概述】

银行木马Janeleiro近期较活跃，Janeleiro木马自2019年以来一直瞄准巴西的企业用户，涉及多个垂直领域，涉及工程、医疗保健、零售、制造业、金融、运输和政府等领域。Janeleiro木马在攻击活动中试图通过弹出窗口来欺骗受害者，这些弹出窗口的外观类似于巴西一些大型银行的网站，弹出窗口包含伪造的表格，旨在诱使恶意软件的受害者输入银行凭证和个人信息。

【参考链接】

https://www.welivesecurity.com/2021/04/06/janeleiro-time-traveler-new-old-banking-trojan-brazil/

27. 黑客利用Fortinet VPN中的关键漏洞

【概述】

高级持续威胁（APT）组织利用FortiOS网络安全操作系统中的已知漏洞，并将目标锁定为Fortinet的SSL VPN产品，旨在破坏大中型企业的安全性。FortiOS SSL VPN用于边界防火墙，负责从其他公共Internet连接中隔离敏感的内部网络。

【参考链接】

https://www.hackread.com/fbi-cisa-hackers-exploit-fortinet-vpn-vulnerabilitie

28. 针对Applus公司的恶意软件攻击阻止了美国某些州的车辆检查

【概述】

车辆检测服务提供商Applus Technologies，是测试、检查和认证领域的全球领导者，该公司最近受到恶意软件网络攻击，被迫从Internet断开其IT系统的连接，以防止恶意软件传播。此次攻击活动影响了美国八个州的车辆检查，包括康涅狄格州、乔治亚州、爱达荷州、伊利诺伊州、马萨诸塞州、犹他州和威斯康星州。

【参考链接】

https://securityaffairs.co/wordpress/116338/malware/malware-attack-on-applus.html

29. 针对医疗保健组织的网络钓鱼事件使更多人受影响

【概述】

随着医疗保健组织继续成为网络钓鱼事件的受害者，涉及受损电子邮件帐户的健康数据泄露影响的个人数量继续增加。2021年第一季度美国卫生和公共服务部记录健康数据泄露事件125起，涉及约940万人，其中最大规模的网络钓鱼事件影响近130万人。

【参考链接】

https://www.inforisktoday.com/healthcare-phishing-incidents-lead-to-big-breaches-a-16339

30. 勒索团伙通过电子邮件向受害者客户索要筹码

【概述】

一些勒索软件团伙正在采用一种新的压力策略，以迫使更多的受害者组织支付勒索要求：直接通过电子邮件向受害者的客户和合作伙伴发送电子邮件，警告他们的数据将泄漏到暗网中，达到勒索目的。

【参考链接】

https://krebsonsecurity.com/2021/04/ransom-gangs-emailing-victim-customers-for-leverage/

31. 攻击者正在滥用GitHub基础设施来挖掘加密货币

【概述】

攻击者正在滥用GitHub Actions功能，该功能是为了允许自动执行软件工作流而实施的，攻击过程将具有此功能的存储库定位为目标，以启用该功能来添加恶意的GitHub操作并填充恶意的“拉取请求”以执行恶意攻击者的代码，旨在滥用其基础设施来非法开采加密货币。

【参考链接】

https://securityaffairs.co/wordpress/116294/malware/github-infrastructure-attacks-miner.html

32. 被忽视的固件保护

【概述】

微软发布的一份新报告显示，过去两年中，全球80%的企业都是针对固件的网络攻击的受害者，同时指出，只有29%的目标组织分配了预算来保护固件。该研究基于来自中国、德国、日本、英国和美国的1000位企业安全决策者贡献的数据，显示大多数安全投资将用于安全更新、漏洞扫描和高级威胁防护解决方案。

【参考链接】

https://www.microsoft.com/en-us/secured-corepc

33. Conti勒索软件清理费用苏格兰机构110万美元

【概述】

Conti勒索软件团伙在2020年平安夜攻击了苏格兰环境保护局，到目前为止，此次攻击事件让苏格兰环境保护局已花费了将近790,000英镑（110万美元），在该金额中，有635,000美元用于稳定该机构的IT平台。

【参考链接】

https://www.bbc.com/news/uk-scotland-56612867

从边界防护
到数据交互
再到安全部署
数据安全高枕无忧

IATF行为域
全面覆盖边界接入
网络基础设施
计算环境及支撑性设施域

从风险评估
到渗透测试
再到代码审计
合规绿灯一路狂飙

从现场运维，
到后台服务，
再到管理体系
业务连续顺风顺水

贴身服务 加油干

绿盟科技城商行信息安全解决方案

无缝衔接 | 密切配合

THE EXPERT
BEHIND GIANTS
巨人背后的专家

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

NSFOCUS绿盟科技

安全月报

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/