金融行业

2 月报
2020 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

“安全中台”让安全举重若轻

行业研究

远程办公安全防护指南

从常态化演练看安全建设

浅析5G网络安全需求

欧洲名校遭黑客勒索付了30 个比特币赎金

印度APT 组织趁火打劫对我国医疗机构发起定向攻击！丧尽天良！

NSFOCUS

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

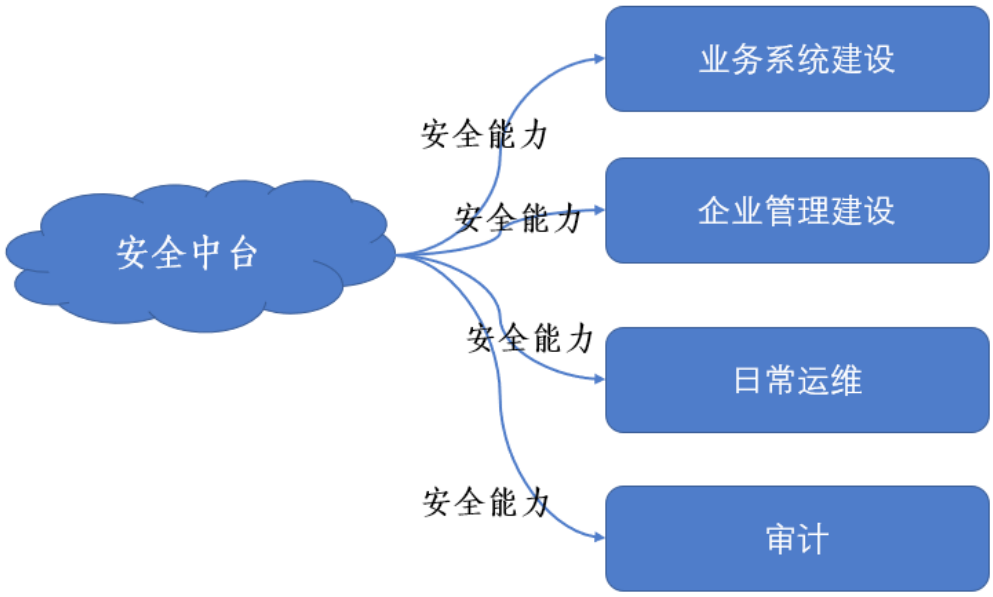
无缝衔接 —— 密切配合

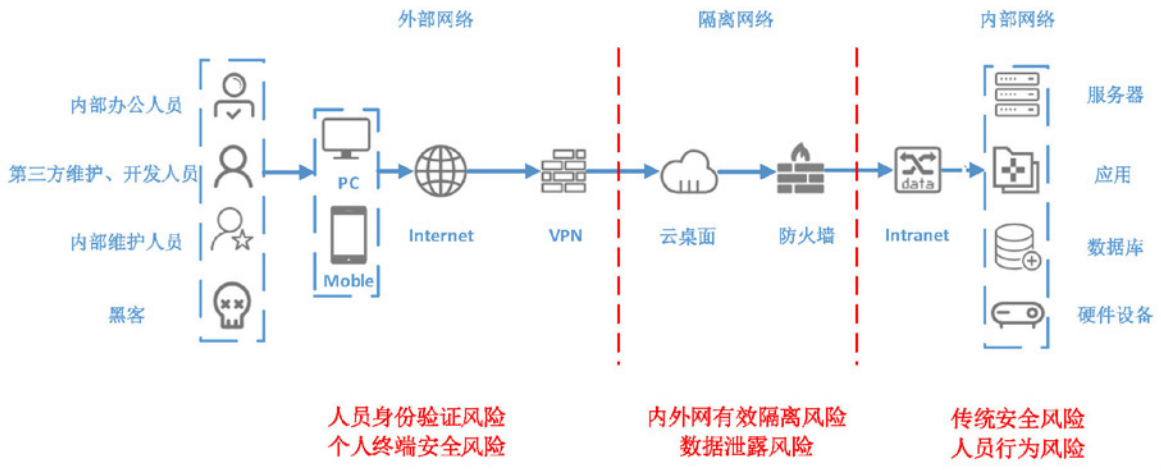
THE EXPERT
BEHIND GIANTS
巨人背后的专家

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

本|期|看|点





安全月报

2020年第2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

安全观点

行业研究

漏洞聚焦

安全态势

NSFOCUS

安全观点

“安全中台”让安全举重若轻

金融事业部　梁晴

1. 安全中台的概念

中台和前台、后台对应，在应用系统中指的是在一些系统中，被共用的中间件的集合。常见于网站架构、金融系统等。企业的安全中台是指基于标准的协议和流程，将企业现有的安全资源和专业安全服务能力，通过IT技术共享给企业一线的各个业务单元或其他管理部门。提供基于企业业务及管理变化创新的快速集成安全能力的响应支持。

2. 安全中台建设的意义

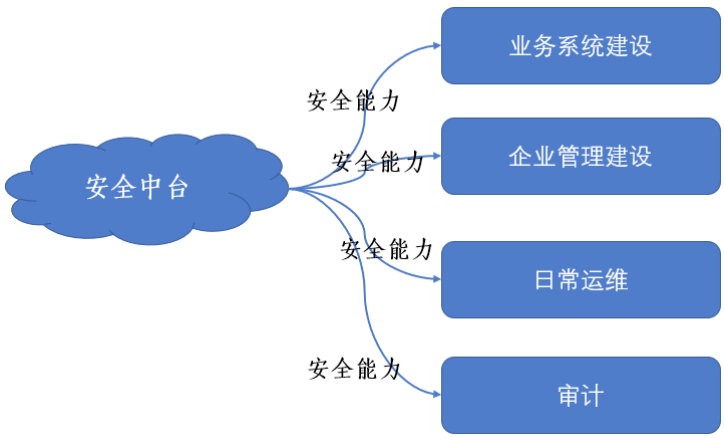
现如今，随着信息技术的不断发展和信息化建设的不断进步，企业中的业务系统、内部管控措施，日常运维工具、内部审计措施不断推出和投入运行。由于各类IT资产众多，业务逻辑复杂，人员不足等因素。越权访问、误操作、滥用、恶意破坏等情况时有发生，另外黑客的恶意访问也有可能获取系统权限，闯入部门或企业内部网络，造成不可估量的损失。

产业互联网时代，安全已成为企业数字化转型的原生需求，既是企业发展的底线，也是制约企业发展的天花板，需要系统性构建。但是对于每个业务系统而言，正面临三个普遍困惑：第一，不知如何评估安全构建投入的成效，信息安全是否存在重复建设的情况。不可能为每个业务单元或部门都配备安全团队及安全技术。第二，业务单元负责人相对来说普遍缺乏信息安全相关经验。借助安全中台，做好产业安全战略官，降低业务系统的安全门槛，帮助业务系统快速构建系统化的安全能力，达到安全成本和效率两方面的平衡。第三，传统的信息安全建设驱动力主要是合规以及风险，信息安全和企业的业务运营关联不密切，可能导

致企业内部人员误以为安全团队只是单纯增加业务部门工作量，没有业务收益。

安全中台的搭建，相当于为企业提供一个随用随取的安全产品“货架”,从而满足企业内各业务系统、内部管控、日常运维、审计等的个性化安全需求。为企业的业务以及整体顺畅运行提供安全支撑服务，安全团队一个很重要的职责是服务企业内部其他部门。目的是提高各业务单元安全水平，提供企业管理的安全策略，跟踪各类用户的操作行为，防止黑客的入侵和破坏并提供防护手段和审计依据。使得信息安全完全融入企业业务，为企业业务正常运行的安全保驾护航，让企业整体的安全举重若轻。这将是企业革新性的安全方式。也为信息安全建设赋予除合规和风险以外的其他重要意义。实现安全运维到整体安全运营的转变

3. 安全中台总体思想



如图所示，安全中台能够提供各种不同级别的安全能力给企业内部各个相关部门，包括各业务系统建设、内部管理系统建设，日常运维操作、审计系统等，使得企业各系统可以实现快速搭建、部署、测试和拆除安全环境，降低安全部署的时间、人力成本。

安全中台具体应该包括以下内容：

1）为安全能力的实现统一标准。

我们需要制定某种标准，让安全能力以某种约定形式进行封装,就像标准服务一样。

2）异构集成，满足安全能力无缝对接

异构集成是安全中台的核心能力之一，也是降低创新成本的关键。异构集成能够快速融合新安全能力，提高兼容性。分别实现安全能力的快速集成和前台应用的快速调用。

3）提供安全流程及规范化能力。

我们都知道企业内部很多工作例如开发、运维、数据管理等是需要协调多个安全功能一起工作，需要完成一系列流程，走过一系列的功能点。如何让这些业务可以很好的协同工作，也需要一个标准的流程。

4. 安全中台的常见安全能力

1）集中帐号管理及访问控制

为用户提供统一集中的帐号管理实现单点登录，并提供安全的身份认证方法（复杂密码，生物识别，token，密钥或以上任意二种组合）。

通过整体访问控制策略保障企业内部使用的物理，网络资源，数据资源和各类应用系统资源等客体的机密性和完整性；访问控制策略包含基于角色以及强制访问控制策略。不仅能够实现被管理资源帐号的创建、删除及同步等帐号管理生命周期所包含的基本功能，而且也可以通过角色或标签来限制账号的访问客体的权限。并记录所有账号的关键操作用于审计。实现整体企业级的综合访问控制平台。

2）安全威胁监控及告警

利用大数据技术统一收集各种基础架构，安全设备以及应用系统等日志。进行综合关联安全分析。发现可能的攻击行为。为相关一线部门提供安全告警，并给出处理建议。实现统一的威胁分析告警平台。

3）漏洞管理

收集各类基础架构以及应用程序的漏洞信息，根据企业的资产重要等级，CVSS评分，利用难度，攻击矢量等度量值来确定漏洞风险级别，给出建议的漏洞修复时间窗口及可落地的漏洞修复方法。修复方法包含但不限于打补丁，修改配置，严格的访问控制措施等。

4）安全开发资源库

为开发部门提供安全需求库，安全设计库，安全代码样例以及可直接调用的安全组件，安全测试用例等资源库。使开发部门可以快速了解当前开发周期内的安全需求，实现方法以及验证方法。为应用开发安全提供有力支撑

5）威胁情报

收集社会以及行业内的安全威胁情报，给企业内部相应部门提供威胁预警。提早进行防范。

6）数据保护

提供数据加解密，数据模糊化，数据脱敏等数据保护安全能力供其他部门按照自身的数据安全需求自行调用。

5. 总结

安全中台主要指能够被共用的安全资源，包括账号管理及访问控制、威胁监控及告警、安全开发资源库、漏洞管理，威胁情报，数据保护等安全能力，并能够按需集成新的安全能力。现在的安全中台,相当于为企业提供一个随用随取的安全能力“货架”, 可以有效的整合企业内的各种安全能力,从而满足不同业务单元及企业管理的个性化安全需求；现在的安全中台也是连接业务能力和安全能力的桥梁, 做到企业安全能力与业务需求的持续对接。将来的安全中台，将向人类的

神经系统一样，可以在转瞬之间，随着外界环境的变化，随时做出身体的应激反应。

可以预见，随着企业内部的安全中台的提供的安全能力越来越完善，安全中台不单单可以为本企业提供安全能力支持，还可以向全社会输出安全能力为本企业产生经济效益，让信息安全成为企业重要业务收入来源之一。

参考文献：

1. https://new.qq.com/omn/TEC20190/TEC2019073000496600.html
2. https://new.qq.com/omn/TEC20191/TEC2019110700886600.html
3. https://www.zhihu.com/question/57717433
4. https://www.jianshu.com/p/40efdeafc8cd
5. http://www.sohu.com/a/362545842_244641

NSFOCUS

行业研究

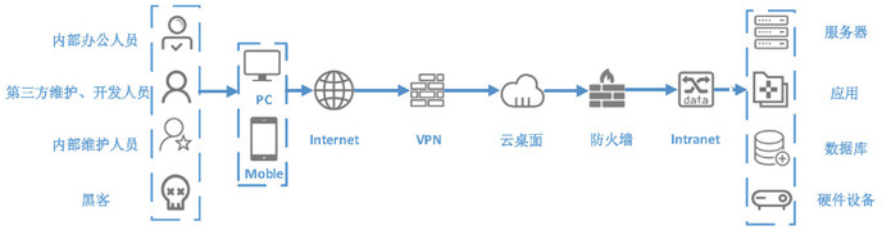
远程办公安全防护指南

绿盟科技　姚兴

因受新型冠状病毒肺炎疫情的影响，多省市单位和企业宣布推迟复工时间，全民抗“疫”时期，在家远程办公模式成为了众多企业的选择。远程办公模式在为我们提供方便的同时，也带来了一些问题，其中安全性就是影响远程办公的重要因素之一。办公设备的不同、网络环境的不同，大规模人员的远程办公带来的安全风险成为我们急需关注和解决的问题。

本文通过对传输路径上的安全风险进行分析，提出一些可行的安全防护指南和建设方案。

1. 整体安全风险分析

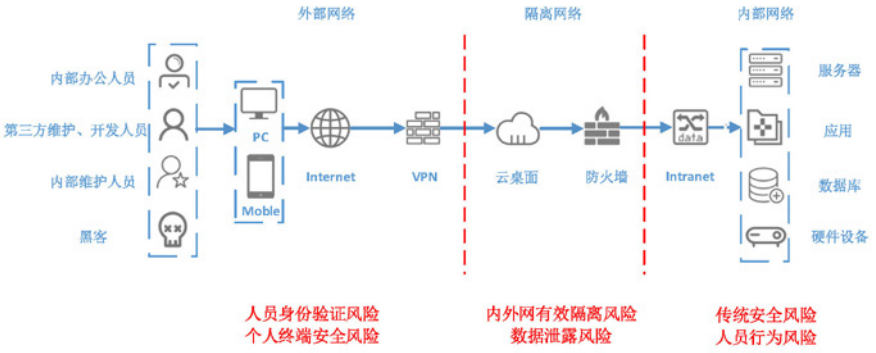


根据上图所示，整个传输路径为：

人员（办公人员、第三方维护、开发人员、内部维护人员及黑客等）→个人设备（PC、移动终端等）→互联网→VPN→云桌面（有些企业无相关措施）→防火墙（有些企业无相关措施）→内部网络→内部设备及应用（服务器、应用、数据库及硬件设备等）。

而在此基础上的最大风险其实是外部访问的“人”，作为安全管理者无法对相关人员的真实性进行确认，而其行为更加无从得知。

所以，远程办公由于在传输路径上访问者的不确定性，增加了内部安全访问风险。对于以往只在内部开放的系统，这种风险被进一步放大，以下我对传输路径风险进行分段分析，详见下图：



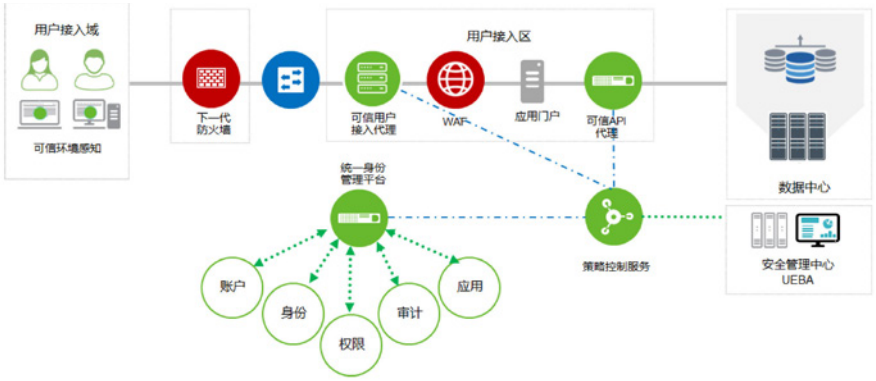
根据上图，远程办公的传输路径可以分成外部网络、隔离网络及内部网络进行分析，其主要安全风险为上图所示，以下将根据相关安全风险提出一些分层次的防护指南，以最大程度缓解或消除相关风险。

2. 外部网络安全防护指南

外部网络由于与互联网相连，同时对于“最核心”的人员无法做到完全掌控，所以遇到的风险也是最大的，对于其主要风险防护及安全运营有以下建议：

◆ 人员身份验证风险防护建议：

1、大型企业及政府/风险等级非常高场景：可以考虑建立“零信任”安全体系，通过建立 “零信任”安全体系第一阶段功能——零信任网络访问，实现初步的用户可信访问通道，账户、认证和授权。



2、中型企业及政府/风险等级高场景：可以优先考虑采用基于双因素或多因素的安全认证体系进行VPN的接入，在条件允许的情况下进行单点登陆建设，提高客户安全体验并增强安全性。

3、小微企业/风险等级一般场景：可以对VPN日志进行定期审计，发现可疑行为进行进一步分析，防止由于黑客入侵或内部人员滥用，引起的安全事件。

◆ 个人终端安全风险防护建议：由于个人终端的不确定性，建议在个人终端上安装“有效”的杀毒软件进行基础防御，所谓“有效”至少满足杀毒软件客户端为最新的客户端，其病毒库也为最新的病毒库。

◆ 安全运营建议：

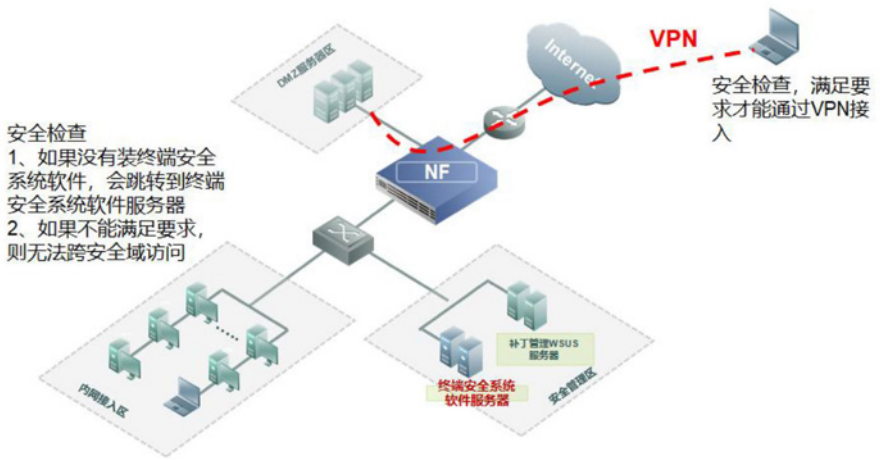
1、在保证业务安全的前提下，更新所有防护和接入设备的软件版本至最新，其他区域设备更新不再赘述；

2、定期VPN设备的账号安全、日志审计是无论大型企业和政府场景还是小微企业场景下都需要认真完成的基础工作，如：对默认及弱口令的排查、异地登陆IP地址进行确认、对非工作时间的访问行为、异常的访问失败频次等问题都是潜在的安全威胁；

3、在部署VPN时，可以考虑个人终端MAC地址与VPN进行绑定，防止非授权的设备访问，同时，对接入VPN在本地落地的内网IP地址需单独划分，以进一步对其进行访问控制及行为审计等操作；

4、在条件允许的情况下，对相关人员使用场景进行分类梳理并进一步进行访问控制，进而减小攻击面，如内部办公人员账号只访问内部web业务系统，内部维护人员通过云桌面访问到堡垒机等；

5、最后可以考虑防病毒软件和VPN进行联动，只有当在个人终端安装杀毒软件并且病毒库版本为最新时，方可接入VPN。

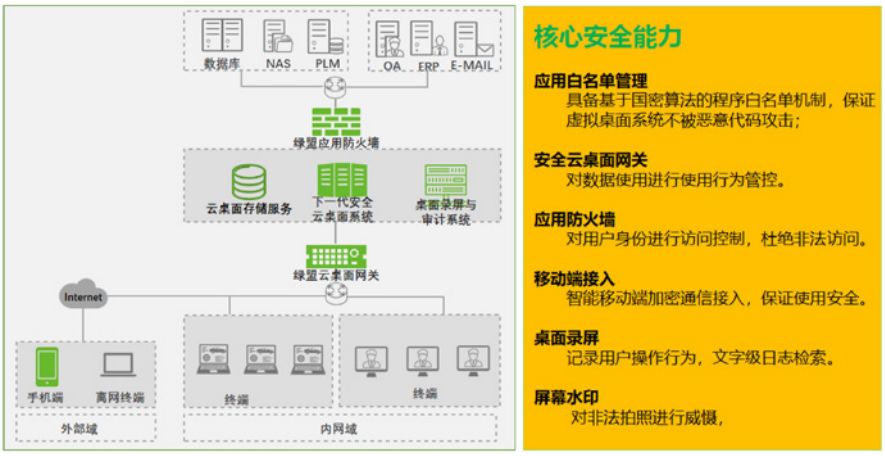


3. 隔离网络安全防护指南

隔离网络是通过进一步的权限细分，应用管控，技术隔离等方式，进一步隔离互联网与内部网络，可以认为是外网与内网的缓冲带，对于其主要风险防护及安全运营有以下建议：

◆ 内外网有效隔离风险防护建议：

1、大型企业及政府/风险等级非常高场景：可以采用“云桌面+堡垒机”的安全接入方案，对于一般全部人员均可以采用云桌面方式，这杨可以对VPN接入的客户端做进一步的隔离，所有数据无法带出云桌面环境，无法拷贝到接入人员本地，尽可能保证数据的安全同时拥有较好的易用性及体验；同时，考虑到远程运维的特殊性，可以考虑进一步使用“云桌面+堡垒机”方式进一步限制远程运维及特殊情况的下的使用场景。



2、中型企业及政府/风险等级高场景：可以考虑堡垒机方式进行远程办公的进一步隔离，防止黑客入侵及内部人员滥用。

3、小微企业/风险等级一般场景：可以针对某些特定场景使用堡垒机方式接入，如运维等需要记录整个操作过程的场景，并做好相关日志审计工作。

◆ 数据泄露风险防护建议：在相关设施不具备数据安全防控能力的情况下，可以考虑在云桌面或者终端安装主机版数据防泄密系统（DLP），尤其需要考虑的是云桌面不具备屏幕水印功能，客户数据泄露是通过拍照屏幕完成的。

◆ 安全运营建议：

1、对云桌面、堡垒机日志进行定期审计，发现可疑行为进行阻断或者进一步追查，包括异常的软件安装，批量数据查看及下载，高危操作如update、

Delete及集中频繁登陆等行为，如果有必要，可以翻看对应时间的录屏操作；

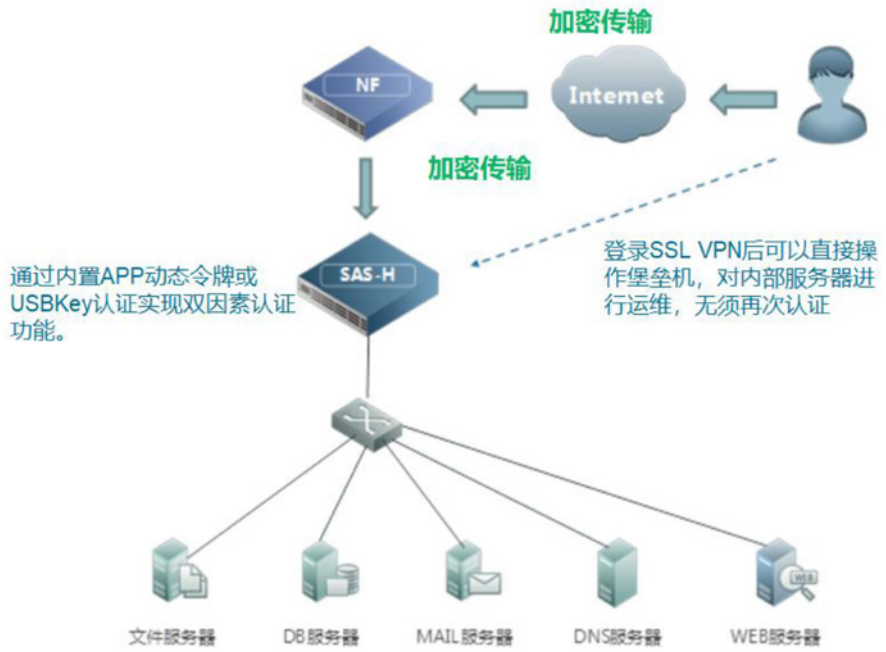
2、由于属于隔离网络，不可避免的需要进行文件上传操作，无论是云桌面、堡垒机都需要支持其上传功能，而其可能带来新的风险，可以对文件上传进行密切关注，限制上传文件类型，并对上传文件进行杀毒及沙箱检测，防止恶意脚本及病毒的上传；

3、建议梳理云桌面及堡垒机的安全功能，包括但不限于应用白名单管理、桌面录屏、屏幕水印、数据操作留痕及数据防泄密等功能，如果有缺失，可以考虑使用其他软件或者硬件进行补充，防止由于功能缺失造成安全风险；

4、在前期梳理相关人员使用场景前提下，进一步梳理云桌面的应用软件，对于不必要的软件进行清理，对于运维人员及相关高级权限的云桌面主机环境应进行访问控制，限制其的登陆权限，防止由于权限过大造成的风险；

5、同时，对堡垒机内部高危操作进行限制，防止黑客或内部人员的不当行为造成系统破坏或故障，并防止数据大规模泄露；

6、可以考虑VPN与堡垒机的联动方案，堡垒机内已经内置了OTP令牌实现双因素认证，通过联动方案实现双因素认证和单点登陆的基本功能。

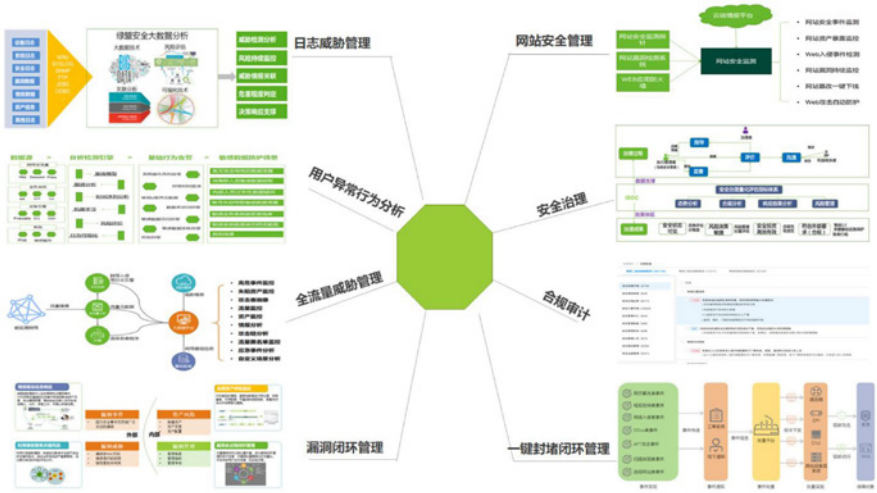


4. 内部网络安全防护指南

内部网络是防御的重中之重，可能存在少数系统以前为纯内部系统，从未在接入外部网络的情况，由于其的特殊性，可能以前并未有完整的防御体系和监控手段，所以对于其主要风险防护及安全运营有以下建议：

◆ 传统安全风险防护建议：

1、大型企业及政府/风险等级非常高场景：可以结合已有的安全设备、安全平台进行进一步整合与分析，建立智能安全运营平台（iSOC），利用大数据、人工智能等先进技术进行关联分析，进一步进行风险分析及阻断，由被动防御变为主动运营。



2、中型企业及政府/风险等级高场景：可以结合已有的安全设备包括防火墙、入侵防御/检测设备（IDS/IPS）、WEB应用防火墙（WAF）、终端入侵与响

应系统（EDR）、对内部系统形成防御，同时结合全流量威胁管理或者日志威胁管理功能，对网络流量日志及安全日志进行集中分析，并部署威胁分析系统（TAC）进行沙箱检测，主动发现潜在的恶意威胁，进行及时处置。

3、小微企业/风险等级一般场景：可以基于现有阻断类设备如防火墙、入侵防御设备（IPS）、WEB应用防火墙（WAF）等进行精细化策略梳理，进而通过自动化阻断来弥补人少事多的局面，同时可以考虑结合日志审计系统（LAS）及网络审计系统（SAS）作为事后追查的补充，形成安全闭环。

◆ 人员行为风险防护建议：通过安全意识培训及行为审计，定期对人员行为风险做出警示，同时结合用户行为分析等技术防御手段，有效提高人员行为风险防控能力。

◆ 安全运营建议：

1、传统安全的问题在内部网络都会遇到，通过设备的有效防御与管理制度的有机结合，适时的监测和审计是必须的。通过不断的内部监测和审计，不断发现内部潜在的安全问题，经过持续改进，不断提高企业自主安全运营能力；

2、基础的访问控制策略，基于使用场景的安全策略梳理，可以进一步加强内部安全防御能力，提高整个体系的安全防御效率；

3、对于内部网络有互联网连接的，建议在保证业务安全的前提下，在互联网出口防火墙设置阻断内部主动外联的安全策略，进而阻止木马或者恶意程序主动外联，造成内部的进一步沦陷及数据泄露；

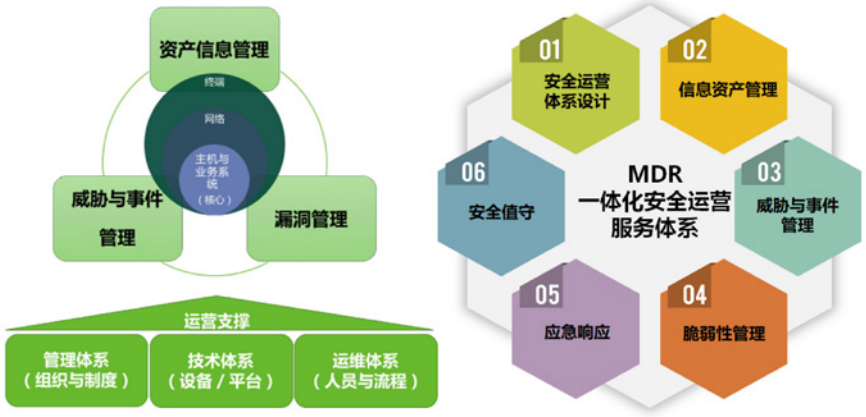
4、有效利用设备的联动功能可以起到事半功倍的效果，如根据业务场景配置堡垒机与入侵检测（IDS）联动——非来自堡垒机的运维操作即进行告警、威胁分析系统（TAC）与入侵防御（IPS）联动——检测到未知威胁自动化阻断等，都会是安全防御工作效率进一步提高；

5、基于大数据、人工智能等新技术的智能安全运营平台（iSOC）可以进一步为安全运营工作赋能，通过对日志、流量、行为等的关联分析，进一步梳理安全策略，最终完成安全编排和自动化响应，提升整个组织的安全能力。

5. 总结

远程办公可以更好的控制和防范疫情传播，减少因为集中办公带来的人员聚集，降低员工上下班出行过程中的风险，但也带来了新的信息安全风险。

这些信息安全风险核心其实是防范“人”的风险，各种安全防护设备固然重要，但是只有通过不断地提升安全运营能力，才能真正提升整个组织的安全能力，实现 “动态感知、智能监控、主动响应、全景可视”的安全目标。



本文通过对远程办公传输路径的风险分析，分层次的提出不同的安全防护指南及解决方案，希望从“基础运营保障、资产安全管理、威胁风险检测控制、脆弱性检测控制、安全风险通报处置、安全风险验证度量、安全检查与风险防范”形成企业安全运营全生命周期的管理闭环，提供“威胁预警、协同对抗、可管可控、智能防御”的安全运营保障能力，打赢这场战“疫”！

从常态化演练看安全建设

金融事业部　吴雪晴

安全形势背景

2017年6月1日，网络安全法正式发布；此后两年中，等保2.0、公安151号令、个人信息保护技术、无线安全、支付安全等相继发布通告及技术要求，同时，全国各地的攻防演练和攻防竞赛也愈发频繁，安全人才的培养和缺口也到达空前热度。社会全行业的安全意识被动提升，安全事件趋于频繁，各行业监管机构均收紧监管要求，敦促各行业进行安全自查。

防守方得分解读

2019年上半年进行的某安全演练，更是各行业信息安全人员的重要保障时期。通过实际的攻击对抗，使各防守方更清晰了安全工作职责、重点以及应急流程等。针对安全建设较为成熟的企业，实际演练，使他们精进了安全工作流程、优化了安全管理制度、弥补了安全防护缺漏、新增了安全防护手段；针对安全建设相对薄弱的企业，则直接提升了他们的安全意识、了解了自身跟标准安全防护的差距，明确了安全建设规划的方向。

从防守方的得分规则来看，一共分了5大方向：发现类、消除类、应急处置类、追踪溯源类、演习总结类。此5个方向的要求，与安全运营工作完全契合，做到针对安全事件的完整闭环。

发现类，即需要及时发现安全事件，包括但不限于：webshell木马、异常账号、恶意邮件、网络攻击进入等；此能力要求防守方具有相关安全检测设备进行流量检测和事件发现。

消除类，即针对发现的安全事件需做到及时处置，包括但不限于：清除webshell木马、处置异常账号、删除恶意邮件等；此能力要求防守方具有相应安全人才及产品可以及时处置安全事件。

应急处置类，即针对紧急事件能做到实时响应，并能提供有效信息。此能力要求防守方具有完善的应急流程和应急组织架构。

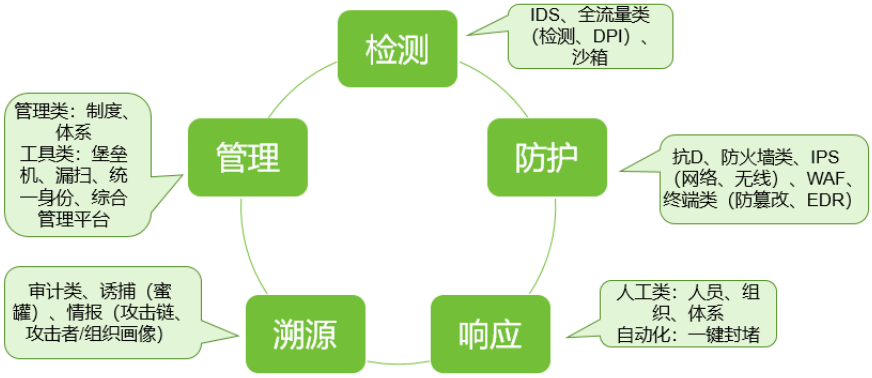
追踪溯源类，即针对安全事件可以溯源分析事件攻击源，定位攻击者及攻击组织画像。此能力要求防守方具有成熟情报体系和第三方安全厂商支持体系。

演习总结类，即针对整个演习过程进行总结，包括防守策略、安全事件分析、安全应急流程等，以提升整网安全防护能力。

基于以上5类能力的分析，可以看出，实际安全能力就是针对安全事件做到可感、可防、可知、可视和可管理的闭环。

安全能力应标

针对以上要求的5大类能力，在日常安全运维工作中，可对应到以下5个安全工作方向：安全检测、安全防护、安全响应、安全溯源及安全管理。



针对各工作可展开方式，以下侧重安全产品的推荐。

安全检测类设备（旁路部署），包括但不限于：IDS、全流量检测类设备、DPI类设备、高级威胁沙箱类设备、数据检测类设备；

安全防护类设备（逻辑串联部署），包括但不限于：抗D、防火墙类（下一代防火墙、数据库防火墙）、IPS、WAF、终端类（防篡改、EDR）；

安全响应侧重流程和组织制度，主流响应产品主要为一键封堵类自动化处置系统；

安全溯源类设备，包括但不限于：审计类设备（日志审计、数据库审计、网络审计）、诱捕类设备（蜜罐、蜜网）、情报平台；

安全管理主要通过相应制度及管理体系达成，主要辅助管理平台包括但不限于：堡垒机、漏洞扫描、统一身份认证、综合管理平台。

总结

安全防护能力，是通过产品、平台、服务和自有安全人员的共同努力构建的，在逐步完善安全产品的覆盖后，应加强安全人才和安全管理的体系建设，以构建完整的安全运营体系。

浅析 5G 网络安全需求

金融事业部　郁海泉

一、引言

移动通信从20世纪80年代诞生后经过三十几年的飞速发展，目前移动通信已经成为连接人类社会的基础信息网络，也是最为普及的信息通信技术。5G作为新一代移动通信技术发展的方向，在提升用户业务体验的基础上，也带来新的应用以及新的商业模式。但同时，5G的发展也面临着许多不可避免的挑战。

二、发展

2013年2月，IMT-2020(5G)推进组正式成立。推进组是聚合中国产学研用力量，推动中国第五代移动通信技术研究和开展国际交流与合作的主要平台。

2016年3月，工信部表示：5G是新一代移动通信技术发展的主要方向。在2016年我国已经和国际5G标准同步，进行了5G标准技术研究。

2017年 Q4，我国5G技术试验第三阶段正式启动。

2018年，5G试商用正式启动。

2019年10月31日，工信部与三大运营商举行5G商用启动仪式。中国移动、中国电信、中国联通正式公布5G套餐，这一仪式说明中国已正式进入5G商用时代。

三、新的挑战

3.1 业务场景

随着移动互联网和物联网业务的快速发展，如何满足人们日常生活中多样化的业务需求？如何实现各行业领域，与金融服务、工业设施、医疗仪器等等行业实现真正的‘万物互联’？为应对以上需求，目前5G业务大致分为3个场景：

- eMBB（增强移动宽带）
  eMBB聚焦对宽带有极高需求的业务，例如高清视频、VR（虚拟现实）、AR（增强现实）等。
- mMTC（海量机器类通信）
  mMTC覆盖对于连接密度要求较高的场景，例如智慧城市、智慧农业等。
- uRLLC（超可靠低时延通信）
  uRLLC聚焦对时延机极其敏感的业务，例如自动驾驶/辅助驾驶、远程控制等。

3.2 技术实现

为提高系统的灵活性和效率，5G网络架构引入了新的IT技术，例如软件定义网络SDN（软件定义网络）和NFV（网络功能虚拟化）、MEC（多接入边缘计算）、网络切片等。

5G网络通过引入虚拟化技术实现了软硬件解耦，即通过NFV（网络功能虚拟化）使得部分功能网元以虚拟功能网元的形式部署在云化的硬件基础设施之上，而同时也改变了传统网络硬件安全隔离的现状，需要保证5G业务在NFV环境下能够得到安全保证；另外，5G网络种通过引入SDN技术，实现了更好的资源配置，而同时也改变了物理架构的安全现状，需要保证虚拟SDN控制网元和转发节点的安全隔离和管理。

为了更好支持上述提及的3个业务场景，5G网络将建立网络切片，给不同场景的业务提供差异化的安全服务和安全服务级别，与此同时网络切片技术又带来了新的挑战，如各切片之间的安全。

3.3 安全保驾护航

根据5G安全设计原则，将5G网络架构分为如下八个安全域：

- 网络接入安全

  保障用户接入网络的数据安全。

- 网络域安全

  保障网元之间信令和用户数据的安全交换。

- 首次认证和密钥管理

  体现统一的认证框架，包括认证和密钥管理等各种机制。

- 二次认证和密钥管理

  用户设备与外部数据网络之间的业务认证以及相关密钥管理。

- 安全能力开放

  体现5G网元与外部业务提供方的安全能力开放，并能实现用户的按需保护。

- 应用安全

  保证用户和业务提供方之间的安全通信。

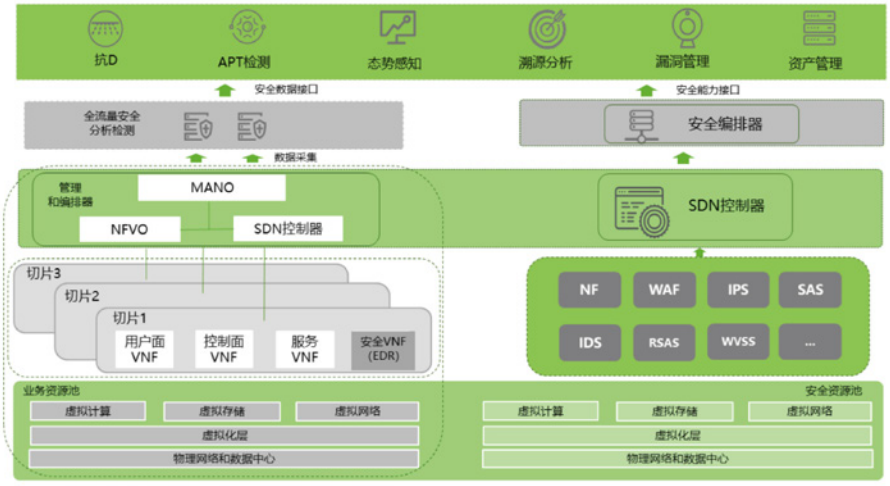
- 切片安全

  实现切片的安全保护，概括为：用户设备和切片间的安全、切片内网络功能和切片外网络功能间的安全、切片内网络功能间安全。

◆ 安全可视化和可配置

用户可以感知安全特性是否实现，且这类安全特性是否可以保障业务的安全使用和提供。

绿盟科技持续关注5G等新技术的发展，对5G网络架构、技术、各应用场景所面临的安全挑战有深入的研究，对于5G时代所面临的安全威胁构建了基于SDN/NFV架构的满足5G网络切片灵活、弹性的安全防护架构，如下：



为了解决5G网络中存在的这些安全问题，绿盟科技可提供通过部署安全服务链的方式来实现有效的安全防护。安全服务链按照一定的顺序串接各类虚拟化（物理）安全设备，对5G网络切片进行安全防护。

通过SDN/NFV等技术实现对需要防护的流量灵活调度、实现对所需防护能力的灵活管理和灵活编排、实现对5G网络安全检测和防护感知。

参考文献

IMT-2020（5G）推进组：5G网络安全需求与架构
IMT-2020（5G）推进组：我国5G最新研发与推进情况
绿盟科技研究通讯：解析5G安全（一）-5G网络架构
绿盟科技：绿盟科技入选2019 5G创新企业，为5G商用保驾护航

欧洲名校遭黑客勒索付了 30 个比特币赎金

摘　要：北京时间6 日消息，马斯特里赫特大学周三披露，去年12 月24 日曾遭遇黑客袭击，被迫支付了30 个比特币的赎金，当时价值20 万欧元，以解除对其IT系统，包括电子邮件和电脑的阻塞。

关键词：标签（欧洲名校、黑客勒索、比特币），技术问题（安全事件）。

内　容：北京时间6 日消息，马斯特里赫特大学周三披露，去年12 月24 日曾遭遇黑客袭击，被迫支付了30 个比特币的赎金，当时价值20 万欧元，以解除对其IT 系统，包括电子邮件和电脑的阻塞。

此类黑客攻击近年来已经司空见惯，2019 年多个公司、医院和机场遭到攻击后，保险公司将网络安全保费最高提高了25%。

马斯特里赫特大学副校长尼克·博斯（Nick Bos）说，校方在考虑了替代方案后决定支付赎金，以避免从零开始重建整个IT 系统的麻烦。

他说：“这对学生、科学家、工作人员的工作以及机构的连续性造成的损害几乎无法想象。”

博斯在周三的一次新闻发布会上透露了该大学对此次黑客攻击已知的情况，包括一个月前一名工作人员点击了一封网络钓鱼邮件，导致了最初的入侵。

网络安全公司Fox-IT 帮助这所大学恢复并分析了发生的事情，确定黑客是臭名昭著的TA505。

信息来源：https://finance.sina.com.cn/stock/usstock/c/2020-02-06/doc-iimxyqvz0632688.shtml

印度 APT 组织趁火打劫对我国医疗机构发起定向攻击！丧尽天良！

摘　要：在全国人民万众一心抗击疫情之时，近日捕获了一例利用新冠肺炎疫情相关题材投递的攻击案例，攻击者利用肺炎疫情相关题材作为诱饵文档，对抗击疫情的医疗工作领域发动APT攻击。

关键词：标签（印度APT、医疗机构、肺炎疫情），技术问题（安全事件）。

内　容：疫情亦网情，新冠病毒之后网络空间成疫情战役的又一重要战场。

就在全国人民万众一心抗击疫情之时，近日，360 安全大脑捕获了一例利用新冠肺炎疫情相关题材投递的攻击案例，攻击者利用肺炎疫情相关题材作为诱饵文档，对抗击疫情的医疗工作领域发动APT 攻击。

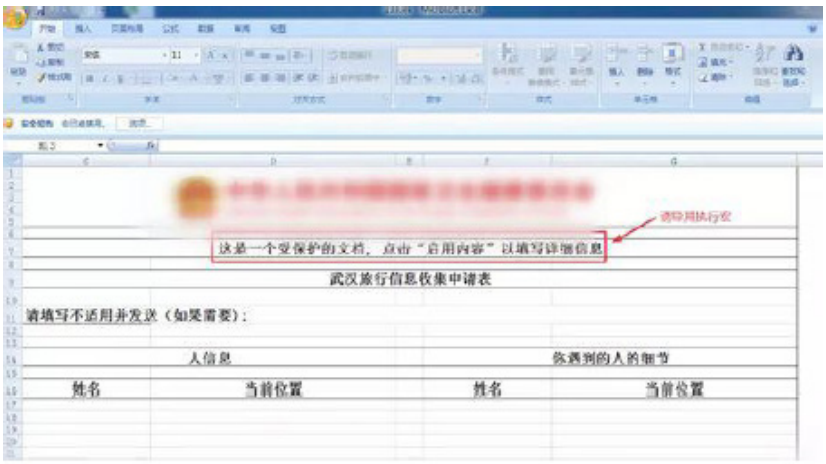
在进一步追踪溯源中，我们发现这起APT 组织隶属于印度黑客组织。抗疫攻坚难题当前，印度APT 组织竟公然瞄准我国医疗机构发动攻击！借势搅局、趁火打劫，此举不仅令人愤慨至极，简直是丧尽天良！

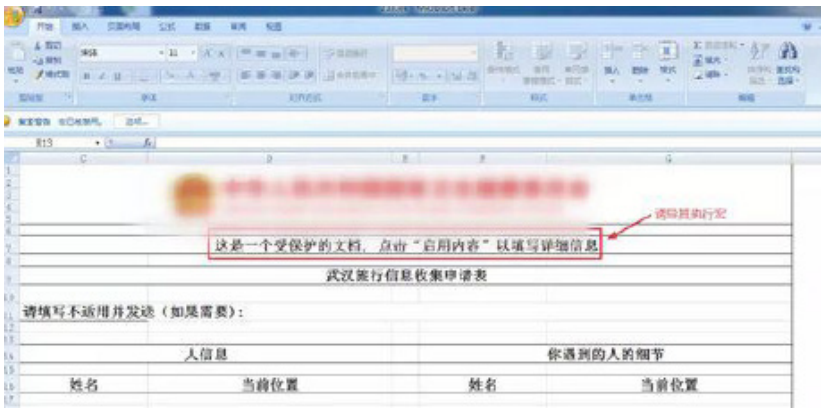
带着满腔的愤怒，我们进一步讲述关于此次攻击的重磅详情！

首先：是谁在趁火打劫，对我国痛下毒手？

在揭开幕后真凶的神秘面纱前，我们先简单了解下此次攻击者的攻击“路数”。

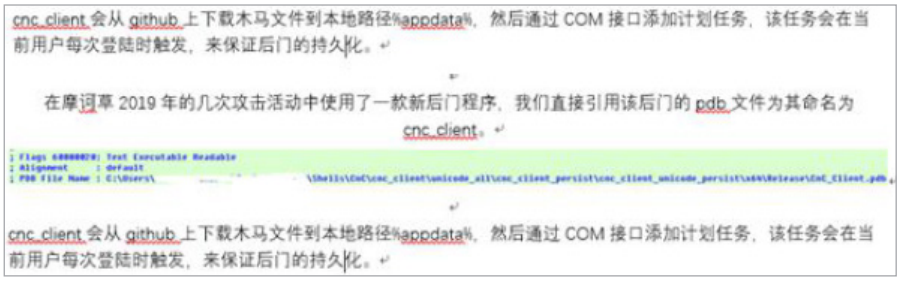
该攻击组织使用采用鱼叉式钓鱼攻击方式，通过邮件进行投递。可恨至极的是，它竟公然利用当前肺炎疫情等相关题材作为诱饵文档，部分相关诱饵文档如：武汉旅行信息收集申请表.xlsm，进而通过相关提示诱导受害者执行宏命令。





简单说，攻击者其将关键数据存在worksheet 里，worksheet 被加密，宏代码里面使用key 去解密然后取数据。然而其用于解密数据的Key 为：nhc_gover，而nhc正是中华人民共和国国家卫生健康委员会的英文缩写。

这里一旦宏命令被执行，攻击者就能访问hxxp://45.xxx.xxx.xx/window.sct，并使用scrobj.dll 远程执行Sct 文件，这是一种利用INF Script 下载执行脚本的技术。然而，此处我们想强调的是，此次攻击所使用的后门程序与之前360 安全大脑在南亚地区APT 活动总结中已披露的已知的印度组织专属后门cnc_client 相似，通过进一步对二进制代码进行对比分析，其通讯格式功能等与cnc_client 后门完全一致。可以确定，攻击者来源于印度的APT 组织！



值得注意的是，该印度APT 组织的攻击目标主要为：中国、巴基斯坦等亚洲地区国家进行网络间谍活动，其中以窃取敏感信息为主。而且在对中国地区的攻击中，主要针对政府机构、科研教育领域进行攻击，尤其以科研教育领域为主。

其次：谁又该提高警惕，免遭其迫害？

在明确了是谁在打我们的时候，又一个重要问题迎来而来，谁是此次攻击的受害者？

不言而喻，当攻击者精心利用新冠肺炎疫情相关题材，作为诱饵文档，进行鱼叉式攻击时，医疗机构、医疗工作领域无疑成为此次攻击的最大受害者。

别有用心国家级APT 组织的搅局，让这场本就步履维艰的疫情之战，更加艰

难。一旦其“攻击阴谋”得逞，轻则丢失数据、引发计算机故障，重则影响各地疫情防控工作的有序推进，危及个人乃至企业政府等各机构的网路安全。尤其面对这等有着国家级背景的APT 组织的攻击，后果简直不堪设想。

最后：攻击者的定向攻击目的，或许更值得深思？

中国有句古话，人生有三不笑：不笑天灾，不笑人祸，不笑疾病。

在重大灾难疫情面前，国家、企业、个人，我们尽我们一切所能做到的，支援武汉，支援前线，几乎所有工作者都在不眠不休的与时间赛跑、与病毒赛跑，在努力打赢这场疫情防御之战。同时，抗击疫情关键时刻，我们还收到来自他国的支持，近日，我国外交部发言人华春莹一口气向11 国致谢。

就是在国内外友人守望相助时，为什么印度APT 组织却如此丧尽天良的对我国医疗机构发动定向攻击？

这里我们不妨有个大胆的猜测：

第一，它们为了获取最新最前沿的医疗新技术。这与该印度APT 组织的攻击重点一直在科研教育领域有着莫大关系；

第二，它们为了进一步截取医疗设备数据。为打赢这场异常艰难的疫情之战，我国投入了重大的人力、物力、财力资源，其中尤其在医疗设备上更是重点，所以该组织此次发动攻击，能进一步截取我国更多的医疗设备数据信息；

第三，扰乱中国的稳定，制造更多的恐怖。疫情面前，不仅是一场与生物病毒的战役，更是一场民心之战，只有民心定了，才能保证社会的稳定。而该组织在此次发动攻击，无疑给疫情制造了更多的恐慌，恐吓之中，进行扰乱社会的稳定。

但无论是哪种猜测，它在此次时刻发动攻击，都将令本就不易的疫情攻坚战更加艰难，但我们更相信我们强大的祖国，相信奋战在任何前线的工作人员，不仅是卫士医疗团队、人民子弟兵，还有那些保证我们网络安全的勇士们，我们相信人定胜天！我们一定能打赢这场疫情之战，也一定能守护好网络空间这片净土！

加油，中国！

信息来源：https://mp.weixin.qq.com/s/kLZUf44WmeS_Qnc90fWKNA

网络诈骗横行英国金融业知名对冲基金的网站被克隆

摘　要：伦敦一些顶级对冲基金和资产管理公司成为诈骗网站的目标，这些诈骗网站会复制知名对冲基金和资管公司的名字和网站，制作假网站，试图从毫无戒心的投资者中骗钱。英国主要金融监管机构FCA 发出的大量警告（今年迄今大约每天一次），突显出该行业对虚假网站的担忧。

关键词：标签（网络诈骗、对冲基金、网站克隆），技术问题（安全事件）。

内　容：伦敦一些顶级对冲基金和资产管理公司成为诈骗网站的目标，这些诈骗网站会复制知名对冲基金和资管公司的名字和网站，制作假网站，试图从毫无戒心的投资者中骗钱。英国主要金融监管机构FCA 发出的大量警告（今年迄今大约每天一次），突显出该行业对虚假网站的担忧。

尽管到目前为止，已知上当受骗的人寥寥无几。但随着骗子变得越来越大胆，两家颇具知名度得资管公司艾尔格布里斯（Algebris）和元盛资产管理（Winton Group）已成为骗子们得目标。

该监管机构警告称，诈骗者通常使用真实公司的名称，制作一个与原网站设计类似的网站。该机构警告称，今年1 月和2 月，意大利投资者戴维-塞拉（Davide Serra）创建的Algebris UK 和英国亿万富翁戴维-哈丁（David Harding）创建的Winton Group 可能会被克隆网站。这些案件曝光之际，英国政府周三表示，可能会任命电信监管机构英国通信办公室（Ofcom）来监管这个行业。英国政府正在考虑出台新的立法，以打击流氓网络运营商。

据一位知情人士透露，Winton Group 在wintonfinance.com 网站成立后向FCA投诉。

在另一起事件中，一段被描述为Winton 创始人哈丁与Bitsmax 的访谈视频于12月26 日发布在视频网站上，发布者是一个以Bitsmax 为名义注册的账户。Bitsmax在其网站上自称是一家英国认证的加密货币投资平台。这位知情人士说，这段视频实际上是哈丁在一次投资会议上的讲话。这段视频一直在网上流传，直到周一，谷歌(1518.27, 9.48, 0.63%)的一名发言人表示，该视频已被删除。接近温顿的消息人士称，该公司此前曾花费数周时间试图删除该视频。

FCA 在周二发布了针对Bitsmax 的警告。2 月3 日，Winton 在社交媒体上发布了一个更笼统的警告，随后该公司在2 月5 日通过其网站向客户发布了一个警告，称Bitsmax 与公司及其创始人存在虚假关联。

到目前为止，FCA 在今年已经发布了40 个关于克隆站点的警告，而去年是365个，2018 年是303 个，2017 年是111 个。该机构上月发出警告的公司包括一些未经授权的公司，它们自称与Natixis 投资管理公司、英杰华投资者全球服务公司（Aviva Investors Global Services）和Redhedge 资产管理公司（Redhedge Asset Management）有关联。

英杰华的一位发言人表示：“在金融服务行业，克隆网站和其它网络诈骗越来越普遍。”在英杰华的案例中，这位发言人说，一个自称为www.avibonds.com 的克隆网站使用了英杰华投资者真实网站的背景。

英杰华（Aviva）和Redhedge 表示，没有客户或个人损失过钱，而法国外贸银行（Natixis）在12 月10 日（FCA 发出警告前28 天）在其网站上发布警告时表示，“公众可能是受害者”。

Redhedge 首席执行官兼首席信息官安德烈-西米纳拉（Andrea Seminara）表示：“我们会定期检查这样的克隆公司，并在适当的时候与监管机构保持持续对话。”

这家资产管理公司的首席运营官埃洛伊丝-利普金（Eloise Lipkin）表示，FCA在他们投诉后48 小时内就对该公司的Redhedge 投资发出了警告。

信息来源：https://www.cnbeta.com/articles/tech/942855.htm

美国男子于暗网上运行非法操作涉嫌洗钱 3 亿美元比特币被捕

摘　要：据外媒报道，近日美国当局逮捕了一名36 岁俄亥俄州男子拉里·哈蒙，并指控其在暗网上运行“比特币混合器”服务，该服务器帮助犯罪分子掩盖了约3亿美元的比特币交易活动。

关键词：标签（暗网、涉嫌洗钱、比特币），技术问题（安全事件）。

内　容：据了解，比特币区块链是一个公共数据库。在许多情况下，用户购买新的比特币基金，有时会链接到信用卡、银行账户或PayPal 账户。与此同时，“Helix”在此次事件中充当了比特币混合器（Bitcoin Tumbler）的一种服务，该服务是从用户那里收取资金, 将金额分割成很多个小部分,并使用数千笔交易，将原始资金发送并重新组装到新的比特币地址当中，通过这一系列的操作将原始资金隐藏在微交易中。

美国国税局刑事调查主管唐·福特近日在司法部的一份新闻稿中表示，此次哈蒙行动的唯一目的是向执法部门隐瞒暗网上的犯罪交易。此次调查中，调查人员再次扮演了犯罪破坏者的角色，从一个触角到另一个触角，拆解了它们之间相互关联的网络以进行调查。

根据美国司法部的文件，哈蒙把“Helix”作为一个附属于他的主要服务Grams的二级项目。据悉，Helix 公司为潜在买家提供了一种在购买产品时隐藏身份的方式，它允许用户搜索毒品，并在他们所在的地区找到最便宜的毒品以进行交易。

美国司法部表示，自2014 年以来，哈蒙一直在运营Helix，它对所有的“Helix”滚转操作收取2.5%的费用，并帮助洗钱超过35 万枚比特币，交易时价值约3 亿美元，如今价值35 亿美元。调查人员表示，随着服务的发展，哈蒙也与其他黑暗网络服务合作。根据起诉书，哈蒙与当时最大的非法产品暗网市场AlphaBay 联手，AlphaBay负责向其用户推荐Helix 作为一个安全的比特币交易选项。

根据报道，此次调查是美国司法部针对比特币非法操作提出的第一个案例。目前美国司法部表示，除了想让哈蒙在监狱里度过漫长的几年，美国司法部还将寻求没收其三处房产，他们认为这三处房产是犯罪嫌疑人用通过Helix 获得的非法资金购买的。

信息来源：https://mp.weixin.qq.com/s/cOPastH8bu3YyJEKJFU-1Q

NSFOCUS

漏洞聚焦

微软发布 2 月补丁修复 100 个安全问题
安全威胁通告

发布时间：2020 年 2 月 12 日

综述

微软于周二发布了2月安全更新补丁，修复了100个从简单的欺骗攻击到远程执行代码的安全问题，产品涉及Adobe Flash Player、Internet Explorer、Microsoft Edge、Microsoft Exchange Server、Microsoft Graphics Component、Microsoft Malware Protection Engine、Microsoft Office、Microsoft Office SharePoint、Microsoft Scripting Engine、Microsoft Windows、Microsoft Windows Search Component、Remote Desktop Client、Secure Boot、SQL Server、Windows Authentication Methods、Windows COM、Windows Hyper-V、Windows Installer、Windows Kernel、Windows Kernel-Mode Drivers、Windows Media、Windows NDIS、Windows RDP、Windows Shell以及Windows Update Stack。

本月微软月度更新修复的漏洞中，严重程度为关键（Critical）的漏洞共有12个，重要（Important）漏洞有 88个。

Critical漏洞概述

以下为此次更新中包含的12个Critical级别漏洞。

Microsoft Scripting Engine

- CVE-2020-0673、CVE-2020-0674

微软曾于1月17日发布过一个有关Internet Explorer漏洞（CVE-2020-0674）的安全公告，表示该漏洞发现在野外被利用的情况，当时公告仅包括可应用的变通办法和缓解措施，本次更新中新增了针对该漏洞的补丁。

脚本引擎在处理Internet Explorer中内存对象的方式中存在以上远程执行代码漏洞。

成功利用漏洞的攻击者可以获得与当前用户相同的用户权限。如果当前用户使用管理用户权限登录，则攻击者可以控制受影响的系统。然后，可能会安装程序。查看，更改或删除数据或创建具有完全用户权限的新帐户。

在基于Web的攻击场景中，攻击者可能会搭建一个特制的网站，然后诱使用户访问该站点。不过攻击者无法强迫用户查看恶意内容。所以通常会通过电子邮件或即时消息的方式来诱导用户。此外，攻击者还可能在承载IE渲染引擎的应用程序或Microsoft Office文档中嵌入标记为“初始化安全”的ActiveX控件。

Internet Explorer 9、10、11 均受影响。

关于漏洞的更多详情及更新下载，请参考微软官方安全通告：

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0673

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0674

◆ CVE-2020-0710、CVE-2020-0711、CVE-2020-0712、CVE-2020-0713、CVE-2020-0767

ChakraCore脚本引擎在处理内存对象的方式中存在以上远程执行代码漏洞。成功利用漏洞的攻击者可以获得与当前用户相同的用户权限。

关于漏洞的更多详情及更新下载，请参考微软官方安全通告：

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0710

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0711

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0712

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0713

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0767

RDP

◆ CVE-2020-0681、CVE-2020-0734

这是 Windows远程桌面客户端中的两个远程代码执行漏洞。

成功利用此漏洞的攻击者可以在连接到恶意服务器的用户计算机上执行任意代码。然后，攻击者可能会安装程序。查看，更改或删除数据或创建具有完全用户权限的新帐户。

要利用此漏洞，攻击者需要控制服务器，然后诱使用户连接到该服务器。如果用户访问了恶意的服务器，则可以触发此漏洞。虽然攻击者无法强迫用户连接到恶意服务器，但他们可能会通过社工，DNS中毒或中间人（MITM）技术诱使用户进行连接。攻击者还可能破坏合法服务器，在其上托管恶意代码，然后等待用户连接。

关于漏洞的更多详情及更新下载，请参考微软官方安全通告：

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0681

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0734

Windows

◆ CVE-2020-0662

Windows处理内存对象的方式中存在一个远程执行代码漏洞。成功利用此漏洞的攻击者可以在目标系统上以提升的权限执行任意代码。

为了利用此漏洞，拥有域用户帐户的攻击者可以创建特制请求，从而使Windows执行具有提升权限的任意代码。

关于漏洞的更多详情及更新下载，请参考微软官方安全通告：

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0662

LNK

◆ CVE-2020-0729

Microsoft Windows中存在一个远程执行代码漏洞，如果处理了.LNK文件，

该漏洞可能允许远程执行代码。

成功利用此漏洞的攻击者可以获得与本地用户相同的权限。

攻击者可能向用户提供可移动驱动器或远程共享，其中包含恶意的.LNK文件和关联的恶意二进制文件。当用户在Windows资源管理器或任何其他解析.LNK文件的应用程序中打开此驱动器（或远程共享）时，恶意二进制文件将在目标系统上执行攻击者选择的代码。

关于漏洞的更多详情及更新下载，请参考微软官方安全通告：

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0729

Media Foundation

◆ CVE-2020-0738

Windows Media Foundation不正确地处理内存中的对象时，存在内存损坏漏洞。

成功利用此漏洞的攻击者可以安装程序，查看、更改或删除数据或创建具有完全用户权限的新帐户。

攻击者可以采用多种方式利用此漏洞，例如，说服用户打开特制文档，或说服用户访问恶意网页。

关于漏洞的更多详情及更新下载，请参考微软官方安全通告：

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0738

修复概况

本次更新的漏洞修复情况见下表：

产品	CVE 编号	CVE 标题	严重程度
Adobe Flash Player	ADV200003	February 2020 Adobe Flash 安全更新	Important
Internet Explorer	CVE-2020-0673	Scripting Engine 内存破坏漏洞	Critical
Internet Explorer	CVE-2020-0674	Scripting Engine 内存破坏漏洞	Critical

产品	CVE 编号	CVE 标题	严重程度
Microsoft Edge	CVE-2020-0663	Microsoft Edge 特权提升漏洞	Important
Microsoft Edge	CVE-2020-0706	Microsoft Browser 信息泄露漏洞	Important
Microsoft Exchange Server	CVE-2020-0688	Microsoft Exchange 内存破坏漏洞	Important
Microsoft Exchange Server	CVE-2020-0696	Microsoft Outlook 安全功能绕过漏洞	Important
Microsoft Exchange Server	CVE-2020-0692	Microsoft Exchange Server 特权提升漏洞	Important
Microsoft Graphics Component	CVE-2020-0745	Windows Graphics Component 特权提升漏洞	Important
Microsoft Graphics Component	CVE-2020-0746	Microsoft Graphics Components 信息泄露漏洞	Important
Microsoft Graphics Component	CVE-2020-0792	Windows Graphics Component 特权提升漏洞	Important
Microsoft Graphics Component	CVE-2020-0709	DirectX 特权提升漏洞	Important
Microsoft Graphics Component	CVE-2020-0714	DirectX 信息泄露漏洞	Important
Microsoft Graphics Component	CVE-2020-0715	Windows Graphics Component 特权提升漏洞	Important
Microsoft Graphics Component	CVE-2020-0744	Windows GDI 信息泄露漏洞	Important
Microsoft Malware Protection Engine	CVE-2020-0733	Windows Malicious Software Removal Tool 特权提升漏洞	Important
Microsoft Office	CVE-2020-0695	Microsoft Office Online Server 欺骗漏洞	Important
Microsoft Office	CVE-2020-0697	Microsoft Office Tampering Vulnerability	Important
Microsoft Office	CVE-2020-0759	Microsoft Excel 远程代码执行漏洞	Important
Microsoft Office SharePoint	CVE-2020-0693	Microsoft Office SharePoint XSS Vulnerability	Important
Microsoft Office SharePoint	CVE-2020-0694	Microsoft Office SharePoint XSS Vulnerability	Important
Microsoft Scripting Engine	CVE-2020-0767	Scripting Engine 内存破坏漏洞	Critical
Microsoft Scripting Engine	CVE-2020-0710	Scripting Engine 内存破坏漏洞	Critical
Microsoft Scripting Engine	CVE-2020-0711	Scripting Engine 内存破坏漏洞	Critical

产品	CVE 编号	CVE 标题	严重程度
Microsoft Scripting Engine	CVE-2020-0712	Scripting Engine 内存破坏漏洞	Critical
Microsoft Scripting Engine	CVE-2020-0713	Scripting Engine 内存破坏漏洞	Critical
Microsoft Windows	CVE-2020-0666	Windows Search Indexer 特权提升漏洞	Important
Microsoft Windows	CVE-2020-0667	Windows Search Indexer 特权提升漏洞	Important
Microsoft Windows	CVE-2020-0668	Windows Kernel 特权提升漏洞	Important
Microsoft Windows	CVE-2020-0669	Windows Kernel 特权提升漏洞	Important
Microsoft Windows	CVE-2020-0670	Windows Kernel 特权提升漏洞	Important
Microsoft Windows	CVE-2020-0671	Windows Kernel 特权提升漏洞	Important
Microsoft Windows	CVE-2020-0672	Windows Kernel 特权提升漏洞	Important
Microsoft Windows	CVE-2020-0675	Windows Key Isolation Service 信息泄露漏洞	Important
Microsoft Windows	CVE-2020-0676	Windows Key Isolation Service 信息泄露漏洞	Important
Microsoft Windows	CVE-2020-0677	Windows Key Isolation Service 信息泄露漏洞	Important
Microsoft Windows	CVE-2020-0678	Windows Error Reporting Manager 特权提升漏洞	Important
Microsoft Windows	CVE-2020-0679	Windows Function Discovery Service 特权提升漏洞	Important
Microsoft Windows	CVE-2020-0680	Windows Function Discovery Service 特权提升漏洞	Important
Microsoft Windows	CVE-2020-0681	Remote Desktop Client 远程代码执行漏洞	Critical
Microsoft Windows	CVE-2020-0682	Windows Function Discovery Service 特权提升漏洞	Important
Microsoft Windows	CVE-2020-0685	Windows COM Server 特权提升漏洞	Important
Microsoft Windows	CVE-2020-0701	Windows Client License Service 特权提升漏洞	Important
Microsoft Windows	CVE-2020-0727	Connected User Experiences and Telemetry Service 特权提升漏洞	Important
Microsoft Windows	CVE-2020-0737	Windows 特权提升漏洞	Important

产品	CVE 编号	CVE 标题	严重程度
Microsoft Windows	CVE-2020-0739	Windows 特权提升漏洞	Important
Microsoft Windows	CVE-2020-0740	Connected Devices Platform Service 特权提升漏洞	Important
Microsoft Windows	CVE-2020-0741	Connected Devices Platform Service 特权提升漏洞	Important
Microsoft Windows	CVE-2020-0742	Connected Devices Platform Service 特权提升漏洞	Important
Microsoft Windows	CVE-2020-0743	Connected Devices Platform Service 特权提升漏洞	Important
Microsoft Windows	CVE-2020-0747	Windows Data Sharing Service 特权提升漏洞	Important
Microsoft Windows	CVE-2020-0748	Windows Key Isolation Service 信息泄露漏洞	Important
Microsoft Windows	CVE-2020-0753	Windows Error Reporting 特权提升漏洞	Important
Microsoft Windows	CVE-2020-0754	Windows Error Reporting 特权提升漏洞	Important
Microsoft Windows	CVE-2020-0755	Windows Key Isolation Service 信息泄露漏洞	Important
Microsoft Windows	CVE-2020-0756	Windows Key Isolation Service 信息泄露漏洞	Important
Microsoft Windows	CVE-2020-0757	Windows SSH 特权提升漏洞	Important
Microsoft Windows	CVE-2020-0657	Windows Common Log File System Driver 特权提升漏洞	Important
Microsoft Windows	CVE-2020-0658	Windows Common Log File System Driver 信息泄露漏洞	Important
Microsoft Windows	CVE-2020-0659	Windows Data Sharing Service 特权提升漏洞	Important
Microsoft Windows	CVE-2020-0698	Windows 信息泄露漏洞	Important
Microsoft Windows	CVE-2020-0703	Windows Backup Service 特权提升漏洞	Important
Microsoft Windows	CVE-2020-0704	Windows Wireless Network Manager 特权提升漏洞	Important
Microsoft Windows	CVE-2020-0732	DirectX 特权提升漏洞	Important
Microsoft Windows Search Component	CVE-2020-0735	Windows Search Indexer 特权提升漏洞	Important

产品	CVE 编号	CVE 标题	严重程度
Remote Desktop Client	CVE-2020-0734	Remote Desktop Client 远程代码执行漏洞	Critical
Secure Boot	CVE-2020-0689	Microsoft Secure Boot 安全功能绕过漏洞	Important
SQL Server	CVE-2020-0618	Microsoft SQL Server Reporting Services 远程代码执行漏洞	Important
Windows Authentication Methods	CVE-2020-0665	Active Directory 特权提升漏洞	Important
Windows COM	CVE-2020-0749	Connected Devices Platform Service 特权提升漏洞	Important
Windows COM	CVE-2020-0750	Connected Devices Platform Service 特权提升漏洞	Important
Windows COM	CVE-2020-0752	Windows Search Indexer 特权提升漏洞	Important
Windows Hyper-V	CVE-2020-0661	Windows Hyper-V 拒绝服务漏洞	Important
Windows Hyper-V	CVE-2020-0662	Windows 远程代码执行漏洞	Critical
Windows Hyper-V	CVE-2020-0751	Windows Hyper-V 拒绝服务漏洞	Important
Windows Installer	CVE-2020-0683	Windows Installer 特权提升漏洞	Important
Windows Installer	CVE-2020-0686	Windows Installer 特权提升漏洞	Important
Windows Installer	CVE-2020-0728	Windows Modules Installer Service 信息泄露漏洞	Important
Windows Kernel	CVE-2020-0736	Windows Kernel 信息泄露漏洞	Important
Windows Kernel	CVE-2020-0716	Win32k 信息泄露漏洞	Important
Windows Kernel	CVE-2020-0717	Win32k 信息泄露漏洞	Important
Windows Kernel	CVE-2020-0719	Win32k 特权提升漏洞	Important
Windows Kernel	CVE-2020-0720	Win32k 特权提升漏洞	Important
Windows Kernel	CVE-2020-0721	Win32k 特权提升漏洞	Important
Windows Kernel	CVE-2020-0722	Win32k 特权提升漏洞	Important
Windows Kernel	CVE-2020-0723	Win32k 特权提升漏洞	Important

产品	CVE 编号	CVE 标题	严重程度
Windows Kernel	CVE-2020-0724	Win32k 特权提升漏洞	Important
Windows Kernel	CVE-2020-0725	Win32k 特权提升漏洞	Important
Windows Kernel	CVE-2020-0726	Win32k 特权提升漏洞	Important
Windows Kernel	CVE-2020-0731	Win32k 特权提升漏洞	Important
Windows Kernel-Mode Drivers	CVE-2020-0691	Win32k 特权提升漏洞	Important
Windows Media	CVE-2020-0738	Media Foundation 内存破坏漏洞	Critical
Windows NDIS	CVE-2020-0705	Windows Network Driver Interface Specification (NDIS) 信息泄露漏洞	Important
Windows RDP	CVE-2020-0660	Windows Remote Desktop Protocol (RDP) 拒绝服务漏洞	Important
Windows Shell	CVE-2020-0655	Remote Desktop Services 远程代码执行漏洞	Important
Windows Shell	CVE-2020-0702	Surface Hub 安全功能绕过漏洞	Important
Windows Shell	CVE-2020-0729	LNK 远程代码执行漏洞	Critical
Windows Shell	CVE-2020-0730	Windows User Profile Service 特权提升漏洞	Important
Windows Shell	CVE-2020-0707	Windows IME 特权提升漏洞	Important
Windows Update Stack	CVE-2020-0708	Windows Imaging Library 远程代码执行漏洞	Important

修复建议

微软官方已经发布更新补丁，请及时进行补丁更新。

声明

Adobe 2 月安全更新安全威胁通告

发布时间：2020 年 2 月 12 日

综述

当地时间2月11日，Adobe官方发布了2月安全更新，修复了Adobe 多款产品的多个漏洞，包括Adobe Experience Manager、Adobe Digital Editions、Adobe Flash Playe、Adobe Acrobat and Reader以及Adobe Framemaker等。

官方通告地址：

https://helpx.adobe.com/security.html

漏洞概述：

Adobe Experience Manager

Adobe已发布Adobe Experience Manager 安全更新，修复了1个安全漏洞。

漏洞概括如下：

漏洞类别	漏洞影响	严重程度	CVE 编号
不受控制的资源消耗	拒绝服务	Important	CVE-2020-3741

关于漏洞的具体影响版本及修复情况，请参考Adobe官方安全通告：

https://helpx.adobe.com/security/products/experience-manager/apsb20-08.html

Adobe Digital Editions

Adobe已发布Adobe Digital Editions安全更新，修复了2个安全漏洞。

漏洞概括如下：

漏洞类别	漏洞影响	严重程度	CVE 编号
缓冲区错误	信息泄露	Important	CVE-2020-3759
命令注入	任意代码执行	Critical	CVE-2020-3760

关于漏洞的具体影响版本及修复情况，请参考Adobe官方安全通告：

https://helpx.adobe.com/security/products/Digital-Editions/apsb20-07.html

Adobe Flash Player

Adobe已发布Adobe Flash Player安全更新，修复了1个安全漏洞。

漏洞概括如下：

漏洞类别	漏洞影响	严重程度	CVE 编号
类型混淆	任意代码执行	Critical	CVE-2020-3757

关于漏洞的具体影响版本及修复情况，请参考Adobe官方安全通告：

https://helpx.adobe.com/security/products/flash-player/apsb20-06.html

Adobe Acrobat and Reader

Adobe已发布Adobe Acrobat and Reader安全更新，修复了17个安全漏洞。

漏洞概括如下：

漏洞类别	漏洞影响	严重程度	CVE 编号
越界读取	信息泄露	Important	CVE-2020-3744 CVE-2020-3747 CVE-2020-3755
堆溢出	任意代码执行	Critical	CVE-2020-3742
缓冲区错误	任意代码执行	Critical	CVE-2020-3752 CVE-2020-3754

漏洞类别	漏洞影响	严重程度	CVE 编号
UAF	任意代码执行	Critical	CVE-2020-3743 CVE-2020-3745 CVE-2020-3746 CVE-2020-3748 CVE-2020-3749 CVE-2020-3750 CVE-2020-3751
堆栈耗尽	内存泄露	Moderate	CVE-2020-3753 CVE-2020-3756
特权提升	任意文件系统写入	Critical	CVE-2020-3762 CVE-2020-3763

关于漏洞的具体影响版本及修复情况，请参考Adobe官方安全通告：
https://helpx.adobe.com/security/products/acrobat/apsb20-05.html

Adobe Framemaker

Adobe已发布Adobe Framemaker 安全更新，修复了21个安全漏洞。
漏洞概括如下：

漏洞类别	漏洞影响	严重程度	CVE 编号
缓冲区错误	任意代码执行	Critical	CVE-2020-3734
堆溢出	任意代码执行	Critical	CVE-2020-3731 CVE-2020-3735
内存损坏	任意代码执行	Critical	CVE-2020-3739 CVE-2020-3740
越界写入	任意代码执行	Critical	CVE-2020-3720 CVE-2020-3721 CVE-2020-3722 CVE-2020-3723 CVE-2020-3724 CVE-2020-3725

漏洞类别	漏洞影响	严重程度	CVE 编号
越界写入	任意代码执行	Critical	CVE-2020-3726 CVE-2020-3727 CVE-2020-3728 CVE-2020-3729 CVE-2020-3730 CVE-2020-3732 CVE-2020-3733 CVE-2020-3736 CVE-2020-3737 CVE-2020-3738

关于漏洞的具体影响版本及修复情况，请参考Adobe官方安全通告：

https://helpx.adobe.com/security/products/framemaker/apsb20-04.html

解决方案

Adobe官方已经发布新版本修复了上述漏洞，用户应及时升级进行防护。

详细信息及操作可参考各产品漏洞部分的官方通告链接。

微软 SQL Server Reporting Services 远程代码执行漏洞 (CVE-2020-0618) 安全威胁通告

发布时间：2020 年 2 月 17 日

综述

在上周发布的微软月度更新中，包含一个存在于SQL Server Reporting Services（SSRS）中的远程代码执行漏洞CVE-2020-0618。目前已存在针对该漏洞的 PoC，请相关用户尽快安装补丁进行防护。

SQL Server Reporting Services (SSRS)是微软基于服务器的报表生成软件，它是Microsoft SQL Server服务套件的一部分，通过Web界面进行管理，可用于准备和交付各种交互式报告。

SSRS应用中的功能允许经过身份验证的攻击者向受影响的Reporting Services实例提交精心构造的HTTP请求，利用应用中的反序列化问题在服务器上执行代码。

尽管只有授权用户才能访问该应用程序，但是最低权限（浏览器角色）足以利用此漏洞。

相关链接：https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0618

受影响产品版本

- ☐ Microsoft SQL Server 2012 Service Pack 4（QFE）
- ☐ Microsoft SQL Server 2014 Service Pack 3（CU）
- ☐ Microsoft SQL Server 2014 Service Pack 3（GDR）
- ☐ Microsoft SQL Server 2016 Service Pack 2 (CU)
- ☐ Microsoft SQL Server 2016 Service Pack 2 (GDR)

解决方案

由于攻击者可通过对请求数据包编码绕过Web应用防火墙的防护，强烈建议用户安装补丁进行修复。

微软官方已为受支持版本发布了针对该漏洞的安全补丁，请参阅微软官方通告下载安装。

产品	版本	更新编号
SQL Server 2016 Service Pack 2 (GDR) 安全更新	13.0.5026.0 - 13.0.5101.9	KB4532097
SQL Server 2016 Service Pack 2 CU11 安全更新	13.0.5149.0 - 13.0.5598.27	KB4535706
SQL Server 2014 Service Pack 3 (GDR) 安全更新	12.0.6024.0 - 12.0.6108.1	KB4532095

产品	版本	更新编号
SQL Server 2014 Service Pack 2 CU4 安全更新	12.0.6205.1 - 12.0.6329.1	KB4535288
SQL Server 2012 Service Pack 4 (QFE) 安全更新	111.0.7001.0 - 11.0.7462.6	KB4532098

同时，建议禁止匿名访问，确保只有经过身份验证的用户才能访问相关应用。如果怀疑服务器已经受到威胁，除安装相应补丁外，请及时更改服务器的账户口令，防止被攻击者利用。

官方通告：

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0618

声明

Cisco（思科）发现协议漏洞（CDP）安全威胁通告

发布时间：2020 年 2 月 7 日

综述

北京时间2月6日，思科（Cisco）官方修复了存在于CDP协议中的5个高危漏洞，该协议可允许思科设备在内网环境通过多播消息互相分享消息，主要影响IP电话和摄像头设备。

此次公开的5个漏洞均属于内存溢出漏洞，实际利用难度大，在特定条件下可造成远程代码执行。思科在漏洞公告中指出： Cisco发现协议是第2层协议。要利用此漏洞，攻击者必须与受影响的设备位于同一广播域中（第2层相邻）。

漏洞CVE：

- ☐ CVE-2020-3110
- ☐ CVE-2020-3111
- ☐ CVE-2020-3118
- ☐ CVE-2020-3119
- ☐ CVE-2020-3120

受影响的设备

Cisco FXOS Software, Cisco IP Camera Firmware, Cisco IP Phone Firmware, Cisco NX-OS Software, Cisco IOS-XR, and Cisco UCS Fabric Interconnects

不受影响的设备

Cisco IOS and Cisco IOS-XE Software, and firewalls such as the Cisco ASA, Cisco Firepower 1000 Series, and Cisco Firepower 2100 Series. (Though CVE-2020-3120 affects the Firepower 4100 Series and Firepower 9300 Security Appliances)

缓解措施

思科官方已经发布新版本修复了这些漏洞，请用户尽快升级进行防护。

详情参考思科官方通告指南：

https://community.cisco.com/t5/security-blogs/insights-about-multiple-vulnerabilities-in-cisco-discovery/ba-p/4023505

参考链接

https://www.helpnetsecurity.com/2020/02/05/cdpwn-vulnerabilities/

https://www.armis.com/cdpwn/#devices

https://community.cisco.com/t5/security-blogs/insights-about-multiple-vulnerabilities-in-cisco-discovery/ba-p/4023505

NSFOCUS

安全态势

暗网情报

分类	发现时间	暗网交易标题
金融	2020/02/02 22:38	19 年 8 月至 11 月某证券会员信息
金融	2020/02/02 14:20	218w 全国股民基民数据
金融	2020/02/03 02:30	沿海发达城市股民数据 10W
金融	2020/02/02 23:23	19 年 98000 条某银行信用卡用户数据详细信息

分类	发现时间	暗网交易标题
金融	2020-02-03 22:36	股民数据 10800 条 19 年某证券网点新开户数据
金融	2020-02-03 16:55	59w 某银行理财客户带手机号身份证地址等
金融	2020-02-03 23:26	12 万 8 某银行信用卡持卡人含申办时的所有信息
金融	2020-02-02 13:34	某银行企业通讯录
金融	2020-02-05 00:32	股民数据 98w7 某投资公司数据含姓名手机微信
金融	2020-02-05 01:19	8w8 浙江某投顾公司 19 年股民数据
金融	2020-02-05 16:40	某银行_千万富豪个人数据
金融	2020-02-06 13:26	某证券_股民数据 23 万
金融	2020-02-06 21:39	理财数据 10w 条某银行理财客户信息

分类	发现时间	暗网交易标题
互联网	2020-02-11 10:23	某社工库 120G 数据自动发货
非法枪械	2020-02-11 10:30	各种气枪 cad 图纸详细安装教程 37GB 自动发货
金融	2020-02-11 22:31	银行卡数据 1809 条各大行银行卡数据含卡号等
互联网	2020-02-13 00:39	某网站 335w 全国宝妈数据
金融	2020-02-13 16:08	2020 年第一批某证券短信拦截股民数据 38w
互联网	2020-02-13 17:12	最新 1 月某棋牌 99000 条数据
金融	2020-02-13 18:47	52794 条网赚兼职粉_短信劫持数据
互联网	2020-02-13 22:16	某女性购物平台_网购数据 16 万
金融	2020-02-13 22:20	今年全国高尔夫球_球会联盟会员信息 11 万

◆ 更多详细内容，可与绿盟科技商务人员联系或联系邮箱csc@nsfocus.com

热点资讯回顾

1. 雄迈产品漏洞

【概述】

近日，有国外安全研究员指出海思（HiSilicon）芯片中预留后门，事后多方研究员以及海思官方都澄清并表示该后门源于雄迈软件的设备，并非海思芯片。后门主要利用端口9530/tcp 侦听特殊命令，攻击者通过此端口开启telnet 服务，并利用默认的口令登录，从而控制设备。

【参考链接】

https://mp.weixin.qq.com/s/yMJWxJvtgeuzSfYTN6vn7Q

2. 思科修复CDP 协议漏洞

【概述】

北京时间2 月6 日，思科（Cisco）官方修复了存在于CDP 协议中的5 个高危漏洞，该协议可允许思科设备在内网环境通过多播消息互相分享消息，主要影响IP 电话和摄像头设备。此次公开的5 个漏洞均属于内存溢出漏洞，实际利用难度大，在特定条件下可造成远程代码执行。

【参考链接】

http://blog.nsfocus.net/cisco20200207/

3. 安卓蓝牙组件高危漏洞

【概述】

近日，谷歌发布2 月安卓安全补丁，其中修复了一个高危的蓝牙组件漏洞（CVE-2020-0022）。该漏洞无需用户的交互操作，在设备打开蓝牙时即可被攻击，攻击者成功利用该漏洞即可在目标系统上执行任意代码。同时研究人员还指出该漏洞可能被攻击者用来制作可以自主传播的蠕虫型漏洞。

【参考链接】

http://blog.nsfocus.net/cve-2020-0022/

4. MyCERT 警告APT40 开展的网络间谍活动

【概述】

MyCERT(马来西亚计算机紧急响应小组)最近观察到针对马来西亚政府官员的攻击活动，攻击者通过发给政府官员的鱼叉式网络钓鱼消息，冒充新闻记者、贸易出版物的个人或相关军事组织，诱导受害者感染恶意软件后，从政府系统中窃取机密文件。此次攻击活动疑似由攻击组织APT40 发起。

【参考链接】

https://www.mycert.org.my/portal/advisory?id=MA-770.022020

5. Gamaredon 组织加强针对乌克兰的攻击

【概述】

在过去的几月中，威胁组织Gamaredon 不断更新其工具集并加强对乌克兰政府和执法部门的攻击活动。Gamaredon 是一个自2013 年以来一直活跃网络威胁组织，主要针对乌克兰政府进行恶意活动，其主要目的是窃取政府，军事人员资料信息。

【参考链接】

https://labs.sentinelone.com/pro-russian-cyberspy-gamaredon-intensifies-ukrainian-security-targeting/

6. Charming Kitten 组织针对世界各地公众人物的攻击活动

【概述】

近期发现Charming Kitten 组织的一系列网络钓鱼活动，新攻击活动的重点是窃取受害者的电子邮件帐户信息并查找有关他们的联系人/网络的信息，受害者包括记者、政治和人权活动家。Charming Kitten（又名Group 83、Newsbeef、iKittens、Parastoo、Newscaster）是伊朗网络间谍组织，自2014 年左右开始活跃。

【参考链接】

https://blog.certfa.com/posts/fake-interview-the-new-activity-of-charming-kitten/

7. Metamorfo 新变种针对多个国家金融机构

【概述】

Metamorfo 是一个恶意软件家族，针对在线金融机构的客户。2020 年1 月发现Metamorfo 变种仅针对巴西金融机构的客户，近日发现Metamorfo 第二个变种，针对多个国家/地区更多金融机构的客户，收集受害者计算机数据并与其命令和控制服务器进行通信。

【参考链接】

https://www.fortinet.com/blog/threat-research/another-metamorfo-variant-targeting-customers-of-financial-institutions.html

8. 2020 年恶意软件状况报告：Mac 威胁首次超Windows

【概述】

Malwarebytes Labs 方面表示，其提供的分析内容包括了对Mac 和Windows PC，Android 和iOS 的威胁，以及一些基于浏览器的攻击。此外，该团队还检查了消费者和企业对全球特定区域和行业所面临威胁的检测。并研究了2019 年的数据隐私状况，包括州和联邦立法，以及一些大型科技公司的隐私失败与其他前瞻性政策并列。

【参考链接】

https://www.oschina.net/news/113352/2020-state-of-malware-report-mac-windows-threats

9. 2020 全球网络威胁全景报告

【概述】

根据最新的IBM 全球威胁调查报告《X-Force 威胁情报指数2020》，受攻击网络中60%的初始访问都是利用以前窃取的凭据或已知的软件漏洞，从而使攻击者更少依赖欺骗来获取访问权限。

【参考链接】

https://www.aqniu.com/industry/63124.html

10. 2019 年涉华APT 态势简析

【概述】

2019 年是不平静的一年，网络空间对抗与博弈、国家背景的APT 活动有着更加明显的网络战争趋势，呈现地缘政治特征的国家背景黑客组织发动的APT 攻

击，穿插在现实国家政治和军事博弈过程中，网络空间威胁或已成为各国情报机构和军事行动达到其情报获取或破坏目的所依赖的重要手段之一。境外APT 组织对我国党政机关和关键基础设施攻击从未停止，对我国网络安全造成严重威胁

【参考链接】

https://mp.weixin.qq.com/s/fcgmWF2mZOtCuHluuYYr1A

11. 2019 年云上挖矿僵尸网络趋势报告

【概述】

2019 年共发现80 个成规模的挖矿木马团伙，以累积感染量定义木马活跃度。从受害者主机的操作系统来看69%为Linux 操作系统，31%为Windows 操作系统，Top10 中的挖矿木马团伙的攻击目标也主要是Linux操作系统。

【参考链接】

https://www.freebuf.com/articles/paper/226605.html

12. 2019 勒索病毒专题报告

【概述】

勒索病毒作为全球最严峻的网络安全威胁之一，2019 年持续对全球范围内的医疗、教育、能源、交通等社会基础服务设施，社会支柱产业造成重创。围绕目标优质化、攻击精准化、赎金定制化的勒索策略，以数据加密为核心，同时展开数据窃取、诈骗恐吓的勒索战术稳定成型，促使勒索病毒在2019 年索取赎金的额度有明显增长。老的勒索家族持续活跃，新的勒索病毒层出不穷，犯罪行为愈演愈烈，安全形势不容乐观。

【参考链接】

http://hackernews.cc/archives/29423

13. 网络安全的“核脏弹”：史上最危险域名即将出售

【概述】

谁掌握了corp.com，谁就拥有了被动攻击全球企业网络的超级僵尸网络，不计其数的企业内部设备，瞬间都会主动投怀送抱，成为这个僵尸网络的肉鸡。是什么让corp.com 成为史上最危险的域名？其拥有者为何要出售这个“火云邪神”级别的域名？这对全球企业网络安全意味着什么？近日网络安全知名博主Krebs撰文深入分析此事。

【参考链接】

https://www.aqniu.com/news-views/62919.html

14. Emotet 木马利用新型冠状病毒主题邮件传播

【概述】

最近Emotet 木马的活动有所增加，它通过诱导用户打开恶意电子附件文档来实现传播，附件主题描述为有关新型冠状病毒预防措施的通知，攻击活动针对日本用户。

【参考链接】

https://exchange.xforce.ibmcloud.com/collection/18f373debc38779065a26f1958dc260b

15. Konni 组织利用CARROTBALL 针对美国政府机构

【概述】

近期发现一种新的恶意软件CARROTBALL 被用于定向攻击活动中，恶意软件通过鱼叉式钓鱼邮件附件分发给美国政府机构和与朝鲜问题相关的专业人士，主题围绕朝鲜正进行的地缘政治问题诱导受害者打开。此次攻击活动疑似由Konni组织发起，该组织是一个与韩国有关的威胁组织。

【参考链接】

https://unit42.paloaltonetworks.com/the-fractured-statue-campaign-u-s-government-targeted-in-spear-phishing-attacks/

16. Winnti 组织针对香港高校

【概述】

2019 年11 月发现Winnti 针对两所香港大学发起新的攻击活动，攻击活动中发现ShadowPad 后门的新变种，它使用新的启动器部署并嵌入许多模块。Winnti是一个与中国有关的威胁组织，至少自2010 年以来一直活跃，该组织主要针对游戏行业，但也不断扩大其定位范围。

【参考链接】

https://www.welivesecurity.com/2020/01/31/winnti-group-targeting-universities-hong-kong/

17. xHunt 活动：继续针对科威特的水坑攻击活动

【概述】

最近发现到一个科威特政府组织的网站被植入了恶意代码，以试图收集网站访问者的登录凭据，该网站自2019 年5 月至2020 年1 月期间，引用了Hisoka 活动相关C2 服务器上托管的图像，攻击者以试图从网页的访问者那里以NTLM 散列的形式被动地获取帐户凭据。

【参考链接】

https://unit42.paloaltonetworks.com/xhunt-campaign-new-watering-holeidentified-for-credential-harvesting/

18. Aggah 活动：针对意大利零售行业

【概述】

针对意大利零售行业的攻击活动近期被发现，攻击基于合法的第三方服务构建了自定义的stager 植入程序，活动中分发的恶意软件包含AZOrult 和Lokibot 木马变种，其中AZOrult 恶意软件主要针对美国、阿拉伯联合酋长国以及巴基斯坦、德国和以色列的少量受害者，而Lokibot 是众所周知的信息窃取器。

【参考链接】

https://blog.yoroi.company/research/aggah-how-to-run-a-botnet-without-renting-a-server-for-more-than-a-year/

19. 超过20 万个Wordpress 网站遭受黑客攻击

【概述】

由于Code Snippets 插件中存在严重的跨站点请求伪造（ CSRF ） 漏洞CVE-2020-8417，超过20 万个WordPress 网站受到攻击。Code Snippets 插件允许用户执行代码，而无需在其主题的functions.php 文件中添加自定义片段。

【参考链接】

https://securityaffairs.co/wordpress/97037/hacking/code-snippets-plugin-csrf-flaw.html

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

安全月报

绿盟科技金融事业部出品

主办/ 绿盟科技金融事业部

地址/ 北京市海淀区北洼路4号益泰大厦3层

邮编/ 100089

电话/ 010-59610688-1159

传真/ 010-59610689

网站/ www.nsfocus.com

客户支持热线/ 400-818-6868

股票代码/ 300369

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