金融行业

5 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

2021安全意识管理新观察

行业研究

洞见RSA 2021 | 如何理解网络安全“弹性”主题?

洞见RSA 2021 | 深度社会工程学攻击,你了解多少?

洞见RSA 2021 |
大数据场景下的安全数据分析及威胁模型构建

洞见RSA 2021 |
如何设计安全的控制系统远程访问

七分真、三分假的合成身份诈骗
给银行带来10 亿坏账

人脸识别黑产:真人认证视频百元一套

NSFOCUS

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

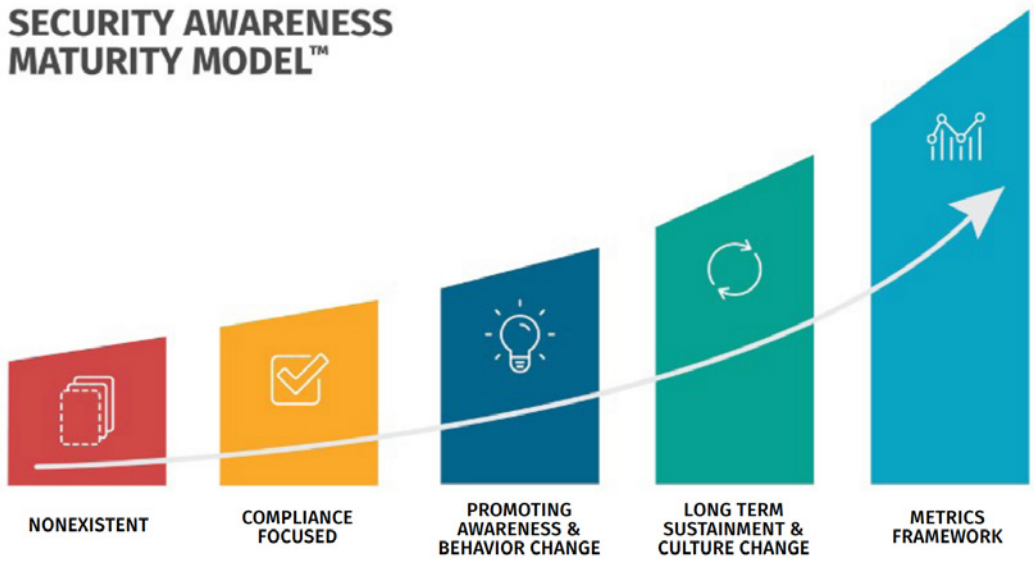
多年以来，绿盟科技致力于安全攻防的研究，为运营商、政府、金融、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。在这些巨人的背后，他们是备受信赖的专家。

客户支持热线：400-818-6868

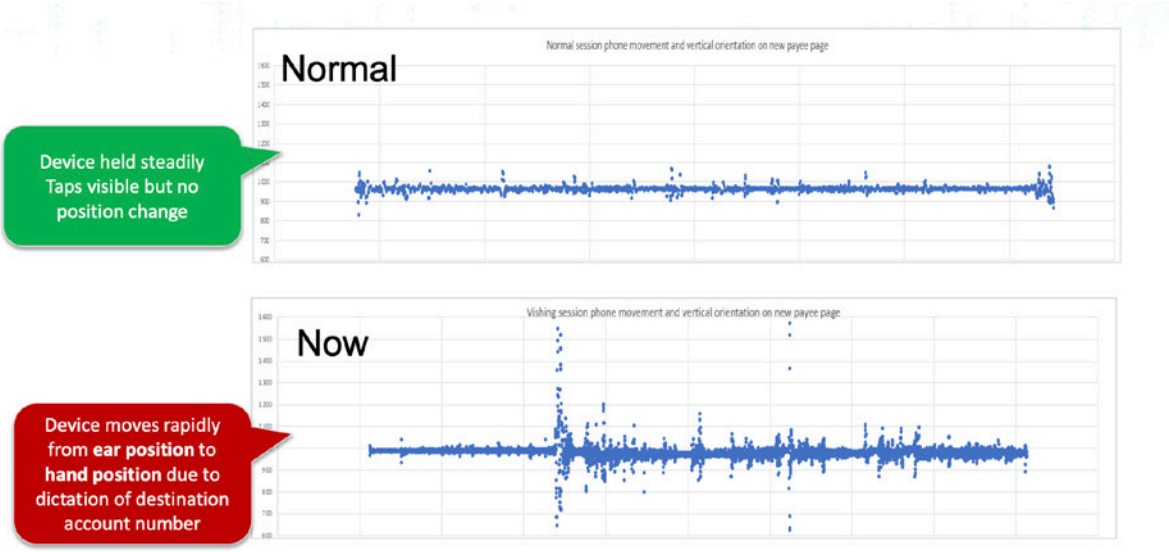
NSFOCUS绿盟科技

本|期|看|点

P4 2021 安全意识管理新观察



P12 洞见 RSA 2021| 深度社会工程学攻击，你了解多少?



安全月报

2021年第5期

绿盟科技金融事业部

目录 CONTENTS

安全月报在线阅读

绿盟科技官方微信

NSFOCUS

安全观点

2021 安全意识管理新观察

绿盟科技　傅戈

一、前言

近年来，在法律法规和监管相继不断完善和加强的双轮驱动下，我国企业的网络安全体系防护建设迈上了新的台阶，防护能力也日益加强。在此过程中，笔者观察到一些企业机构的安全意识管理相对其它网络安全管理内容还相对薄弱，仍有很大的提升改善空间。

安全意识管理本质是改变员工的思维模式以及该思维模式下固有的行为方式。近现代心理学大师勒温提出人的行为（B）和个人影响因素（P）以及环境影响（E）有关，即

B = f（P,E）。而美国心理学大师班杜拉则将该理论进一步发展并提出“交互决定论”。即个人（P）、环境（E）和行为（B）是一个相互动态影响的矩阵。根据这些理论，我们从管理的视角出发就不难看出，安全意识管理的发力点可以放在个人影响和环境影响这两个因素。个人影响因素可以通过安全意识培训的方式进行。通过培训帮助员工了解或加深对企业机构安全策略的认知和理解、扩展员工的网络安全知识面、及时了解最新的网络全威胁和安全案例。环境影响因素则可以通过管理制度、技术措施去规范并强化机构内部的安全管理，让员工时刻感知到机构内部安全管理的严肃性。此外如果机构内部是一种以正向激励为主，惩戒为辅的内部安全文化环境，则员工参与机构网络安全管理活动主动意愿更高，对于可能和正在发生的安全威胁更有可能进行及时地上报、制止或纠正。

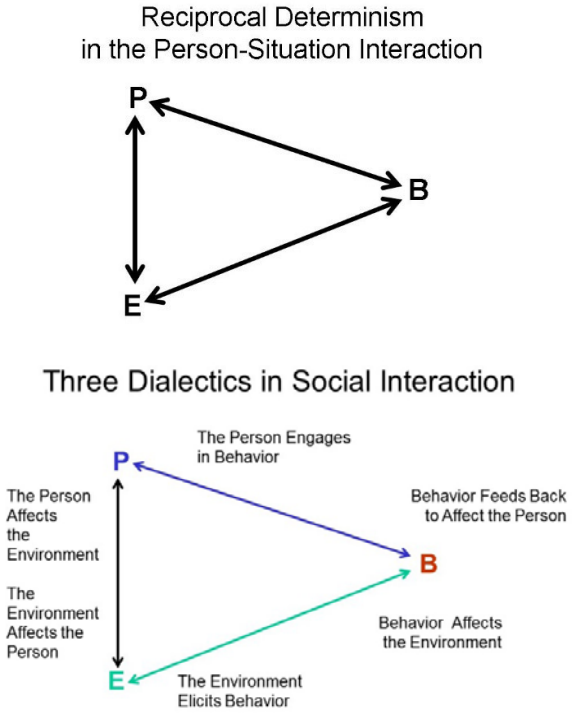


图1：“交互决定论”示意图[1]

二、当前存在的一些问题

国内部分企业机构目前在安全意识管理工作方面还存在着一些不足，导致企业机构整体安全意识管理效果相对有限。这些安全意识管理问题主要集中在以下五个方面：

1. 机构内安全意识管理职责存在分配误区

尽管绝大多数机构已经认识到安全意识是信息安全管理体系中必不可少的一项内容，但少部分机构认为安全意识与员工自身息息相关，涉及的是人自身的风险，因此将安全意识管理的职责放到人力资源部甚至是工会一类的部门。只有当需要进行安全意识培训的时候才让IT部门或者安全部门的人员进行参与。但从网络安全管理的角度上来看，安全意识是安全管理的关键内容之一，安全部门自身对于安全的理解更为全面、对于因员工安全意识不足而可能导致的风险损失有更为深入的认识。此外，优秀的安全部门对安全意识工作开展的出发点并不仅仅从公司管理制度或合规要求出发，而是基于业务、机构安全政策/策略、合规性遵从等多个维度的考量。因此将该项管理职责交由安全部门是更为恰当的选择。

2. 安全意识管理投入资源不足

目前多数机构安全意识管理中投入资源最大的往往是支付外部培训讲师的费用，而用于提升安全意识的其他方式手段，如用于安全意识宣传的音视频材料、展示材料、安全意识测试、安全意识内部学习课件等几乎无投入。培训固然是好的，但是员工安全意识的养成是一个长期的过程，需要多种方式和手段的协助，仅依靠单一的手段通常难以获得更佳的效果。

3. 安全意识培训本身存在较多问题

培训次数和培训时长不足

- “一万小时专家定律”所揭示的道理在此依然适用，那种一年仅投入半天进行安全意识培训的管理行为很难期望参训员工能在短时间内接受相关知识内容并形成行动改变。

培训内容与业务关联性较低

- 安全意识的培训材料多数较为初级浅显。很多安全意识的培训内容通常仅限于密码安全、邮件安全、上网安全、办公环境安全等方面的基础内

容。对于实际业务操作中可能存在的风险问题大多都没有涉及。例如如何避免软件开发中出现业务逻辑错误，如何避免安全测试造成的不必要危害、如何避免网络或安全运维中出现安全误操作等。

- 安全意识培训中通常缺乏我国对计算机网络犯罪相关法律法规的介绍讲解，没有起到法律层面的警示和威慑作用。
- 安全意识培训材料通常不分培训受众，出现要么过于陈述专业技术或者过于偏重案例故事分享的情况，培训效果欠佳。

培训讲师教学技能不足

绝大部分机构邀请的外部培训讲师通常来自于第三方安全厂商或服务商的人员，也有少部分来自于本机构安全部门的员工。这些临时受聘的培训讲师大多都有一个问题，即他们的全日制工作并非专业培训。因此尽管自身技术水平较高，但将内在知识体系以一种听众可接受的方式陈述出来却需要另外一种技能-即教学技能。教学技能缺失或不足的培训讲师常常难以针对实际受众群体的情况将本来就复杂的安全理论知识进行由深入浅或者由浅入深的培训教学。因此，自然也难以达到机构设想的培训初衷。

4. 安全意识管理工作闭环性不足

大多数机构在安全意识的管理过程中没有形成管理的闭环。这些机构的安全意识管理通常没有从管理制度、管理机制、技术手段、人员意识、人员行为、操作风险、合规要求等方面开展过完整的现状评估。其次，在开展执行安全意识的管理活动后没有对培训后的知识掌握情况、人员意识的改进、行为的变化、管理制度和机制的不适应性等进行有效的评估并根据评估结果做出改进、修正等后续工作措施。

5. 安全意识管理工作的正向激励不足

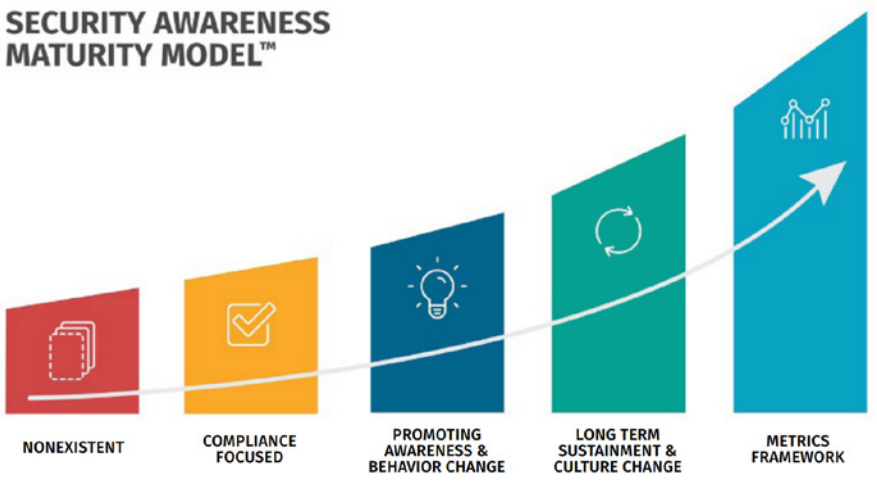
不少机构的安全管理制度通常仅见对于违规处罚的条款，而鲜见如何奖励发现违规事件、违规行为的激励条款。倒金字塔管理法则是现代管理学中较为推崇和倡导的一个管理理念。实践中机构必然需要员工积极参与安全意识管理，因此可以尝试利用上述这个管理理念，通过管理制度或管理机制赋予员工相应的权利、鼓励他们建言献策，对因制止安全威胁，降低机构风险损失的行为给与及时激励，形成一种以正向激励为主、结果导向的企业安全文化。

三、安全意识能力成熟度模型

前面讨论了一些安全意识管理中存在的问题。对于机构的管理者而言，对于发现的问题可以进行整改，但是如何评判机构现有的安全意识管理处于什么样的一个层级呢？这里推荐一个能力成熟度模型供读者参考。

美国著名的SANS机构在2011年集合100多位网络安全专家通过研究讨论

后发布了一个关于安全意识管理的能力成熟度模型。该模型将企业的安全意识管理分为了五个阶段。每个阶段的定义如下：



图：安全意识能力成熟度模型[2]

- “不存在”阶段：

  企业机构中没有任何安全意识管理计划。员工不知道自己是攻击的目标之一，不知道他们的行为将直接影响到企业机构的安全，此外也不知道机构中的安全政策以及如何遵循该政策及相关管理要求规定。这将导致员工极易成为网络攻击的受害者。

- “专注合规遵从性”阶段：

  企业机构已经制定了安全意识管理计划。但该计划的设计主要是为了满足特定的合规性或审计要求。计划中的培训仅限于年度或突发事件触发的临时性提供。员工不能确定机构的安全策略或者也不能清晰知晓他们在保护机构信息资产方面的角色和职责。

- “意识提升和行为改变”阶段

  在这个阶段，机构中安全意识管理计划能够确认安全意识管理的对象群体，培训的主题能应对人员风险中最大影响面并最终能够支持机构的发展使命。管理计划不仅限于年度培训，而且还包括持续和加强的培训。培训内容往往是以一种积极的方式进行交流，鼓励员工行为改变。因此，内部员工能够理解并遵循机构的安全政策，积极认识、预防和报告安全事件。

- “长期坚持和文化变革”阶段

安全意识管理计划在一个长期的网络安全管理生命周期内拥有适当的流程、资源和领导支持，包括（至少）对计划的年度审查和更新。安全意识管理本身是机构组织文化的一个既定部分，不断的保持更新并富有吸引力。因此该计划已经跨越了改变员工行为的范畴，而是正在改变员工的信仰、态度和安全感。

- “指标框架”阶段:

  在这个最佳阶段，安全意识管理计划有一个和同组织任务相一致的强大指标框架，以跟踪进展和衡量影响。因此，该计划可以不断改进，并能够证明投资回报。衡量标准是每个阶段的重要组成部分，这一级别强调机构真正拥有一个成熟的安全意识管理计划，并且该计划必须能够向机构管理者展示其价值所在。

SANS机构的安全意识成熟度模型为我们提供一个较好的对标参照，作为企业机构的安全管理者可以对机构的安全意识管理现状进行评估以了解企业处于安全意识成熟度模型的哪个阶段以及未来的改进方向与目标。

结束语

在信息安全管理活动中，“人”的因素是管理者们普遍认为最具变化性、最难以管控和最大的安全威胁变量之一。美国ISACA组织2020年一份安全报告[3]中显示，如果机构遭遇网络攻击，受调查的管理者认为威胁参与者的因素中内部人员（包含恶意员工和非恶意员工）因素占到了21%，占比仅低于网络攻击者的因素（22%）。而另一份报告[4]显示2020年48%的受调查机构表示至少在新冠疫情期间经历过至少1次钓鱼邮件攻击，25%的受访者在过渡到远程工作后遭受勒索软件攻击。安全意识管理的对象是企业机构本身员工，在一些管理场景中也包含第三方的人员。良好的安全意识管理将在很大程度上降低人员风险暴露面以及因人为失误而带来的安全风险。因此，加强安全意识管理，增加该管理方向的资源投入应该被企业机构管理者所重视，建议应视为一项优先予以考虑的安全战略投资。

参考文献

[1] https://www.ocf.berkeley.edu/~jfkihlstrom/SocialOntology2016.html

[2] https://www.sans.org/security-awareness-training/resources/maturity-model/

[3] 《State of Cybersecurity 2020 Part2: Threat Landscape and Security Practices》, ISACA, https://www.isaca.org/bookstore/bookstore-wht_papers-digital/whpsc202

[4] https://www.netwrix.com/download/collaterals/2020_Cyber_Threats_Report.pdf

NSFOCUS

行业研究

洞见 RSA 2021| 如何理解网络安全“弹性”主题？

“多、准、快、稳”的提高网络安全弹性

美国最大的成品油管道运营商科洛尼尔公司，在当地时间5月7日，因勒索软件攻击导致关停输油管道。经过近一周的应急处理，于当地时间5月12日恢复运营。事件导致美国东海岸成品油价格上涨。受影响区域，等待加油汽车排成长龙，美国航空也因缺少燃油停飞航班。

近年来，网络安全事件导致业务停顿的案例比较普遍。2018年8月，台湾积体电路制造股份有限公司也曾遭遇过勒索软件事件，导致数个晶元厂停产。2016年底，数十万摄像头组成的僵尸网络Mirai以当时最大的DDoS流量(620G)，攻击了美国域名服务商Dyn，导致多家知名网站无法访问。世界经济论坛《2020年全球风险报告》从发生的可能性和造成灾难性破坏的能力角度出发，将网络攻击列为当今十大商业风险之一。

面对网络攻击，如何有效防御？在攻击事件发生后，如何快速恢复业务，减少损失？这是2021年RSA大会所选定的主题词“Resilience(弹性)”的意义所在，也是大会要重点探讨的内容。RSA大会是网络安全行业的盛会，受疫情影响，将在美国时间5月17日至20日线上举行。

RSA大会所指的“弹性”，特指网络安全弹性或者网络空间弹性(Cyber Resilience)。其内涵是将网络安全、业务持续性和企业弹性相结合，应用灵活的安全战略，快速应对威胁，在网络攻击发生时最大程度减少损失，并能保持业务正常运转。

网络安全弹性也有正面的案例。最为杰出的代表莫过于奈飞(Netflix)公司成功应对亚马逊AWS(Amazon Web Service)云上的一次严重的系统中断事件。奈飞的流媒体业务，部署在AWS云服务上，虽然亚马逊AWS的服务水平协议SLA(Service Level Agreement)水平高达99.95%，但不是100%。2015年9月20日，亚马逊美国东部区域(US-EAST-1 Region)的DynamoDB 服务出现故障，引发连锁反应，致使与其关联的20多个服务失效。运行在这一区域的众多知名互联网企业，如Airbnb、Nest、IMDb的网站不能访问。得益于事前的故障模拟和应急演练，奈飞公司成功避开故障区域，将访问流量迁移到AWS其他区域，没有收到任何影响。

如何评价企业网络安全弹性优劣？显然，业务恢复运营的时间是一个关键考量指标。因为勒索软件的加密，导致工业企业停工停产，需要重装受感染的主机的操作系统，才能彻底清除病毒，然后再连接到网络中，恢复业务系统。这个过程一般会经历几天时间。其次，业务恢复的比例，也是一个评价因素。总体而言，业务恢复时间越短，恢复的比例越大，网络安全弹性则越大，反之亦然。

提高网络安全弹性，可以从“多、准、快、稳”四个角度切入，这是体系化建设与实战化运营所追求的安全实效目标。

1) 防护威胁多

内外兼修的安全体系建设，对内是从防守者角度，梳理资产，定期开展风险评估，减少攻击面。对外则构建纵深防御架构。

2) 攻击画像准

常态化威胁监控。结合威胁情报和大数据智能分析等手段，能够在海量告警中准确的发现威胁，对攻击团伙，攻击手段精准画像。

3) 应急响应快

实战化安全运营。出现安全事件后，能够快速应急响应。攻防演练是检验业务系统安全性的最佳实践。

4) 业务运行稳

安全建设和运营的终极目标，就是保障业务持续稳定运行。

关注本届RSA大会，同时更应该关注您的企业的网络安全和弹性。您对业务停摆的最长容忍时间是多长？想要提高网络安全弹性，先从网络安全应急响应预案和演习开始吧。

根据多年攻防经验，绿盟科技应急响应服务结合绿盟科技专业应急响应团队数十年的技术积累，整合公司的研究、产品、服务等能力，针对突发性威胁快速研究分析漏洞细节，提取攻击特征，输出到威胁情报和产品规则，形成防护能力，提供可落地的安全防护方案，依托覆盖全国的安全服务体系，帮助企业尽快对有重大危害的信息系统和网络安全事件作出响应。在安全事件管理的全生命周期中，通过有效的制度流程、组织管理及技术手段，为企业提供多阶段、多层级、多形式服务，有效降低安全事件造成的影响和损失，提升企业应对威胁的能力。

参考资料

1.《2020年全球风险报告》
https://www.weforum.org/reports/the-global-risks-report-2020
2.奈飞公司Blog
https://netflixtechblog.com/chaos-engineering-upgraded-878d341f15fa

洞见 RSA 2021| 深度社会工程学攻击，你了解多少？

BioCath公司在RSA 2021会议上带来了一场精彩的演讲。演讲人从福尔摩斯-红发会的故事，引发了对社会工程学(Social Engineering)的讨论，并进一步探讨了关于深度社会工程学攻击的课题。

一、网络安全与社会工程学

结合网络安全来定义社会工程学：

从心理学的角度出发，密谋一场精心的骗局，诱使目标人物泄露机密信息，以达到收集信息，欺诈或访问用户系统等目的。而社会工程学的运用通常是复杂骗局中必不可少的步骤之一。

目前来讲，在社会工程学的范畴下，网络安全可能会遭受的攻击类型分为以下四种：

1. 静态的机密信息收集 (Static Credentials Harvesting)

钓鱼攻击 / 语音钓鱼攻击 / 短信钓鱼攻击 : 这类攻击会诱骗受害者主动地泄露机密信息，如个人信息，银行信息等敏感内容。

2. RAT陷阱 (RAT Traps)

在攻击前，攻击者会诱导受害者在其个人电脑或移动手机上安装远程控制工具(RAT)。

3. OTP的收集与用户的分心

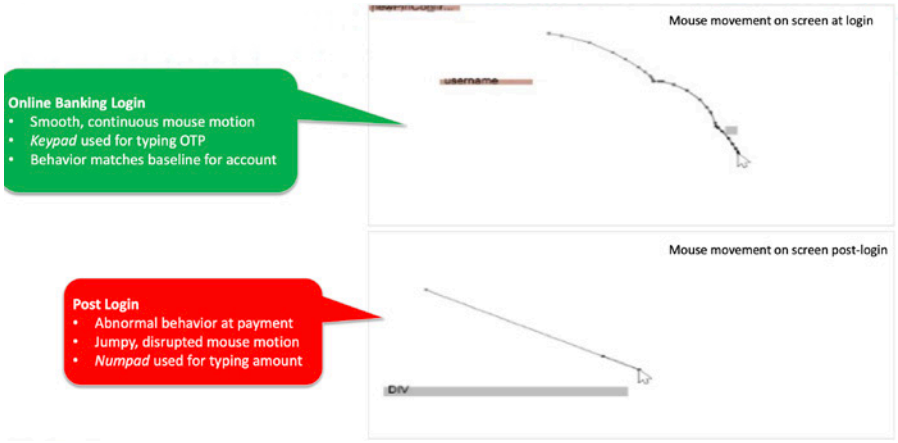
通过电话诈骗收集OTP以供立即使用。比如木马MITB的功能，旨在分散用户注意力和收集OTP。

4. 深度社会工程学攻击

与传统的社会工程学攻击不同，深度社会工程学攻击，看似是一个更完美的骗局，让受害者浑然不知，从心理上认识不到自己已深陷骗局之中。其真正的目的是使其资金直接转给欺诈者。

二、标准的社会工程学攻击

随着网络的发展，以及电子金融的普及。越来越多的网络骗局已经转向电子银行，其最终的目的都是使用各种手段来骗取受害者的财产。但是，对于前三种的社会工程学攻击，从一些细节是可以识别正常和非正常的操作。例如，下图中的两个例子是在登录页面下，正常操作和不正常操作所带来差异，具体表现为鼠标移动的轨迹和付款流畅程度等。



正常操作下登录网银：

鼠标移动的轨迹流畅且连续，键盘用于输入OTP， 所有的行为与账户的基准是匹配的。

非正常操作下登录网银：

鼠标的移动轨迹出现跳跃、卡顿或中断，付款存在异常（因为远程控制你的攻击者可能在不同的国家）。

尽管，这些离线的社会工程学攻击是无法直接检测的。但是我们可以通过用户级别和总体级别的异常来检测欺诈。比如从鼠标移动的轨迹，滚轮滚动方式与时间，键盘删除信息的方式，选择国家的方式等。

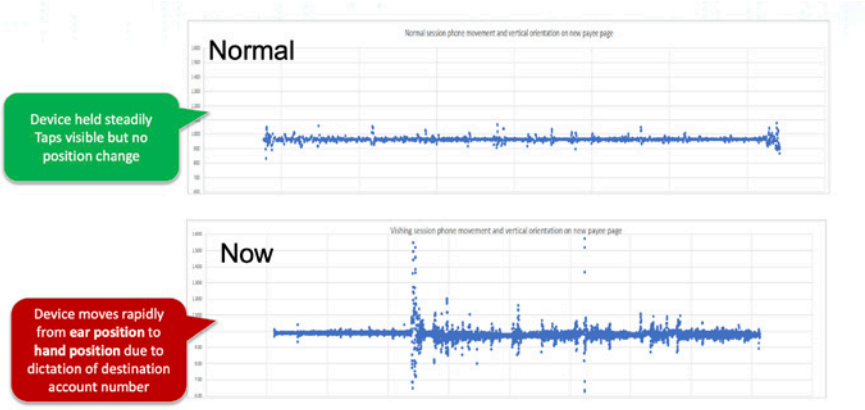
三、深度社会工程学攻击

深度社会工程学攻击，是一种全新的骗局。2019年首次在英国出现，后来逐渐蔓延到欧洲、澳洲以及北美洲各地。

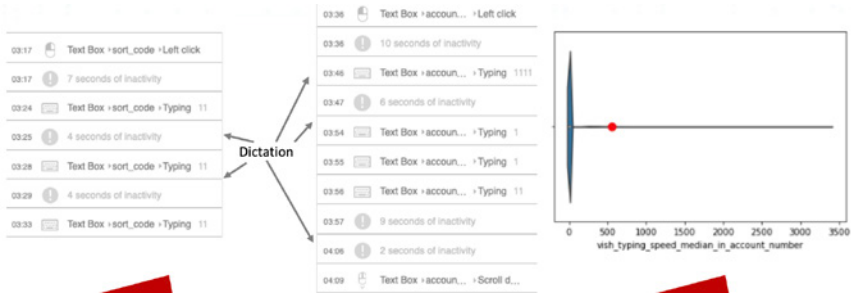
我们可以从一些细微的痕迹上，来观察用户在遭受这种攻击时，所表现出的一些不寻常行为。

比如，被攻击者停留在银行的页面上时间过长，鼠标会有过长的时间来回移动，且从行为上疑似用户不知道要干什么 。因为在整个过程中，攻击者不断的利用语言去营造一个故事，让被攻击者去相信自身并不是在一个骗局中，所以被攻击者的行为看似是分心的，并不是专注在银行的页面上。并且，在最终点击提交的按钮上，被攻击者的行为显得极为犹豫。

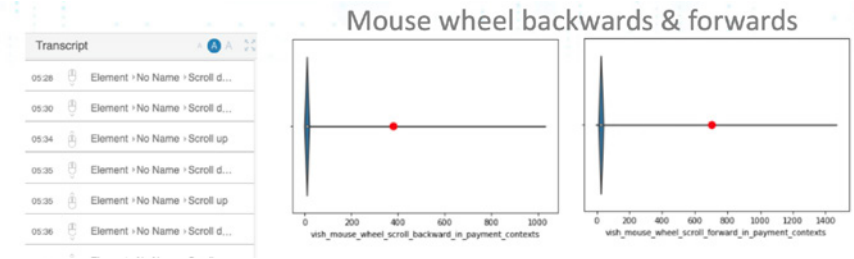
攻击者采用电话语音时，在正常的情况下，语音的总体音量是平稳的，没有出现大的改变。但是在深度社会工程学攻击下，语音会出现波动。根据BioCath公司的分析，因为用户要记录目的账号，所以手机经常会从耳边移动到不同位置。如下图：



从用户输入信息（如账号等）的时间上，我们可以发现一些不同。总体时间上，用户的输入所用是时间比正常情况下的要短，因为用户需要听写对方给予的新账号。



同样，还有一些细微的行为可以看出用户的犹豫和不安。比如，点击提交按钮的时间，以及在交易后，用户频繁地滚动鼠标滚轮。如图，滚动滚轮的频率远高于正常情况下的次数。



最后，整合多个微弱信号中的不同，通过机器学习，最终去判定是否受到攻击。

总结

标准的社会工程学攻击 ，目前的趋势

1. 说服用户在PC /移动设备上安装远程访问工具。

2. 假装自己是银行，诱骗用户通过电话提供OTP码。

3. 在特洛伊木马攻击中使用，以分散用户注意力和收集OTP。

深度社会工程学攻击，一种全新的犯罪类型

1. 引导用户向犯罪分子汇款。

2. 受信任的设备，没有恶意软件/ RAT，没有犯罪的行为。

3. 由于这是完全授权的交易过程，因此不是真正的欺诈行为，但监管机构要求采取行动。

洞见 RSA 2021| 大数据场景下的安全数据分析及威胁模型构建

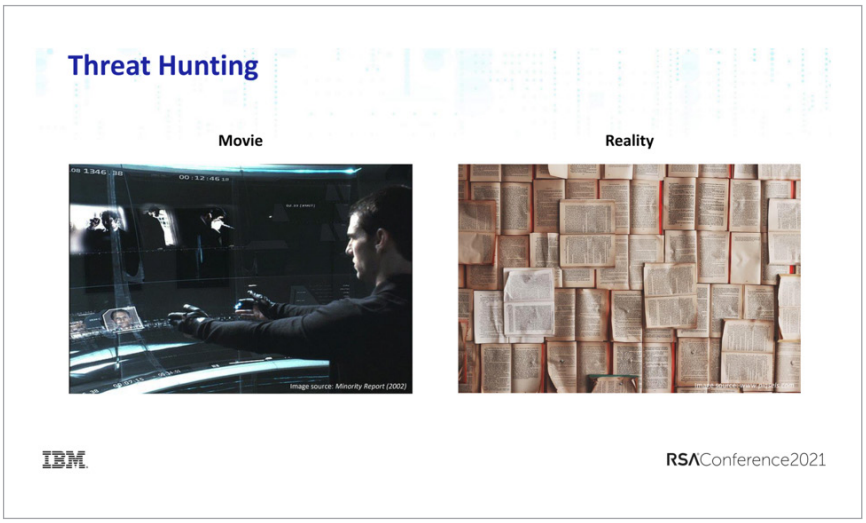
摘要：安全“老司机们”的经验，值得一看

RSA 2021如期在线上举行，大会主题为：Resilience（弹性），强调可恢复性和健壮性。该主题在如今世界疫情导致的混乱大背景下非常贴切，这或许也是黑客&威胁、风险管理相关内容在本届主题中占比最大的原因之一。当然，作为具有世界影响力的信息安全大会，传统安全所关注的一系列相关问题仍是讨论热点。很多参展厂商针对安全领域持续关注的课题提出了自己的思路，其中大部分是再次强调过去实践验证有效的成功经验和方法，另一部分则是创新尝试。

大数据场景下，威胁数据分析和威胁狩猎一直是国家相关监管部门和企业主要的安全应用场景，也是RSA一定会涉及的主题。内容往往涵盖宏观的威胁框架和业务流，以及具体的行之有效的算法应用和数据处理方法等。绿盟君通过梳理本届参展厂商汇报演讲内容，对海量数据背景下部分厂商的数据处理分析和威胁模型构建思路进行总结。

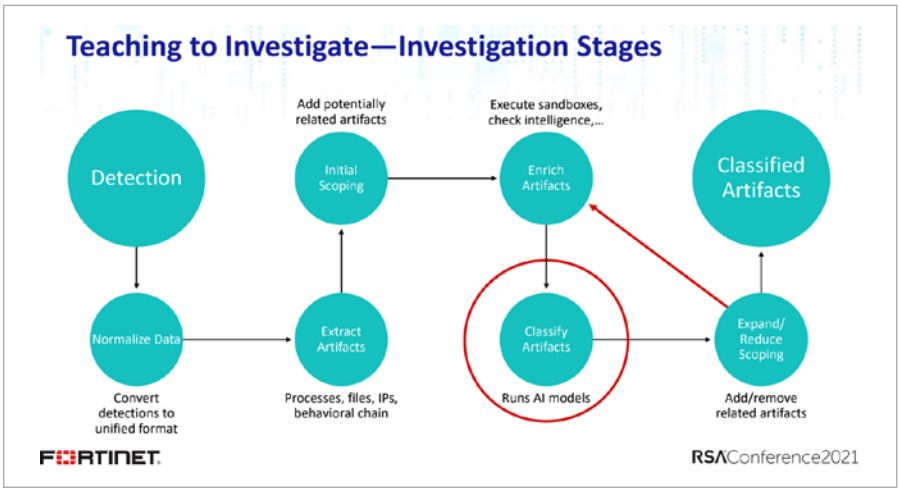
一、海量多模态数据的处理方法

大数据场景下，威胁安全分析一开始需要面对的问题就是如何有效处理接入的海量告警。在一个典型的大数据场景下，接入的数据往往是海量且异构的。

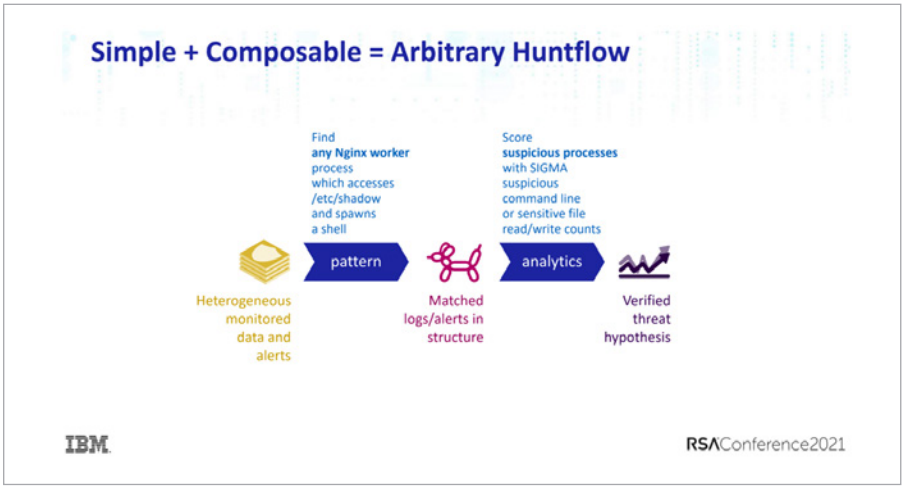


这一阶段的核心诉求在于，一方面希望接入一切能够接入的数据以保证威胁特征的完整性，这些数据通常包括终端数据、各种网络流量探针数据、威胁情报甚至研判人员发出的相关日志等。而另一方面，又希望接入的数据能够得到有效整合和筛选，凸显出真正值得关注的少量数据，从而保证威胁特征的有效性。一定程度上这两个需求互相矛盾，但利用行之有效的范式化方法和特征关联筛选之后，仍然可以同时被满足。

来自Fortinet 的Roy Katmor和Udi Yavo在演讲中列出他们在数据处理阶段的一些关键步骤，包括数据范式化、特征提取、关联和富化。

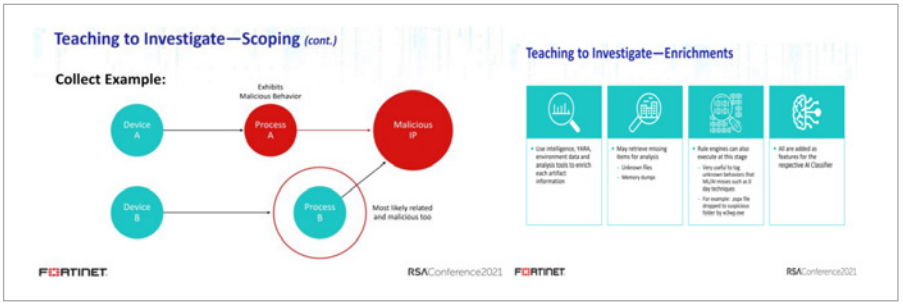


IBM的Xiaokui Shu和Jiyong Jang在介绍他们的开源项目Kestrel时，将他们的威胁狩猎业务流定义为2个关键环节：多模态告警数据的模式化，以及基于该模式的分析模型。



需要指出的是，Xiaokui Shu所说的多模态数据的模式化是基于威胁特征层面的模式化，而非是简单的数据(record)层面，这是他们后续进行基于实体（entity based）的威胁分析模型构建的基础。

此外，基于初始数据进行有效的关联扩展（Scoping）和上下文的富化（conetxt enrich）可以有效补充更多的威胁特征，以支撑后续威胁模型的训练和推理。



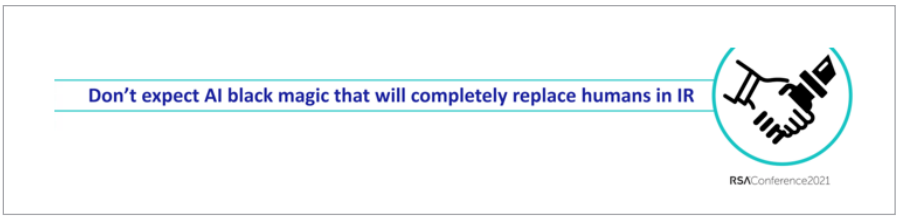
在如何有效聚焦和筛选数据方面，Stamus Networks的两位专家给出了他们的思路。

首先，他们认为可以基于真实的具体威胁源、C&C等类型，或者一系列TTP层面的要素组合方式进行筛选，而非简单根据量化的危险程度筛选。另外，从目标资产视角来进行筛选也是不错的思路。

综上所述，大数据场景下的海量多模态数据处理思路可以总结为几个关键环节：多源数据的采集、数据的范式化、数据的特征富化以及基于特征的筛选。每一个关键环节的具体做法往往依赖于具体安全业务场景和需求，更取决于后续威胁模型的具体数据要求。

二、威胁模型构建方法

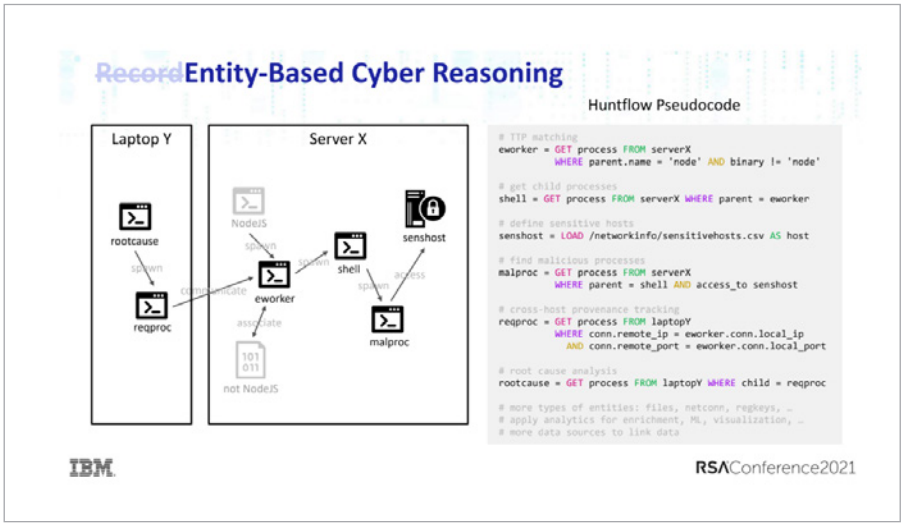
大数据场景下的威胁模型构建往往绕不开各种人工智能算法的参与，但与当年机器学习（尤其是深度学习）刚取得突破性进展时“机器学习无所不能”的氛围不同，近年来，包括信息安全在内的各个行业对于人工智能，特别是机器学习的局限性等问题越来越清晰，Fortinet 的两位专家在他们的《Applying Artificial Intelligence to the Incident Response Function》中就指出，在事件响应方面AI不能完全取代人工。



因此，目前绝大多数研究人员不再盲目相信智能算法，而是转而寻求人工深度参与的“半智能”方法，将专家知识和智能算法进行结合，从而提升算法的可控性和可解释性。

Fortinet的两位专家通过在分类模型的训练数据中引入模拟攻击数据来进一步加强对分类模型的人工干预，并基于细化的威胁特征场景来进一步构建不同的分类模型，降低对分类模型的过度依赖，提升分类模型的可控性。

而IBM的Xiaokui Shu和Jiyong Jang则提出了另一个相对较为新颖的思路：基于行为特征构建的威胁实体，结合专家构建分析模型进行推理。



这个方法有一个前提，就是前文提到的利用行为特征模式化多模态数据，将海量多源异构数据转化为威胁实体，从而能从接近行为的层面进行关联推理。

他们还进一步提出，可以参照STIX的框架进行对应，将STIX中的域对象和关系对象对应威胁实体和推理生成的关联边，从而极大地提升模型的共享和导入能力。

三、绿盟科技相关研究

绿盟科技平行实验室一直持续关注大数据场景下多模态数据的感知理解和威胁模型构建方面的研究。与上文所介绍的几个厂商的研究者方法类似，我们基于对威胁安全的认知，构建了绿盟科技威胁安全知识图谱，并基于图谱本体，将大数据平台接入的多模态数据范式化理解为威胁实体，依托知识图谱保存的威胁语义知识，在实体层面扩充并关联事件语义，结合专家知识和攻击链等模型对事件进行整合及筛选。

在威胁模型构建方面，通过抽取事件及相关上下文语义特征，与图谱中APT组织、恶意代码家族进行特征向量相似度计算，对威胁事件的攻击团伙进行归因。

此外，绿盟科技构建以威胁源为核心的特征图模型，并利用图计算进行多次迭代的聚类，从而发现隐藏于海量事件中的团伙活动。团伙特征也会在简单研判之后保存至图谱团伙知识库中，团伙知识库同样支持STIX格式的导入和导出。

小结

通过梳理本届RSA中大数据场景下的数据分析和威胁模型构建相关方面的研究汇报，我们发现一些传统的思路没有改变，如尽可能接入可能包含威胁特征的多源数据，在保留威胁特征的前提下进行数据的范式化和筛选等。威胁情报引入、上下文语义的富化等处理方法也逐渐被更多厂商提及。

另外，值得一提的是，随着业界对于包括机器在内的人工智能算法的理解逐渐趋于理性，几乎不再看到单纯依靠人工智能算法支撑安全业务的情况，更多安全研究者正在考虑进一步分解安全业务，并加强专家知识的主动干预，从而在有效利用人工智能算法高效处理能力的基础上，提升算法的可控性和可解释性。

洞见 RSA 2021| 如何设计安全的控制系统远程访问

摘要：从RSA 2021看控制系统远程访问

在2021年RSA大会上，美国燃油管道运营商Colonial Pipeline遭网络攻击事件引起了广泛讨论，根据有关网络安全专家分析，此次燃油管道公司遭受的攻击是由于疫情期间该公司职员在家办公远程访问输油管道控制系统，可能导致远程桌面软件账户登陆信息泄漏所致。

如何设计安全的控制系统远程访问?值得我们进一步的探讨和解决。

远程访问存在的问题

远程访问有个比较容易被忽视的问题：目前关于远程访问的很多设计/架构已经过时，相关标准需要重新制定和更新以达到当前的安全标准，但是各种设备的涌现导致标准制定需要考虑很多问题。完全杜绝远程访问，采用封闭隔离模式也不是长久之计。

在万物互联和IOT高速发展的情况下，远程连接必不可少，尤其是在工业控制环境中。现场设备的配置更新、界面设置等很多操作无法由安全人员完成，需要由供应商或控制系统现场人员协助。疫情前人们就已经在考虑摒弃传统的人员在设备现场操作模式，疫情的到来更加速了这个需求。一些传统的架构设计已经不允许我们在独立隔离的环境中完成各种操作，我们必须要直面远程访问带来的各种风险。

远程访问的需求增加

建造落成的时间久远等原因导致很多机构系统过时，特别是一些关键基础设施的工控控制系统。在业务需求变更的条件下，系统需要进行远程访问进行数据交互，即使存在很大的安全隐患，也必须根据手头的情况想办法“完成任务”。但这些系统应用的时间久远且牵一发动全身，无法立刻迁移到新的安全模型。那么到底是什么导致了远程访问的需求增加呢?

1. 业务需求

安全企业和客户需要进行数据交互，从而相互协作以满足业务需求。但是与一些科技公司相比，控制系统的工程师们有一种传统的固有思维“能用就行”，不会更多考虑更新或安全措施等问题，因为他们认为这些“无谓”操作会引入潜在的控制环境风险，造成不必要的损失。这也是需要远程访问能力的原因。安全人员可以去做那些控制工程师们不愿做的事情，如更新升级/打补丁等，通过开放某个远程访问接口，让指定的人去提升安全性，皆大欢喜。但随之而来的问题是：通过远程接口在解决一些安全问题的同时，也引入了新的问题，如开放一些协议通信的本身就存在安全隐患。当然仅仅开放一个端口用来连接肯定是不合适的，我们需要考虑如何在建立安全接口的同时，避免它带来的安全隐患（不要给操作员和攻击者同时开放访问接口）。

安全人员的建议同样可能带来负面影响，阻碍原本业务的顺利进行，出现从“新系统不太安全但是效率高”到“老系统比较安全但是效率低”的结果。所以找到平衡点也是在工业控制环境中引入远程访问的重要问题。

2.政策需求

政府的需求也会迫使提供远程访问功能，如需要在一定时间内回应突发事件，操作员第一时间响应并到现场操作的行为并不现实，只能通过远程访问来避免迟到。有些现场位置偏远，离开远程访问的支持将导致响应突发事件效率低下，不仅无法达成政策指标，也会造成实际风险的响应延迟，增加损失。控制系统确实需要满足发生特殊事件时的特定需求的现实，在后疫情时代更加明显，如远程访问才能确保业务能够照常进行。

3. 成本和其它

还有很多原因造成远程访问需求的逐渐增加，如远程维护支持比现场支持的

费用更低。还有一些第三方提供的业务优化服务，布置在云端，将控制现场的数据接收过来后，通过优化算法再传回控制器，对整体工业流程进行优化操作。虽然确实可以让整体生产控制过程优化，但这也产生了一个新的安全隐患点。

如何定制远程访问控制体系？

近年来，有很多ICS/OT环境的安全事件都与访问控制有关，因此很多人并不看好远程访问，认为会使目标更加脆弱，但这些安全隐患都源于远程访问功能实现过程中的缺陷和不足。直接开放一个外界链接端口或引入一款协议用于数据通信肯定会带来很多安全问题（如端口忘记关闭或引入的协议本身就存在漏洞等）。理论上如何实现远程访问有很多更好的方式，如利用分开的Token使用多重认证系统，远程接入的人员持有一个Token，通知控制系统的管理人员获取响应的Token后，获取访问权限。如利用DMZ对关键环境的网络进行隔离，在这个缓冲环境中分配指定的访问凭证，并拥有完整的监听权限。

关于如何才能最大程度降低风险，目前还没有统一的标准架构，所以企业需要根据自身的业务需求和安全标准来量身定制远程访问控制体系。

监控访问行为

与一般的IT系统不同，在工业控制环境中更难监控所有访问行文。一方面不同系统使用不同的远程访问功能，在成本和收益角度来看，小众的系统由于使用人少可能会疏于监控。而有些功能虽然设计时是为了完成X目标（如开启远程接口用于系统固件的下载更新），但攻击者可能会挖掘出该系统的潜在功能Y，因此监控很难及时发现恶意的Y行为，尤其是远程访问。

总之，好的理论要用好的方式来实现。任何远程行为都应该有详尽的日志记录，并做好访问的权限控制，对于任何远程访问行为都拥有完整的监控能力，以便在发生异常事件后回溯定位问题根源。

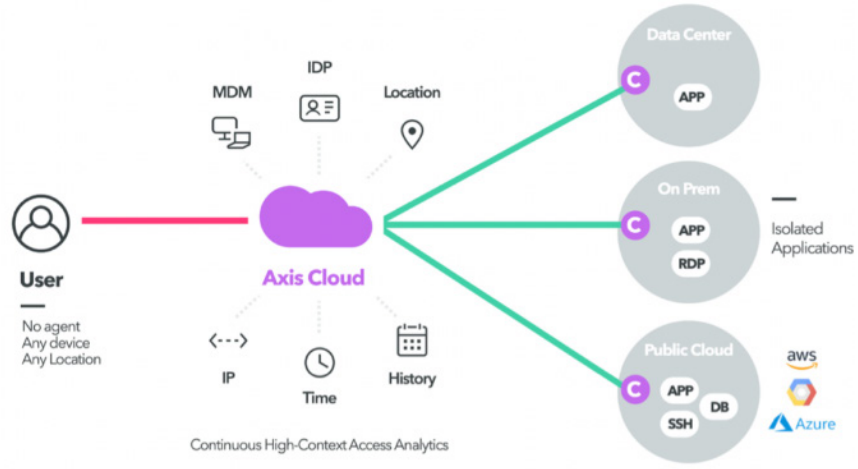
洞见 RSA 2021| 零信任的困境与破局之路
从 RSA2021 看零信任

从RSA2021看零信任

数字化转型中，云计算、大数据、物联网、移动互联等技术的业务应用加速落地，新技术元素的导入，提升业务效率，同时也带来了新的安全风险。面对传统安全防护方案的局限性，“零信任”提供了新的安全思想，零信任秉持 “从不信任，始终验证”的原则，在不可信网络中构建对应用系统的安全访问是零信任的终极目标。

随着零信任安全的持续火热和崭新的安全理念，吸引越来越多的企业希望向零信任转型，本次RSA大会，零信任也成为此次会议的热门话题之一，众多厂商从不同角度对零信任架构做出了分析；包括数据安全与个人隐私、云安全、弹性与恢复、身份安全等其他热门话题也都和零信任密切相关。

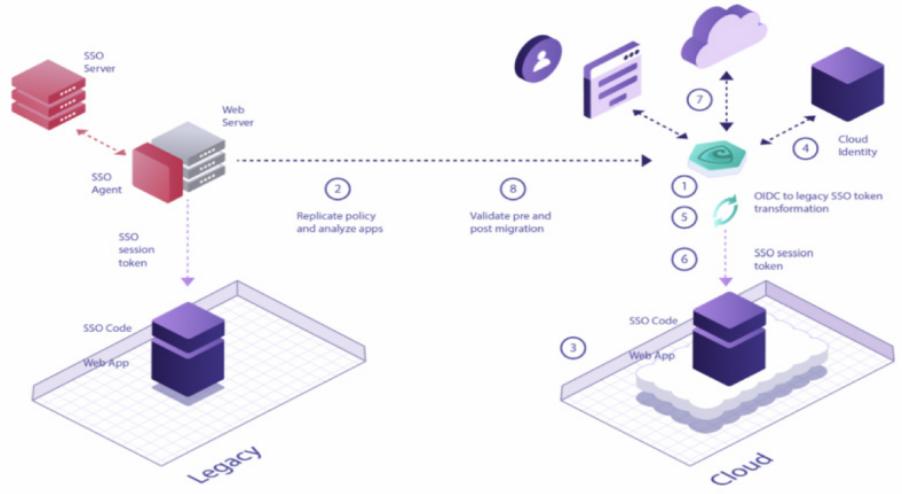
同时在RSA创新沙盒TOP10中有两家公司产品和零信任相关，Axis Security公司的零信任方案（Application Access Cloud），直译过来就是“应用访问云”，此方案的创新之处在于依托于云计算，使用无终端化方式接入，应用服务侧只需部署连接器即可，这样大大减少了企业从传统VPN接入方式向零信任网络迁移的技术阻碍。当然此方案也有一定的局限性，事实上，无终端化是相对而言的，只是覆盖了主流服务，如Web服务、RDP服务、SSH服务、Git服务和数据库服务等。如果终端只需要访问这些服务，就不必安装终端。但是如果安装终端则允许终端访问几乎任何形式的网络服务，应用范围会更加的广阔。



图片摘自Axis Security公司官网

STRATA公司的企业多云身份管理，能够对接多种云服务的身份数据和访问控制策略基础设施。同时，方案适配多种身份认证协议，在应用零改造的基础上实现统一管理。STRATA MVERICS平台联动三个产品，身份发现（Identity Discovery）、连接目录（Connector Catalog）以及身份编排引

擎（Identity Orchestrator）提供关键能力。由于零信任架构强调“以身份为中心”，建立基于身份的细粒度访问控制。因此此方案可以大大推动零信任架构实施，让企业以最小的代价完成零信任架构迁移的第一步。



图片摘自STRATA公司官网

关于零信任的未来思考

零信任是一种新型的网络安全架构，可以从零开始建设，也可以在现有的基础设施之上构建新的安全防护机制。基于各类创新技术的不断发展对现有技术的冲击，厂商需要做好合理的用户引导，在未来的很长一段时间内，做好传统安全技术和零信任技术共存的心理准备，一边运行，一边建设，逐步替换，保证新旧技术的平滑演进。

包括我们在为企业推广零信任安全解决方案的时候，不能完全颠覆企业当前的安全建设成果，而去打造一个全新的零信任安全体系。需要充分考虑零信任方案如何和客户当前存量安全产品相互融合，为企业的安全保驾护航。

零信任方案在设计之初，就需要包容的心态，要与各种安全能力和谐共处。围绕零信任“永不信任，持续认证”的安全理念，将各种安全能力统一归属到零信任体系之下，将其作为零信任的“耳目”。通过丰富的异构产品接口，收集各安全产品的安全日志和安全事件，进行集中分析和研判，打造全访问链的动态可信访问。

绿盟科技零信任实践

结合上述思考，作为网络安全行业资深厂商，绿盟科技很早就开始布局零信任领域，历经数年从最早期的SDP研究，时至今日已经有了成熟的零信任解决方案支撑不同行业客户的特定安全访问场景及安全需求。

方案概述

绿盟科技零信任安全解决方案基于设备评估，用户认证和行为分析，持续集成分析和验证信任关系，以此在不可信网络中构建安全系统，覆盖了远程安全办公、暴露面收敛、统一安全访问、数据安全访问及终端安全接入等典型应用场景。

方案核心产品包括：

- 一体化终端安全管理系统UES
- 安全认证网关SAG
- 统一身份认证平台UIP
- 零信任分析和控制平台ISOP-ZTA

方案特点：

- 方案产品灵活组合，分层解耦，可独立部署，支持根据客户实际需求分阶段或选择性建设。

- 通过客户端和安全认证网关从访问主体到访问客体之间，建立安全访问通道。
- 采用SDP方案，实现业务应用的彻底隐身，让攻击无从下手。
- 绿盟零信任大脑作为总分析和控制中心，由终端安全管理平台，统一身份认证平台，分析和控制平台组成，构建风险和信任综合分析能力，动态决策响应能力，实现纵深防御。

核心能力

- 全面感知

上下文环境感知。终端安全状态感知，网络环境上下文感知，威胁情报输入的感知等。

- 最小授信

终端可信，用户可信，网络可信，应用可信，最小化权限访问资源，实现最小授信。

- 持续评估

从认证系统，安全设备，网络流量，终端安全等多维度获取信息，持续分析用户和实体行为，确保用户在访问过程中的行为可信。

- 动态决策

根据用户及终端的安全风险，自动化的下发策略，执行阻断，二次验证，隔离等操作，实现基于风险的自适应安全访问控制。

客户价值

统一安全可信访问

- ☐ 全面隐藏应用，减少暴露面
- ☐ 统一MFA认证，杜绝弱口令，避免未授权访问
- ☐ 细粒度会话控制，防止越权访问，攻击横向扩散
- ☐ 全面日志审计，关联分析，闭环处置

零改造快速合规

- ☐ 统一多因素认证，满足等保2.0对身份认证因子相关要求
- ☐ 国密加密，满足等保2.0，密码法对关键基础设施传输和存储加密的要求
- ☐ 无需大批量业务改造和替换，快速合规

全方位降本提效

- ☐ 节约管理&运维&人员成本
- ☐ 提高办公访问效率，提高员工工作效率
- ☐ 账户&权限统一管理，业务灵活扩展，数字化转型无忧

一致便捷的用户体验

- ☐ 访问低延迟，更少等待
- ☐ 无密码认证，无需记忆繁杂密码

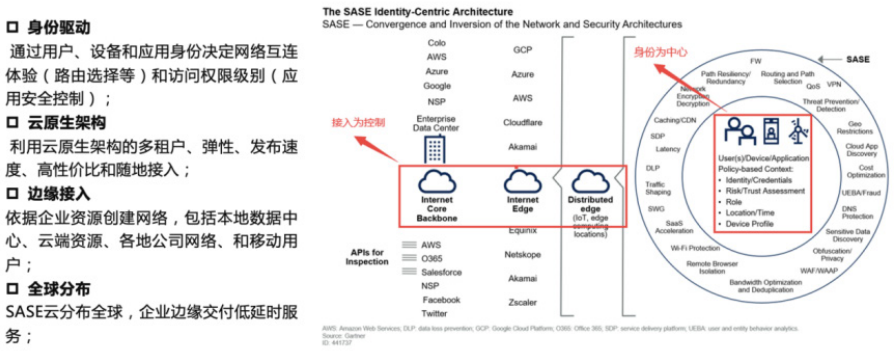
推荐建设步骤

写在最后

“网络安全的未来在云端”，随着信息化数字化办公的兴起，越来越多的企业将自身应用迁移到了云端，或者直接购买云上的SaaS服务。这种方式大大提升了办公效率，任何个人都可以通过BYOD设备快速访问企业应用，做到随时随地办公。但同时也增加了企业应用的安全风险，由于应用部署在云端，企业不得不去考虑这些应用的安全性，包括访问权限、服务隔离、数据放泄露、安全审计等。

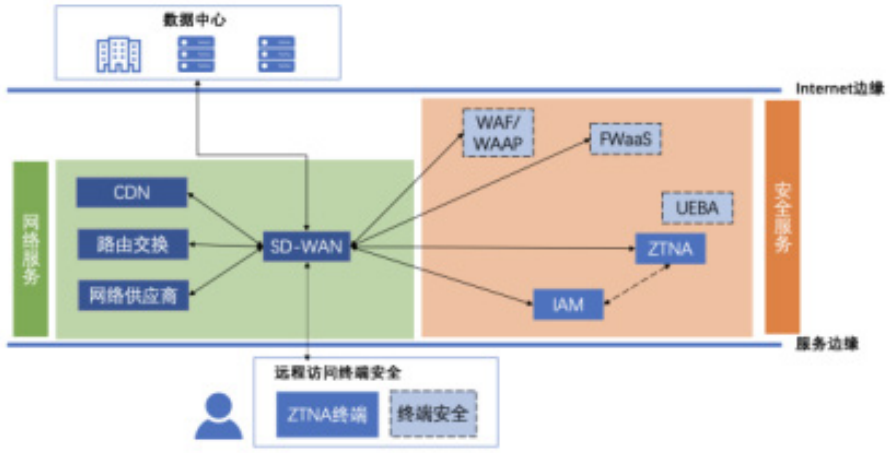
基于这种背景，Gartner于2019年提出一个全新的安全概念SASE（Secure Access Service Edge），即“安全访问服务边缘”。 SASE是一种整合各种云原生的安全功能，例如SWG、IPS、NGFW、CASB等，基于零信任网络访问（Zero Trust Network Access，ZTNA）模型建立推出的一种管理型服务，从而满足企业在数字化转型过程中的动态安全访问需求。SASE 是一种基于实体的身份，实时上下文 分析、企业安全/合规策略，以及在整个会话中持续评估风险/信任的服务。

SASE同样是以身份为驱动，ZTNA架构为核心，这些理念和零信任高度一致，可以看做零信任在云场景的扩展和演进。因此在关注零信任的发展和趋势时，有条件的情况下可以和SASE方案做适度的融合，贴合更多的用户场景。

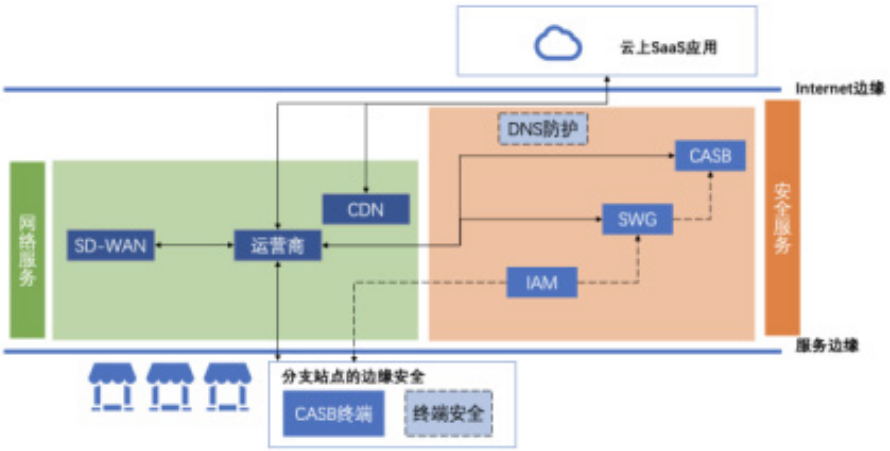


SASE技术全景图

绿盟科技也将于近期发布SASE安全解决方案，分别推出两款产品NIA（NSFOCUS Internet Access）和NPA（NSFOCUS Private Access），涵盖不同的应用场景，为企业的数据中心和云上应用安全保驾护航。



绿盟云安全内网访问服务（NSFOCUS Private Access）



绿盟云安全公网访问服务（NSFOCUS Internet Access）

NPA是基于零信任的云安全内网访问服务，适用于用户到私有数据/程序的连接，基于零信任原则，云端控制器根据上下文做接入控制，提供多因子认证、三方身份认证、暴露面隐藏等能力。NIA依托服务化的云上安全网关，基于防火墙、IPS、沙箱等为客户提供针对Web和Internet的威胁保护。

如需更多信息，敬请关注绿盟科技官网发布。

七分真、三分假的合成身份诈骗给银行带来 10 亿坏账

摘　要：2020 年10 月，四川警方查处了一个上百人的诈骗团伙，和一般的诈骗团伙不同的是，这帮人的诈骗对象不是一般的消费者，而是金融机构。

关键词：标签（合成身份、金融诈骗），技术问题（安全事件）。

内　容：《移动支付网》消息：2020 年10 月，四川警方查处了一个上百人的诈骗团伙，和一般的诈骗团伙不同的是，这帮人的诈骗对象不是一般的消费者，而是金融机构。

这帮诈骗犯通过收购“僵尸企业”“空壳公司”等方法，掌控了多地公积金缴存渠道，为6千人包装公积金信息，通过手机在线上向多家银行申请公积金贷款，最终给这些银行带来10 亿多坏账。

这样通过在数字平台上结合真实和伪造的信息进行诈骗的手段被称为合成身份诈骗。这样的诈骗手段在国外已经不怎么新鲜，2019 年美联储发布报告指出，合成身份诈骗在美国日益猖獗。

在国内，侦破此案的专案组与相关部门充分沟通后认为，此案堪称全国贷款诈骗典型。这样的手段也经常出现在网贷骗贷案中。

合成身份诈骗的可怕之处从案例可以看出，合成身份诈骗与一般的诈骗有两处最大的不同，首先诈骗对象不同，合成身份诈骗的目标一般为金融机构；其次，合成身份诈骗采用真假结合的方式骗过风控，迷惑性非常高。

结合案例来说，银行在对贷款申请进行审核的时候，面对的资料几乎是天衣无缝的，几乎所有的信息都是真的，身份信息真实可查、公积金存缴信息真实可查、征信信息真实可查，唯一的破绽在于这些信息都不是本人所拥有的，是由诈骗分子虚假伪造而来。

而几乎所有操作都可以通过线上完成帮助了骗子掩盖自己的行为。事实证明这样的手段很成功，成功次数超过6000 次，银行很难进行有效防范。

另外，由于新冠疫情影响，金融机构数字化转型速度加快，通过远程渠道进行身份认证逐渐流行。如果在远程身份认证上增加太多环节，往往会降低用户的使用体验，从而失去用户。流线型且无障碍的远程身份认证体验是很多金融机构希望的样子。

但是“流线型且无障碍的体验”往往会带来一定程度的风险，风险就来自于这些专业的诈骗分子，他们会不断地去测试漏洞，确定目标，然后集中攻击。

这一点在过去的“网贷骗贷”中很常见，犯罪分子几乎每天都会通过电脑不断试错，企图寻找平台风控漏洞，通过部分IP 地址不断发来借款申请——每次借款人的收入、年龄、婚姻状况、工作等各有细微不同，以此不断“试错”摸出平台的风控侧重点或漏洞。

人脸识别？不一定那么靠谱

针对这样的诈骗手段，金融机构也不是没有任何办法，在金融科技的加持下，引入人工智能技术，对借款人做人脸识别。这种做法的好处，一是能有效验证申请人的身份，防止伪冒他人身份申请贷款，二是借助微表情等人工智能识别技术捕捉到借款人在面审回答问题环节的细微、异常的神情变化，从而发现群体潜在的骗贷行为。

但人脸识别不一定那么的靠谱。从技术上来说，通过真人认证视频骗过验证并不是难以做到。

近日就有媒体报道，贩售卖真人人脸识别视频的黑灰产大量藏匿在QQ 群中和境外网站中，其中QQ 群名称多包含“过脸”“识别技术”等关键词，从而方便买家检索到相关信息。

在App 平台人脸验证黑产中，百元一套的验证视频属于“价高质优”产品，因为使用了真人录制的动态验证视频，验证通过率较高，还有一种低廉的人脸认证方式，即使用动态软件将人脸照片制作成“动态视频”，配合“外挂”软件进行验证。“低廉的一套只要几元钱，需求量大的话甚至可以低至0.5 元一套。”一名卖家表示，人脸动态验证的成功率，主要取决于照片动态化处理的细致程度，但真人录的视频肯定可以100%通过。

无论是真人录制视频还是照片动态化处理，在完成App 人脸动态验证的重要工具就是手机和外挂软件。黑产卖家表示，从二手交易平台上花费200 余元就可以买来某品牌二手R9 手机，然后将刷机包植入到手机中。

当App 需要通过摄像头进行人脸验证时，用手遮挡摄像头，手机“外挂”就会启动，通过修改相关数据和设置，将提前做好的动态人脸视频导入到App 中完成认证。

除了技术手段，诈骗分子可以直接通过“纯白户”进行诈骗。所谓的纯白户指没有贷过款，没有办过信用卡，“征信纯洁得像一张白纸的客户”。诈骗分子往往会选择使用老年人或失业、偏远地区的人，以诈骗或金钱的手段让他们进行具体的诈骗步骤，从而让这一步形同虚设。

在文章开头的案例中，50 多岁洪某就是一名“纯白户”，她来自重庆一个小山村，连智能手机都不会使的她在广东打工时，遭遇传销，被传销头目介绍给一名她不认识的男子，在其“帮忙缴纳公积金”的鼓吹下，办理了银行卡。随后在该男子的操作下，洪某在手机上向银行申请了贷款20 多万。不过，这20多万，在到账的时候就被转走了，洪某只得了2 万多元。“白”得了2 万多元，洪某很高兴，即便贷款逾期银行发来催款短信等，她也无动于衷。

如果不是细心的工作人员在洪某提取公积金时被工作人员发现端倪，此案根本不会被发现。对于被盗取身份的受害者、特别是弱势群体来说，合成身份诈骗可能要等到其个人信息受到损害后的数年才被识别和确认。

银行等金融机构必须要面对一个事实，由于侦破欺诈难度大、犯罪成本低以及金融体系数字化程度不断提高，未来此类金融诈骗行为恐将继续存在。虽然合成身份欺诈不会很多，但是会严重影响其资本和贷款损失。

想要解决问题，金融科技或许需要在身份认证相关技术上再多迈出一步。

信息来源：https://mp.weixin.qq.com/s/nou_41AQ1GsrilGfBBkJFA

人脸识别黑产：真人认证视频百元一套

摘　要：身份证正反面照片、手持身份证照片和点头、摇头张嘴视频，多藏身于社交平台，卖家称能通过多家APP 平台视频验证。

关键词：标签（黑产，信息泄露），技术问题（安全事件）。

内　容：3 月30 日至4 月5 日，新京报记者调查发现，这种地下黑产交易大多藏匿在QQ 群中和境外网站中，其中QQ 群名称多包含“过脸”“识别技术”等关键词，从而方便买家检索到相关信息。

在APP 平台人脸验证黑产中，百元一套的验证视频属于“价高质优”产品，因为使用了真人录制的动态验证视频，验证通过率较高，还有一种低廉的人脸认证方式，即使用动态软件将人脸照片制作成“动态视频”，配合“外挂”软件进行验证。

“低廉的一套只要几元钱，需求量大的话甚至可以低至0.5 元一套。”一名卖家表示，人脸动态验证的成功率，主要取决于照片动态化处理的细致程度，但真人录的视频肯定可以100%通过。

对于人脸识别信息买卖，北京云嘉律师事务所律师赵占领表示，据民法典规定公民对个人信息享有民事权利，未经本人同意非法收集买卖他人信息会构成民事侵权。

人的脸部特征信息是能够直接识别特定自然人的真实身份的信息，属于个人信息范畴，如果未经用户同意买卖个人信息涉嫌违法犯罪。

张女士在注册微博进行人脸验证时，被提示自己的身份证信息已经被注册过，但此前她并未下载和使用过微博。

张女士咨询微博客服了解到，若扫脸注册微博时提示“该身份证已经绑定其他账号”或“身份证使用次数超限”，是由于身份证已经绑定其他账号。目前，一个身份证号可以绑

定2 个微博账号，当身份证号绑定账号数量达到上限时，就无法再使用当前身份证号进行验证。

“肯定是我的信息被泄露了。”张女士称，她平时还算比较注重个人信息保护的，身份证除了上学入职、办银行卡、办电话卡、住酒店、买车票用过，其他地方就没有使用过了。

张女士的遭遇并非唯一，多名网友曾发帖称自己在注册微博、QQ、公众号等，发现个人身份信息被盗用。

随着个人信息被冒用数量的增多，网络相关的反馈和投诉也随之增多，随之而来的是各大APP 平台的安全验证升级，以动态人脸识别作为安全验证方式。在APP 平台安全验证升级迭代中，这条黑色产业链的从业者也在利用漏洞，“专研”其如何破解这一“困局”。这条伴随着互联网实名制发展而兴起的黑产利益链，也从最初单纯收集贩卖姓名、身份证号，升级到了收集贩卖手持身份证照片、人脸视频和照片动态处理软件。

一名在暗网中贩卖个人信息的黑产卖家介绍，身份证正反面照片、手持身份证照片和人脸点头、摇头视频，一套100 元，量大的话可以优惠，如果一次性购买100套，价格可压低到10 元一套，“如果数量少真的便宜不了，我们收集这些信息的成本也高。”

接着，对方发来两段别人录制的张嘴、眨眼、点头、摇头视频，称“这些是真人录制的视频，验证大部分APP 都没问题，比照片处理的动态视频通过率高”。

多名黑产卖家称，他们开发包括借贷、走路赚钱等APP，其售卖的这些信息便来自于用户下载注册这些APP 时所采集的，“这些人大多是工厂工人，还有一些网络兼职人员。”

但这些网络刷单兼职人员，并不知道自己在做一些APP 认证的单子时，会泄露隐私。

来自山西的白女士告诉新京报记者，她从半年前开始做一些刷单等网络兼职，有时候刷单量有限，她就会做一些APP 认证的单子。

白女士表示，这些单子需要扫描对方提供的二维码下载APP 然后进行实名认证，实名认证的过程大多数会让上传身份证正反面照片、进行人脸识别，之后才算注册成功。一个单子大概5 元-15 元不等，有的认证要求复杂的

价格会高一点。

在兼职刷单中，有的只需要上传姓名和身份证号，这样的每单3元，需要进行人脸识别的价格可能会到十几块钱。白女士说，有的APP 在进行人脸认证的时候，眨眼摇头幅度大一点，或者人脸离得近一点，会比较好通过。

“没想到过会有人用这种方式收集个人信息，也从来没有听说过会有人收集人脸识别的动态视频。”白女士称，自己刚开始接这种APP 注册的单子时，遇到身份和人脸信息验证时有过犹豫，但是后来觉得群里大家都在接单，也没听人说出现什么问题，也就开始这样做了。

兼职刷单认证造成的数据泄露，应算是少数。曾有媒体报道，有80%的个人信息数据泄露，都是企业内部员工所为。

不少黑产商贩也认可这个说法。有商贩透露，如今市面上流通的手持身份证照片大多是在小额贷款平台和公司野蛮发展期间，泄露出来的，还有部分是从各行业收集而来的，这种信息交易和使用一般情况下不会被人发现，“当时很多人借钱不还，平台就把这些信息拿出来卖钱了，刚开始挺贵的，现在层层转卖就便宜了。”

除此之外，如今日常使用APP、进出店铺等场合均需要进行人脸信息识别和采集，还有人员以人脸识别技术开发和系统测试为名开展信息采集。

在网络中，新京报记者留意到有人发布招聘信息采集员的信息，工作内容为到乡村采集身份证、人脸信息，可以将食用油、锅等商品作为礼品赠送。

相比真人视频录制，将照片中的人脸通过软件进行动态化处理形成验证视频，成本更低。

3 月31 日，新京报记者通过QQ 群按条件查找，在搜索框中输入“过脸”“识别技术”等关键词，便会出现众多相关QQ 群。记者随机加入6 个QQ 群发现，这些群内的成员从100 余人到1700 余人不等，并且不时有新的成员加入。

QQ 群中，不时有人发布出售微信号、售卖换脸软件的信息，同时还有人在咨询如何将照片中的人物进行动态化处理，并通过人脸识别验证。此外，在新京报记者以需要购买人脸认证技术和软件的身份加入群后，3 个小时内便有多名黑产信息贩卖者添加记者好友，了解需求。

这些黑产卖家表示，他们售卖照片抠图、动态化处理等软件，使照片中的人物张嘴、眨眼、左右摇头和上下点头。之后，通过特定手机开“外挂”进行人脸识别，“我们一般用于验证微信、QQ、陌陌多一些，其他软件也都可以人脸验证。”

3 月31 日，一名从事黑产买卖的商户在其QQ 空间发布消息称，由于微信安全验证升级，暂时已无法通过人脸识别验证，自己正在研究办法。4 月3 日，这名商户表示已经攻克新的安全验证，可以接单。此外，这些商户还售卖身份证正反照片、手持身份证照片以及带有人脸的照片，在黑产圈俗称为“四件套”，每套价格在0.5 元至3 元不等。

当被问起这些证件照片的来源，商户在聊天过程中便开始谨慎起来。最后新京报记者表示对四件套信息有大量需求的情况下，一名卖家表示有人专门负责收集，自己也是从别人那里买来再卖的。

黑产卖家售卖的个人信息，包括身份证号及照片等。无论是真人录制视频还是照片动态化处理，在完成APP 人脸动态验证的重要工具就是手机和外挂软件。

新京报记者通过向黑产卖家询问得知，从二手交易平台上花费200 余元就可以买来某品牌二手R9 手机，然后将刷机包植入到手机中。

部分APP 平台在人脸识别验证过程中，屏幕会变成红、黄、蓝三种颜色，以此验证脸部的亮光，但使用相关外挂软件，也可以完成验证。

“给手机刷机的目的就是获得手机操作的更多权限。”对于照片动态处理后通过人脸识别验证的原理，有两名黑产卖家表示，当APP 需要通过摄像头进行人脸验证时，用手遮挡摄像头，手机“外挂”就会启动，通过修改相关数据和设置，将提前做好的动态人脸视频导入到APP 中，便完成认证。

“真人录的视频通过率肯定高，照片处理的话要看天赋，不能保证你每一次验证都能通过，要看你制作的人脸动态视频是否细致。如果第一次验证失败，就多验证几次，后面可能就会通过。”一名黑产卖家表示，盗用他人信息进行APP 账号注册和验证属于违法行为，且国家打击力度较大，所以自己只卖软件和教学，并不会直接操作。

新京报记者使用该方法，在探探及智联招聘等平台上，都通过了人脸识别。

探探客服工作人员向新京报记者表示，如果发现个人身份信息被盗用认证，只能用户发现后向平台反映，之后用户需要向平台提供本人的身份信息进行审核，审核通过后平台会对已经认证账号进行封禁处理。对于探探平台人脸识别认证漏洞问题，他们将会把情况向上进行反馈。

智联招聘、陌陌等平台的客服人员均表示，对虚假的人脸识别目前没有很好的应对措施，之后会对该情况反馈处理。

个人信息贩卖后被非法使用的案例并不少。

在中国裁判文书网上，一起关于人脸识别验证的刑事判决书显示，从2018年7月份开始，被告人张某、余某等人以牟利为目的，使用其购买的公民个人身份信息注册支付宝账号，并使用软件将公民头像照片制作成公民3D 头像，从而通过支付宝人脸识别认证。

通过这种方式来获取支付宝提供的邀请注册新支付宝用户的相应红包奖励（包括邀请新人红包、通用消费红包、花呗红包等），而每个新注册支付宝至少可以获取28 元收益。截至案发，该团伙非法收集近2000 万条公民身份信息，共使用他人公民个人身份信息注册成功至少547 个通过人脸识别认证的实名支付宝账户，获利4 万元。

北京云嘉律师事务所律师赵占领表示，人的脸部特征信息是能够直接识别特定自然人的真实身份的信息，属于个人信息范畴，如果未经用户同意买卖个人信息是违法行为甚至是犯罪行为。

据民法典规定公民对个人信息享有民事权利，未经本人同意非法收集买卖他人信息会构成民事侵权。另外《刑法修正案（九）》规定了侵犯公民个人信息罪。买卖高度敏感的个人信息达到一定数量，符合司法两高的司法解释中所规定的立案标准的行为就涉嫌刑事犯罪。在这个过程中，无论买方还是卖方都涉嫌构成侵犯公民个人信息罪。

自然人的个人信息被他人非法买卖之后，用于一些违法甚至犯罪行为，那么他对此并不承担法律责任。但需要举证去证明个人信息是被他人非法获取并盗用的。个人信息方面的刑事案件比较多，公安机关每年都会抓获大量侵犯公民个人信息的犯罪嫌疑人。

信息来源：https://www.bjnews.com.cn/detail/161824564315305.html

骗子盯上手机 App“屏幕共享”功能，当心把你银行卡钱转光光

摘　要：近日，国家反诈中心发现，有不法分子利用腾讯会议的视频会议、共享屏幕等功能实施诈骗。

关键词：标签（诈骗，屏幕共享），技术问题（安全事件）。

内　容：国家反诈中心工作人员表示，此类诈骗中，骗子往往诱导受害人使用腾讯会议内的共享屏幕功能。一旦受害人使用此功能，即使诈骗分子不主动询问，也能看到受害人手机上的所有信息，包括输入密码时跳动的字符、收到的验证码等，从而转走受害人卡内资金。

受骗事主的过程实录：

2021 年1 月17 日14 时18 分，我接到“+65945673963”给我打来的电话，通话时长18 分37 秒，对方自称是天津市公安局户籍管理科的民警，说我有个从越南到哈尔滨太平国际机场的非法入境记录。

对方一再坚持，之后让我报警，并帮我转接到自称是哈尔滨市公安局的警察。接通后我把我的情况跟对方描述了一下，对方说帮我做登记。之后说我名下的民生银行的信用卡涉嫌洗钱，我跟对方说我没有办过民生银行的信用卡，对方称我的信息可能被冒用了。

对方称让我配合调查，然后告诉了我一个QQ 号让我添加。我添加完QQ 之后，对方给我发过来一张警官证照片。之后对方通过QQ 语音跟我说，让我下载腾讯会议，并在App 内加入其会议继续跟其聊天。

过程中，对方让我下载搜狗浏览器，并输入其告诉我的网址，并在该网址输入“110”。我按照对方说的操作之后就进入一个“官方网站”，之后对方让我在其中一个位置输入我的身份证号，我输完之后，显示我确实因为洗钱案被通缉了。之后对方让我在腾讯会议内开通共享屏幕，说要审核我的资金，并让我拦截所有的电话和短信。

2021 年1 月17 日16 时21 分11 秒从我工商银行的银行卡内向某银行账户内转账20000 元；

2021 年1 月17 日18 时34 分29 秒从我工商银行卡内向某银行账户内转账32900元；

2021 年1 月18 日9 时41 分16 秒从我工商银行卡内向某银行账户内转账11000元；

2021 年1 月18 日13 时20 分02 秒从我的工商银行卡内向某银行账户内转账5600 元；

……

都是通过手机银行转账。后来我发现自己被骗了。总共被骗89500 元。

反诈分析：

诈骗分子利用腾讯会议的共享屏幕功能可以第一时间直观地看到受害人在手机上的全部操作，包括登录手机银行账户转账的全过程，确保受害人完全在自己的掌控中。

受害人被诈骗分子成功操控，在2 天时间内，一次又一次向对方指定的账号转款。实际中还有不少没有资金的受害人在诈骗分子唆使下，甚至通过网络借贷借钱向对方指定账号转钱。

诈骗分子使用的账号都是购买而来的账号，虽然开户人和账号都清楚，却无法跟其本人建立关联，警方很难从这些账号找到幕后是谁，这就是当前为何要在全国推行“断卡”行动，严厉打击整治惩戒非法开办贩卖电话卡、银行卡违法犯罪活动的原因。

警方提示：报警的正确方式是拨打110，而不是按照来电人提供的信息去拨打电话号码，因为接听电话的可能就是犯罪嫌疑人的同伙。

诈骗分子发送伪造的警官证骗取受害人的信任，还诱导受害人使用腾讯会议与其

沟通，逃避监管。犯罪嫌疑人提供的是虚假网站，此类网站在用浏览器登录时出现不安全的提示，切勿轻易相信。

不要与陌生人开启屏幕共享功能，这样的操作会让你在陌生人面前毫无秘密可言。涉及私人信息，特别是银行卡密码、验证码时，一定要谨慎、谨慎再谨慎。如若被骗，请立即拨打110 报警。

信息来源：https://www.cnbeta.com/articles/tech/1116271.htm

运营商内鬼偷取公民信息赚近九千万，静默期号码也可注册出售

摘　要：近日，“运营商内鬼偷取公民信息非法获利8000 万”引发关注。记者注意到，近年来，内部人员窃取客户信息，偷开、倒卖账号事件并不鲜见，被出售并用于从事网络犯罪的公民信息高达数百万条，涉事金额至少在百万元以上。

关键词：标签（运营商、窃取信息、倒卖账号），技术问题（安全事件）。

内　容：近日，“运营商内鬼偷取公民信息非法获利8000 万”引发关注。南都记者注意到，近年来，内部人员窃取客户信息，偷开、倒卖账号事件并不鲜见，被出售并用于从事网络犯罪的公民信息高达数百万条，涉事金额至少在百万元以上。为何公民信息遭运营商“内鬼”偷取事件频频发生？如何解决？有专家表示，运营商“内鬼”往往是企业外部黑产的重点围猎对象，被“拉下水”的几率很高。专家建议，公司应明确个人信息分级分类的权限，特别要对批量化的导出下载等敏感事件进行预警，避免公司“内鬼”带来的风险。

运营商“内鬼”假借礼品兑换收集他人银行卡号等

据媒体报道，今年2 月，广州警方接到市民反映，某通讯营运公司“客服人员”来电以手机积分即将过期为由，要求客户尽快用积分兑换礼品。随后“客服人员”会用短信将链接发到用户手机里。而所谓的优惠换购，其实是不法之徒在偷偷收集公民个人信息。

广州市公安局民警称，当用户进入由“客服人员”提供的换购链接进行选购时，支付页面会要求用户提供手机号、银行卡号、身份证号等超过正常收集范围的信息。通过此手段掌握了公民个人信息后，不法分子就去注册大量微信账号，

出售给他人用于从事网络诈骗等犯罪活动。

据了解，该犯罪团伙共有9 名成员，其中5 人是某通信运营商公司的内部员工。自2020 年10 月至2021 年1 月，该团伙窃取公民信息，偷开、倒卖微信号250 万个，涉案972 宗，非法获利8700 万元。目前该团伙人员已全部落网。

运营商漏洞：“静默期”号码可注册、出售

记者梳理发现，运营公司内部人员窃取公民信息，偷开、倒卖账号已非首次。

据新华社报道，今年4 月2 日，宁波警方破获一起特大电信诈骗案。嫌疑人刘某作为华南某通信运营商网管中心负责人，利用运营商系统内权限将900 余万条号码出售给向非法短信接口团伙。该团伙用这些号码注册微信实施网络诈骗，涉及被骗资金400 余万元。

值得注意的是，一个手机号只能注册一个微信账号，不法分子是如何利用买来的号码成功注册大量新微信号的?

据办理该案件的广州民警介绍，运营商一般会提前半年从工信部门获得一批号码段，这批号段的手机号码未实名注册和激活，半年之后再推向市场销售。而运营商公司的“内鬼”们，通过内部渠道批量获取了这些未开通手机号的验证码，然后通过内部软件批量化注册大量微信号。

据悉，半年之后，这些被注册了微信的手机号销售到市场，于是出现有人开办新卡却发现已经被注册微信号的情况。独立电信分析师付亮对南都记者表示，偷取公民信息的“内鬼”是钻了运营商监管的“空子”。

“这些号码是前任机主抛弃后被运营商回收的，从运营商回收号码到再次售出，其中有4 个月以上的‘静默期’。在此期间该号码保存在运营商的仓库中无法使用。”付亮解释。他还指出，用处在“静默期”的号码注册微信号再贩卖出去，原则上并不涉及机主的用户隐私。因为不法分子相当于是用第三方信息注册的微信，与前机主无关，与再买到该账号的后机主也无关。这种行为的主要危害在于将账号出售给不法分子从事诈骗活动，从而造成财产损失。

“‘内鬼’抓住了运营商监管不严的漏洞，能在‘静默期’里通过内部渠道偷取到账号，并用内部软件批量注册。直到有用户反映，拿到的新号码已经被开过微信了，才引起运营商的重视展开自我复查。”付亮说。

专家：应明确权责，实现业务全流程可追溯

为什么公民信息遭运营商内鬼偷取事件频频发生？应如何解决？

对此，北京师范大学网络法治国际中心执行主任、博导、中国互联网协会研究中心副主任吴沈括总结了公民信息泄露事件中“内鬼”频发的三个原因。

第一，相比外部人员，他们和数据资产的距离更近，有业务方便，容易得手；第二，“内鬼”往往是企业外部黑产的重点围猎对象，被“拉下水”的几率更高；第三，个别企业设定的不合理业绩要求往往间接促使内部人员为了满足考核要求去铤而走险。

他还指出，这类问题的应对思路应是多方共治的多策并举。“首先，要推动企业内部建立清晰有效的‘定岗定责定人’制度，实现业务操作全流程的可追溯、可审计，确保‘数据-业务-人员’的严格匹配。其次，应鼓励支持建立面向社会大众的投诉举报激励机制，发挥社会力量的外部监督作用。再者，强化典型监管执法案例和司法裁判案例，以案说法，为数据业务运营和民众维权提供清晰的指引。”

从监管角度来看，付亮认为运营商应尽快填补“漏洞”。他强调，要定期对账号数据展开常规性核查，检测是否存在异常性使用现象，从根源上扼杀通过注册贩卖微信号实施网络诈骗的苗头。

此外，谈及“运营商内鬼偷取公民信息”一事，浙江垦丁律师事务所联合创始人麻策直言，个人信息的泄露最难防的并不在外部，而是内部泄露风险。公司在运营中应通过培训加强员工网络安全意识，明确个人信息分级分类权限，特别对批量化的导出下载等敏感事件进行预警，避免公司“内鬼”带来风险。

信息来源：https://www.secrss.com/articles/30764

美国银行自爆社会安全码 SSN 泄露，涉亿账户

摘　要：美国银行Capital One 在邀请第三方安全专家分析2019 的被盗数据时，发现入侵者可访问SSN 数据，特通知相关客户数据泄露事件。
关键词：标签（信息泄露），技术问题（安全事件）。
内　容：美国银行Capital One 已经通知了许多其他客户，告知他们的社会安全号码SSN 在2019 年7 月发生的数据泄露中暴露出来。

在美国，社会安全号码[又称社会保障号码]（Social Security number，SSN）是发给公民、永久居民、临时（工作）居民的一组九位数字号码，是依据美国社会安全法案（Social Security Act）205 条C2 中社会安全卡的记载。这组数字由联邦政府社会安全局针对个人发行。社会安全号码主要的目的是为了追踪个人的赋税资料，但近年来已经实际上成为美国的个人身份识别符(类似大陆身份证，具有唯一性)。

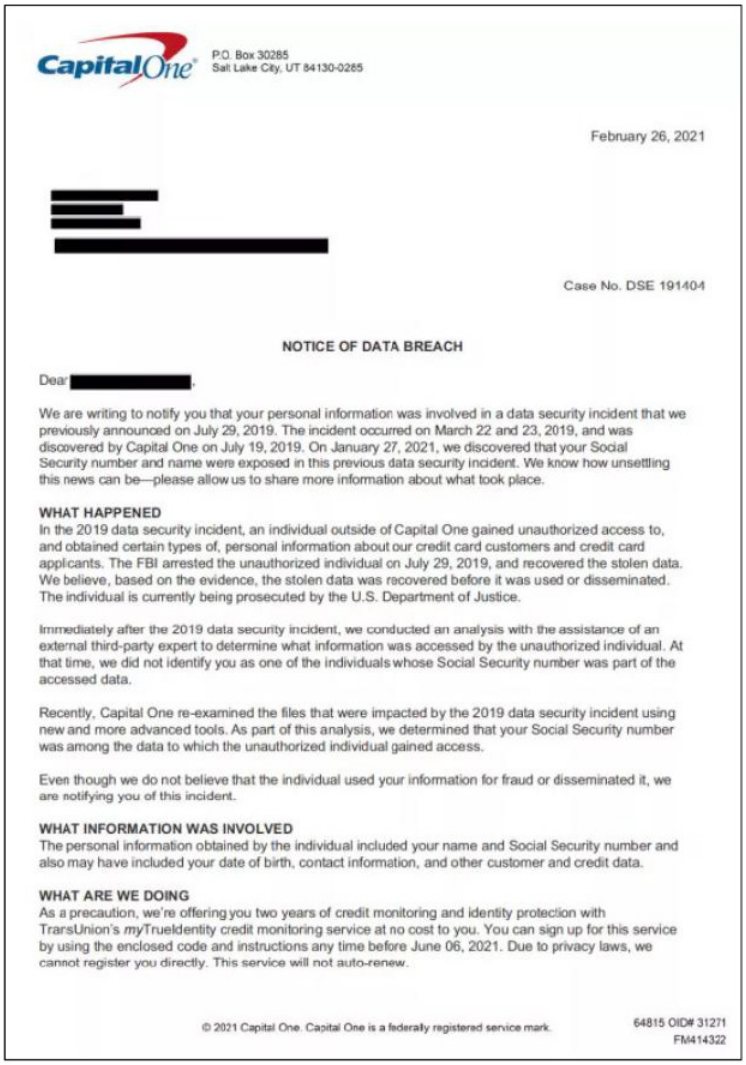
一名黑客入侵了Capital One 的系统，并从1.06 亿个Capital One 信用申请中获取了个人信息。执法部门因安全漏洞而逮捕了黑客佩奇·汤普森（Paige A.Thompson）。

佩奇·汤普森（Paige A. Thompson）是前Amazon Web Services 软件工程师，曾于2015 年至2016 年为Capital One 承包商工作。THOMPSON 在GitHub 上发布了有关Capital One 黑入的文章，她利用配置错误的Web 应用程序防火墙来访问数据。在2019 年7 月17 日，看到该帖子的GitHub 用户将这件事通知了Capital One，2019年7 月19 日，该金融机构发现了入侵并通知了FBI。

Capital One 立即修复了黑客利用的配置问题。佩奇·汤普森（Paige A. Thompson）在西雅图美国地方法院被控计算机欺诈和滥用。当时安全漏洞数据泄露发生在2019年3 月22 日至23 日，黑客访问了2005 年至2019 年之间申请信用卡的客户的信息。

“根据我们迄今为止的分析，此事件影响了美国约1 亿个人和加拿大约600万人。”Capital One 发布的新闻稿表示（目前已删除，原因未知）。“重要的是，没有信用卡帐号或登录凭据受到损害，并且超过99%的社会安全号码也没有受到损害。”“从2005 年到2019 年初，从消费者和小型企业申请我们的一种信用卡产品之时起，获得的最大信息类别就是有关消费者和小型企业的信息。

之前Capital One 一直没提到SSN 社会安全码被泄露，现在，Capital One 在第三方专家的帮助下分析2019 年安全漏洞期间被盗的数据时，发现入侵者可以访问这些客户的SSN 社会安全码，所以才下发了通知。



Capital One
P.O. Box 30285
Salt Lake City, UT 84130-0285

February 26, 2021

[redacted]

Case No. DSE 191404

NOTICE OF DATA BREACH

Dear [redacted],

We are writing to notify you that your personal information was involved in a data security incident that we previously announced on July 29, 2019. The incident occurred on March 22 and 23, 2019, and was discovered by Capital One on July 19, 2019. On January 27, 2021, we discovered that your Social Security number and name were exposed in this previous data security incident. We know how unsettling this news can be—please allow us to share more information about what took place.

WHAT HAPPENED

In the 2019 data security incident, an individual outside of Capital One gained unauthorized access to, and obtained certain types of, personal information about our credit card customers and credit card applicants. The FBI arrested the unauthorized individual on July 29, 2019, and recovered the stolen data. We believe, based on the evidence, the stolen data was recovered before it was used or disseminated. The individual is currently being prosecuted by the U.S. Department of Justice.

Immediately after the 2019 data security incident, we conducted an analysis with the assistance of an external third-party expert to determine what information was accessed by the unauthorized individual. At that time, we did not identify you as one of the individuals whose Social Security number was part of the accessed data.

Recently, Capital One re-examined the files that were impacted by the 2019 data security incident using new and more advanced tools. As part of this analysis, we determined that your Social Security number was among the data to which the unauthorized individual gained access.

Even though we do not believe that the individual used your information for fraud or disseminated it, we are notifying you of this incident.

WHAT INFORMATION WAS INVOLVED

The personal information obtained by the individual included your name and Social Security number and also may have included your date of birth, contact information, and other customer and credit data.

WHAT ARE WE DOING

As a precaution, we're offering you two years of credit monitoring and identity protection with TrarsUnion's *my*TrueIdentity credit monitoring service at no cost to you. You can sign up for this service by using the enclosed code and instructions any time before June 06, 2021. Due to privacy laws, we cannot register you directly. This service will not auto-renew.

© 2021 Capital One. Capital One is a federally registered service mark.

64815 OID# 31271
FM414322

信息来源：https://mp.weixin.qq.com/s/-qrj3R1kEUy4AEBVUrhXEg

NSFOCUS

漏洞聚焦

HTTP 协议栈远程代码执行漏洞（CVE-2021-31166）通告

发布日期 2021-5-12

一、漏洞概述

5 月12 日，绿盟科技监测到微软官方发布5 月安全更新补丁，其中修复了一个HTTP 协议栈远程代码执行漏洞（CVE-2021-31166），该漏洞存在于HTTP 协议栈(http.sys) 的处理程序中，未经身份验证的远程攻击者可通过向目标主机发送特制数据包来进行利用，从而在目标系统上以内核身份执行任意代码。CVSS 评分为9.8，微软表示此漏洞可用于蠕虫式传播。影响十分广泛，请相关用户更新补丁进行防护。

参考链接：

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-31166

二、影响范围

受影响版本

☐ Windows Server, version 20H2 (Server Core Installation)

☐ Windows 10 Version 20H2 for ARM64-based Systems

☐ Windows 10 Version 20H2 for 32-bit Systems

☐ Windows 10 Version 20H2 for x64-based Systems

☐ Windows Server, version 2004 (Server Core installation)

☐ Windows 10 Version 2004 for x64-based Systems

☐ Windows 10 Version 2004 for ARM64-based Systems

☐ Windows 10 Version 2004 for 32-bit Systems

三、漏洞防护

3.1 补丁更新

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

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

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

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

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

Nginx DNS 解析程序漏洞（CVE-2021-23017）通告

发布日期：2021-05-26

一、漏洞概述

近日，绿盟科技监测到Apache Shiro官方发布安全更新，修复了一个新的权限绕过漏洞（CVE-2020-17523）。当Apache Shiro与Spring结合使用时，攻击者可以构造特定的HTTP请求绕过身份验证访问后台功能；目前漏洞细节已公开，请相关用户采取措施进行防护。

Apache Shiro是一个功能强大且易于使用的Java安全框架，功能包括身份验证、授权、加密和会话管理。使用Shiro的API，可以轻松地、快速地保护任何应用程序，范围从小型的移动应用程序到大型的Web和企业应用程序。

参考链接：

https://shiro.apache.org/security-reports.html

二、影响范围

受影响版本

- ☐ NGINX 0.6.18 - 1.20.0

不受影响版本

- ☐ NGINX Open Source 1.20.1 (stable)
- ☐ NGINX Open Source 1.21.0 (mainline)
- ☐ NGINX Plus R23 P1
- ☐ NGINX Plus R24 P1

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：

http://nginx.org/en/download.html

3.2 其他防护措施

若相关用户暂时无法升级nginx至新版本，也可安装补丁进行修复：

http://nginx.org/download/patch.2021.resolver.txt

VMware VCenter Server 远程代码执行漏洞（CVE-2021-21985）通告

发布日期：2021-05-26

一、漏洞概述

5 月26 日，绿盟科技CERT 监测到VMware 官方发布安全公告，修复了VMware vCenter Server 远程代码执行漏洞（CVE-2021-21985）和vCenter Server 插件中的身份验证绕过漏洞（CVE-2021-21986）；由于vCenter Server中的插件Virtual SAN Health Check 缺少输入验证，通过443 端口访问vSphere Client(HTML5)的攻击者，可以构造特殊的数据包在目标主机上执行任意代码。无论是否使用vSAN，vCenter Server 都会默认启用该受影响的插件，CVSS 评分为9.8，请相关用户采取措施进行防护。

vCenter Server 是VMware 公司的一种服务器管理解决方案，可帮助IT 管理员通过单个控制台管理企业环境中的虚拟机和虚拟化主机。

参考链接：

https://www.vmware.com/security/advisories/VMSA-2021-0010.html

二、影响范围

受影响版本

- ☐ vmware vcenter_server < 6.5 U3p
- ☐ vmware vcenter_server < 6.7 U3n
- ☐ vmware vcenter_server < 7.0 U2b
- ☐ Cloud Foundation（vCenter Server）< 3.10.2.1
- ☐ Cloud Foundation（vCenter Server）< 4.2.1

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，对应产品版本的下载链接及文档如下：

版本号	下载地址	操作文档
vCenter Server 7.0 U2b	https://my.vmware.com/en/web/vmware/downloads/info/slug/datacenter_cloud_infrastructure/vmware_vsphere/7_0	https://docs.vmware.com/en/VMware-vSphere/7.0/rn/vsphere-vcenter-server-70u2b-release-notes.html
vCenter Server 6.7 U3n	https://my.vmware.com/en/web/vmware/downloads/info/slug/datacenter_cloud_infrastructure/vmware_vsphere/6_7	https://docs.vmware.com/en/VMware-vSphere/6.7/rn/vsphere-vcenter-server-67u3n-release-notes.html
vCenter Server 6.5 U3p	https://my.vmware.com/en/web/vmware/downloads/info/slug/datacenter_cloud_infrastructure/vmware_vsphere/6_5	https://docs.vmware.com/en/VMware-vSphere/6.5/rn/vsphere-vcenter-server-65u3p-release-notes.html
VMware vCloud Foundation 4.2.1	https://my.vmware.com/en/web/vmware/downloads/details?downloadGroup=VCF421&productId=1121&rPId=67576	https://docs.vmware.com/en/VMware-Cloud-Foundation/4.2.1/rn/VMware-Cloud-Foundation-421-Release-Notes.html
VMware vCloud Foundation 3.10.2.1	https://docs.vmware.com/en/VMware-Cloud-Foundation/3.10.2/rn/VMware-Cloud-Foundation-3102-Release-Notes.html#3.10.2.1	

3.2 临时防护措施

若相关用户暂时无法进行升级操作，也可参考官方给出的措施进行临时缓解：

https://kb.vmware.com/s/article/83829

微软 5 月安全更新多个产品高危漏洞通告

发布日期：2021-05-12

一、漏洞概述

5月12日，微软发布5月安全更新补丁，修复了55个安全漏洞，涉及Windows、Microsoft Office、Exchange Server、Visual Studio Code、Internet Explorer 等广泛使用的产品，其中包括远程代码执行和权限提升等高危漏洞类型。

本月微软月度更新修复的漏洞中，严重程度为关键（Critical）的漏洞有4个，重要（Important）漏洞有50个。请相关用户尽快更新补丁进行防护。详细漏洞列表请参考附录。

绿盟远程安全评估系统（RSAS）已具备微软此次补丁更新中大多数漏洞的检测能力（包括CVE-2021-26419、CVE-2021-31166、CVE-2021-31194、CVE-2021-28476 等高危漏洞），相关用户关注绿盟远程安全评估系统系统插件升级包的更新，及时升级至V6.0R02F01.2301，官网链接：http://update.nsfocus.com/update/listRsasDetail/v/vulsys。

参考链接：

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

二、重点漏洞简述

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

HTTP 协议栈远程代码执行漏洞（CVE-2021-31166）：

HTTP 协议栈（http.sys）存在远程代码执行漏洞，未经身份验证的远程攻击者可通过向目标主机发送特制数据包来利用此漏洞，从而在目标系统上执行任意代码。CVSS 评分为9.8，微软表示此漏洞可用于蠕虫式传播。

官方通告链接：

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-31166

Hyper-V 远程代码执行漏洞（CVE-2021-28476）：

虚拟机管理程序Windows Hyper-V 存在远程执行代码漏洞，CVSS 评分为9.9 。此漏洞使guest VM 可以强制Hyper-V host 的内核读取任意可能无效的地址，在某些情况下成功利用该漏洞的攻击者可以在Hyper-V 的服务器上运行二进制文件或在系统上执行任意代码。

官方通告链接：

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-28476

Microsoft SharePoint 远程代码执行漏洞（CVE-2021-28474/CVE-2021-31181）：

经过身份认证的攻击者可通过访问创建SharePoint 站点利用以上漏洞，实现在目标系统上执行任意代码。

官方通告链接：

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-28474

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-31181

OLE Automation 远程代码执行漏洞（CVE-2021-31194）：

此漏洞存在于Windows OLE中，攻击者搭建一个恶意的网站诱导用户访问，通过Web 浏览器调用OLE自动化利用此漏洞，从而实现远程代码执行。

官方通告链接：

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-31194

Exchange Server 安全功能绕过漏洞（CVE-2021-31207）：

此漏洞为2021 Pwn2Own 竞赛上发现的Exchange Server 漏洞之一，目前已公开披露，攻击者成功利用该漏洞可获取一定的服务器控制权限。

官方通告链接：

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-31207

三、影响范围

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

漏洞编号受影响产品版本

CVE-2021-31166：

Windows Server, version 20H2 (Server Core Installation)
Windows 10 Version 20H2 for ARM64-based Systems
Windows 10 Version 20H2 for 32-bit Systems
Windows 10 Version 20H2 for x64-based Systems
Windows Server, version 2004 (Server Core installation)
Windows 10 Version 2004 for x64-based Systems
Windows 10 Version 2004 for ARM64-based Systems
Windows 10 Version 2004 for 32-bit Systems

CVE-2021-28476：

Windows Server 2012 R2 (Server Core installation)
Windows Server 2012 R2
Windows Server 2012 (Server Core installation)
Windows Server 2012
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows Server 2008 for x64-based Systems Service Pack 2
Windows 8.1 for x64-based systems
Windows 7 for x64-based Systems Service Pack 1

Windows Server 2016 (Server Core installation)
Windows Server 2016
Windows 10 Version 1607 for x64-based Systems
Windows 10 for x64-based Systems
Windows Server, version 20H2 (Server Core Installation)
Windows 10 Version 20H2 for x64-based Systems
Windows Server, version 2004 (Server Core installation)
Windows 10 Version 2004 for x64-based Systems
Windows Server, version 1909 (Server Core installation)
Windows 10 Version 1909 for x64-based Systems
Windows Server 2019 (Server Core installation)
Windows Server 2019
Windows 10 Version 1809 for x64-based Systems
Windows 10 Version 1803 for x64-based Systems

CVE-2021-28474

CVE-2021-31181

Microsoft SharePoint Foundation 2013 Service Pack 1
Microsoft SharePoint Server 2019
Microsoft SharePoint Enterprise Server 2016

CVE-2021-31194

Windows 10 Version 2004 for x64-based Systems
Windows 10 Version 2004 for ARM64-based Systems
Windows 10 Version 2004 for 32-bit Systems
Windows Server, version 1909 (Server Core installation)
Windows 10 Version 1909 for ARM64-based Systems
Windows 10 Version 20H2 for x64-based Systems
Windows Server, version 2004 (Server Core installation)
Windows 10 Version 1909 for x64-based Systems
Windows 10 Version 1909 for 32-bit Systems
Windows Server 2019 (Server Core installation)
Windows Server 2019

Windows 10 Version 1809 for ARM64-based Systems
Windows 10 Version 1809 for x64-based Systems
Windows 10 Version 1809 for 32-bit Systems
Windows 10 Version 1803 for ARM64-based Systems
Windows 10 Version 1803 for x64-based Systems
Windows 10 Version 1803 for 32-bit Systems
Windows Server 2012 R2 (Server Core installation)
Windows Server 2012 R2
Windows Server 2012 (Server Core installation)
Windows Server 2012
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows Server 2008 for x64-based Systems Service Pack 2
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows RT 8.1
Windows 8.1 for x64-based systems
Windows 8.1 for 32-bit systems
Windows 7 for x64-based Systems Service Pack 1
Windows 7 for 32-bit Systems Service Pack 1
Windows Server 2016 (Server Core installation)
Windows Server 2016
Windows 10 Version 1607 for x64-based Systems
Windows 10 Version 1607 for 32-bit Systems
Windows 10 for x64-based Systems
Windows 10 for 32-bit Systems
Windows Server, version 20H2 (Server Core Installation)
Windows 10 Version 20H2 for ARM64-based Systems

Windows 10 Version 20H2 for 32-bit Systems

CVE-2021-31207

Microsoft Exchange Server 2019 Cumulative Update 8

Microsoft Exchange Server 2016 Cumulative Update 19

Microsoft Exchange Server 2016 Cumulative Update 20

Microsoft Exchange Server 2019 Cumulative Update 9

Microsoft Exchange Server 2013 Cumulative Update 23

四、漏洞防护

4.1 补丁更新

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

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

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

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

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

NSFOCUS

安全态势

互联网安全威胁态势

行业动态回顾

1. 新的Qlocker勒索软件每天攻击数百个QNAP NAS设备

【概述】

一种名为Qlocker的新型勒索软件正在肆虐，每天都会感染数以百计的QNAP网络连接存储(NAS)设备，它会控制硬盘，将用户的文件转移到有密码保护的7zip档案中，并要求用户支付550美元的赎金。

【参考链接】

https://therecord.media/new-qlocker-ransomware-is-hitting-hundreds-of-qnap-nas-devices-per-day/

2. 与中国有关的APT组织利用Pulse Secure VPN 0day漏洞入侵美国国防承包商

【概述】

根据FireEye和Pulse Secure发布的联合报告，两个黑客组织利用Pulse Secure VPN设备的一个0day漏洞，入侵了美国国防承包商和全球政府组织的网络。

【参考链接】

https://www.fireeye.com/blog/threat-research/2021/04/suspected-apt-actors-leverage-bypass-techniques-pulse-secure-zero-day.html

3. Joker恶意软件的目标是更多的Android设备

【概述】

Joker恶意软件已经通过华为官方应用商店AppGallery中的恶意应用程序，攻击了全球50多万台Android设备。Joker木马自2017年开始活跃，能够窃取受感染智能手机的短信、通讯录和设备信息。攻击者已在多个活动中使用了该恶意软件。

【参考链接】

https://www.inforisktoday.com/joker-malware-targets-more-android-devices-a-16450

4. Telegram平台在ToxicEye恶意软件活动中被滥用

【概述】

近期黑客通过将其代码嵌入称为ToxicEye的远程访问木马（RAT）中来利用流行的Telegram消息传递应用程序。ToxicEye恶意软件可以接管文件系统，安装勒索软件并从受害者的PC泄漏数据。

【参考链接】

https://threatpost.com/telegram-toxiceye-malware/165543/

5. Lazarus APT在BMP图像中隐藏恶意代码

【概述】

Lazarus是朝鲜的威胁组织之一，至少自2009年以来一直活跃，该组织的目标是美国、韩国、日本和其他几个国家。在最近的攻击活动中，Lazarus将带有恶意HTA对象的BMP文件嵌入到其Loader中，利用网络钓鱼攻击针对韩国。

【参考链接】

https://blog.malwarebytes.com/malwarebytes-news/2021/04/lazarus-apt-conceals-malicious-code-within-bmp-file-to-drop-its-rat/

6. SkidMap病毒利用Redis未授权访问漏洞攻击

【概述】

近期有攻击者利用Redis未授权访问漏洞攻击云服务器，安全专家判定为SkidMap病毒变种的攻击活动，同时发现事件影响云主机约数千台，受害主机已被攻击者控制沦为矿机，下载门罗币、莱特币、比特币挖矿木马，通过挖矿牟利，并可能造成机密信息泄露。

【参考链接】

https://s.tencent.com/research/report/1304.html

7. 黑客可入侵Cosori智能空气炸锅

【概述】

安全专家发现Cosori智能空气炸锅存在两个远程代码执行(RCE)漏洞。Cosori智能空气炸锅是一种具有智能功能的设备，可以用多种方法和设置烹饪食物。黑客可以通过Wi-Fi控制该设备，可以启动和停止烹饪，查看食谱指南和监控烹饪状态。

【参考链接】

https://blog.talosintelligence.com/2021/04/vuln-spotlight-co.html

8. 软件审计平台Codecov遭持续入侵

【概述】

软件审计平台Codecov遭黑客入侵，该事件可影响其2.9万名客户，并且引发大量公司连锁数据泄露。自2021年1月底黑客瞄准Codecov，利用Codecov的Docker映像创建过程中出现的错误，非法获得了其Bash Uploader脚本的访问权限并且进行了修改，这意味着攻击者可导出存储在Codecov用户的持续集成（CI）环境中的信息，最后将信息发送到Codecov基础架构之外的第三方服务器。

【参考链接】

https://about.codecov.io/security-update/

9. 黑客声称正在出售13 TB印度在线订单数据

【概述】

在最近泄露印度用户数据的黑客攻击中，印度一家颇受欢迎的披萨店Domino’s也遭受了网络攻击。据印度IT安全研究员Rajshekhar Rajaharia称，黑客获得了13TB的数据，其中包括1.8亿份订单信息，包括姓名、电话号码、支付信息和100万张信用卡信息。

【参考链接】

https://www.hackread.com/dominos-india-database-hacked-13-tb-data/

10. WhatsApp-Pink：通过群聊传播的恶意软件

【概述】

WhatsApp用户收到一种声称将应用程序的主题从其商标的绿色变为粉红色的链接，这是一种诱饵技术，一旦用户单击该链接，攻击者可入侵手机并窃取照片、短信、联系人等信息。

【参考链接】

https://www.hackread.com/whatsapp-pink-malware-spreads-group-chats/

11. Flubot间谍软件正在迅速传播

【概述】

Flubot间谍软近期非常活跃，尤其针对英国Android用户，受害人在收到一条短信后要求其安装跟踪应用程序的间谍软件，此间谍软件可以窃取受害者密码和其他敏感数据，还会向其设备的联系人发送相同的恶意短信。

【参考链接】

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

12. Purple Lambert新恶意软件

【概述】

Purple Lambert是卡巴斯基安全专家新发现的一个恶意软件，疑似是美国中央情报局CIA武器库的一部分。Purple Lambert具有模块化结构，侦听网络流量中特定的数据包、收集有关受感染系统的基本信息，还使攻击者能够执行其他有效负载。

【参考链接】

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

13. KimSuky新样本分析

【概述】

KimSuky是总部位于朝鲜的APT组织，至少2013年就开始活跃至今。该组织专注于针对韩国智囊团以及朝鲜核相关的目标。KimSuky别名包括Velvet Chollima, Black Banshee, Thallium, Operation Stolen Pencil等。近期发现

KimSuky组织多个新样本，其中包括以新冠疫情为诱饵的恶意样本。

【参考链接】

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

14. 2.5亿美国人的敏感家庭记录遭泄露

【概述】

2021年4月22日，一个名为Pompompurin的黑客泄露了一个包含超过2.5亿美国公民和居民的个人和敏感家庭数据的数据库，该数据库包含价值263 GB的记录，包括1255个CSV子文件，每个子文件包含20万个列表。可以确认的是泄漏的信息包含网络犯罪分子和国家支持的黑客的数据，详细信息包括全名、电话号码、电子邮件地址、出生日期、婚姻状况、性别、房屋费用、信用能力、家庭地址、地理位置、政治派别、拥有车辆数量、薪金和收入明细、房屋中的宠物数量、家庭孩子人数。

【参考链接】

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

15. Shlayer macOS恶意软件滥用零日漏洞绕过Gatekeeper功能

【概述】

苹果已经解决了macOS的零日漏洞，该漏洞已被Shlayer恶意软件利用，绕过了苹果的文件隔离、网守和公证安全检查并下载了第二阶段的恶意负载。Shlayer恶意软件背后的开发人员已成功设法通过其自动公证流程，使Apple批准了其恶意负载，从而可以在macOS上运行。

【参考链接】

https://ti.nsfocus.com/security-news/ruS7

16. Codecov供应链攻击危及多家科技巨头

【概述】

近日，软件审计公司Codecov的产品代码爆出供应链攻击，导致该公司数百个客户的网络遭遇非法访问。最初安全专家认为攻击仅影响Codecov，现在，该事件已被认定是供应链攻击，复杂性堪比SolarWinds供应链攻击。调查人员透露，这次袭击已经导致数百个Codecov客户的网络被访问。Codecov的客户规模

高达2.9万，其中包括许多大型科技品牌，例如IBM、Google、GoDaddy和HP，以及媒体发行商《华盛顿邮报》和知名消费品公司（宝洁）等等。

【参考链接】

https://ti.nsfocus.com/security-news/ruS8

17. Apple AirDrop中漏洞可能泄露用户的个人信息

【概述】

研究人员发现，苹果公司的无线文件共享协议Apple AirDrop存在隐私问题，可能会暴露用户的联系信息，如电子邮件地址和电话号码。此次发现的漏洞可能会影响仍然易受攻击的15亿多苹果设备的所有者。AirDrop是Apple Inc.的iOS和macOS操作系统中的专有临时服务，在Mac OS X Lion（Mac OS X 10.7）和iOS 7中引入，可以通过关闭方式在受支持的Macintosh计算机和iOS设备之间传输文件范围的无线通信。

【参考链接】

https://ti.nsfocus.com/security-news/ruS9

18. Naikon APT在针对军事组织的攻击中使用Nebulae新后门

【概述】

Naikon APT在针对多个东南亚军事组织的多次网络间谍活动中采用新的后门程序Nebulae，该后门能够收集LogicalDrive信息、操作文件和文件夹、从命令和控制服务器下载文件以及将文件上传到命令和控制服务器，列出/执行/终止受感染设备上的进程的能力。Naikon APT主要关注政府实体和军事组织，针对国家包括菲律宾、马来西亚、印度尼西亚、新加坡和泰国等。

【参考链接】

https://ti.nsfocus.com/security-news/ruS5

19. DDoS攻击使比利时政府网站离线

【概述】

近日，比利时公共部门互联网服务提供商Belnet遭受大规模分布式拒绝服务(DDoS)攻击，致使该国许多政府网站及相关服务瘫痪。根据Belnet的说法，攻击始于5月4日上午，影响了使用该公司服务的近200家机构和组织，包括公共部

门、大学和研究机构都部分或完全无法上网，同时网站几乎无法访问。DDoS攻击（包括大量目标设备被僵尸网络中的设备流量吞没而使目标不堪重负）通常是从目标中勒索金钱或掩盖其他攻击的手段。无论采取哪种方式，DDoS攻击都会使组织损失数百万美元以及名誉上的损失。

【参考链接】

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

20. WordPress反垃圾邮件插件可能会暴露网站用户数据

【概述】

在WordPress插件中发现的一个名为“垃圾邮件保护CleanTalk防火墙”的sql注入漏洞，可能会将用户的电子邮件、密码、信用卡数据和其他敏感信息暴露给未经身份验证的攻击者。100,000多个站点上已安装CleanTalk垃圾邮件防护，主要用于清除网站论坛上的垃圾邮件和垃圾评论。此漏洞编号CVE-2021-24295，CVSS为7.5。

【参考链接】

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

21. Dark Scammers团伙冒充WTO进行欺诈活动

【概述】

DarkPath Scammers团伙创建了一个由134个冒充世界卫生组织网站组成的分布式网络，以冒充WHO，诱骗用户访问欺诈性第三方网站，鼓励访问者回答一些简单的问题，以在世界卫生日之际赢得200欧元的奖金。欺诈活动每天吸引来自美国、印度、俄罗斯和其他国家的约200,000用户。

【参考链接】

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

22. N3TW0RM黑客团伙连环作案针对以色列

【概述】

最近，一个名为“N3TW0RM”（networm，网络蠕虫）的黑客团伙连环作案，利用勒索软件对一批以色列公司发动了攻击，其中包含H&M（以色列），物流公司Veritas Logistics。N3TW0RM分别从这两家公司获取了110GB和9GB数据，包含顾客、发票及雇员信息，还包含支付信息。

【参考链接】

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

23. 高通产品漏洞影响约30%的智能手机

【概述】

Checkpoint的研究人员在高通移动站调制解调器中发现了一个缓冲区溢出漏洞，追踪为CVE-2020-11292，攻击者可以利用该漏洞在智能手机上触发内存损坏和执行任意代码。

移动基站调制解调器(MSM)是高通公司在20世纪90年代早期设计的芯片(SoC)系统，多年来，安全研究人员经常针对该组件寻找远程攻击移动设备的新方法，例如通过发送短信或精心制作的无线电包。

【参考链接】

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

24. ShinyHunters泄露印度婚礼门户网站WedMeGood的数据库

【概述】

臭名昭著的黑客ShinyHunters泄露了像Animal Jam、Mashable、

Upstox和WattPad等公司的数据库，近期又发生一起高调的数据泄露事件。ShinyHunters已转储了属于WedMeGood的数据库，WedMeGood是印度颇受欢迎的婚礼策划平台，该平台负责婚礼的各个方面，从寻找场地到摄影师，再到布置婚礼服装。此次泄露41.5GB的敏感数据，其中包括全名、性别、城市、电话号码、电子邮箱地址、密码、预定线索、上次登录日期、账户创建日期、Facebook账号和Airbnb假期信息。

【参考链接】

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

25. Exim修复了邮件传递代理中的21个漏洞

【概述】

Exim是最常用的消息传输代理之一，它已发布了针对21个漏洞的补丁程序，其中包括11个本地漏洞和10个远程代码漏洞，并且会影响从2004年开始的所有版本的Exim服务器，这些补丁程序可能使成千上万的用户面临遭受攻击的风险。

【参考链接】

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

26. 超过40款应用程序被发现泄漏AWS密钥

【概述】

近期发现40多款应用程序（累计下载量超过1亿次），这些应用程序中嵌入了硬编码的Amazon Web Services（AWS）专用密钥，从而其内部网络和用户数据面临网络攻击的风险。AWS密钥泄漏已在一些主要应用程序中发现，例如Adobe Photoshop Fix，Adobe Comp，Hootsuite，IBM的Weather Channel以及在线购物服务Club Factory和Wholee。

【参考链接】

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

27. Ghostwriter攻击活动针对北约盟国

【概述】

Ghostwriter虚假信息攻击正在进行中，目标针对波兰、立陶宛和拉脱维亚的公民，主要目的是破坏对北约在东欧行动的信心，并引起包括美国和加拿大在内的其他国家部署士兵的反对。此次攻击活动归因于UNC1151组织，该组织是从事政府活动的网络间谍活动，从事凭证收集和恶意软件活动。

【参考链接】

https://ti.nsfocus.com/security-news/ruS4

28. 数百万Dell设备易受更新驱动程序缺陷的攻击

【概述】

Dell已修复驱动程序中的漏洞，该驱动程序已在数百万台笔记本电脑、平板电脑和台式机中提供。漏洞编号CVE-2021-21551，CVSS评分8.8。Dell已经在BIOS更新实用程序中包装了易受攻击的驱动程序dbutil_2_3.sys?。

【参考链接】

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

29. 美国最大燃油管道运营商遭网络攻击

【概述】

当地时间2021年5月9日，美国宣布进入国家紧急状态，原因是当地最大燃油管道运营商遭网络攻击下

线。美国最大的成品油管道运营商Colonial Pipeline在当地时间周五（5月7日）因受到勒索软件攻击，被迫关闭其美国东部沿海各州供油的关键燃油网络。

【参考链接】

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

30. 从油气管道公司被勒索，剖析DARKSIDE类组织对关键信息基础设施的影响及应对措施

【概述】

当地时间5月7日，美国最大的燃油管道运营商Colonial?Pipeline因受到勒索软件攻击被迫关闭了其美国东部沿海各州供油的关键燃油网络。此次勒索攻击使美国三个区域受到了断油的影响，共涉及17个州。5月9日，联邦汽车运输安全管理局（FMCSA）发布区域紧急状态声明，放宽了17个州和哥伦比亚特区对携带汽油、柴油、喷气燃料和其他精炼石油产品运输司机的服务时间规定。允许他们额外或更灵活的工作时间，以减轻管道中断导致有关燃料短缺的影响。BBC称多个消息来源证实，是一个名为DarkSide的网络犯罪团伙进行了此次勒索攻击。该团伙在周四入侵了Colonial的网络，并窃取了近100GB的数据，以威胁如果不在周五前支付赎金会将其泄漏到互联网。

【参考链接】

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

31. ICEDID针对金融机构的最新活动

【概述】

前段时间，绿盟科技伏影实验室捕获到一批相似度十分接近的样本。我们对这批样本进行了持续跟踪，并进行了全面的分析，发现其为ICEDID最新活动，本次活动中攻击者新构了一种恶意软件加载器Gziploader。该类样本在2021年3月中旬开始大量活跃，样本数量众多，主要通过垃圾邮件或钓鱼邮件的方式进行传播。

【参考链接】

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

32. Operation TunnelSnake利用后门进行间谍活动

【概述】

Operation TunnelSnake高级持续威胁活动正在进行中，该活动使用一个名为Moriya的Windows rootkit部署一个被动后门来监视受害者，在受害组织内部面向公众的服务器上开展的活动是为了监视网络流量，并向受影响的主机发送命令。据卡巴斯基报道，攻击者使用的是特权植入物，这些植入物通常被用作驱动程序。Moriya Rootkit最初于2019年10月和2020年5月在亚洲和非洲的区域外交组织网络上被发现。研究人员说，这些感染在目标网络中持续了几个月。

【参考链接】

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

33. Babuk勒索软件团伙泄露华盛顿警方数据

【概述】

最近由Babuk勒索软件团伙泄露的文件包含26GB的记录，泄露的数据来自华盛顿警察局，该警局愿意支付10万美元已防止被盗数据泄露，未满足Babuk勒索软件团伙要求的400万美元赎金。Babuk勒索软件团伙从该部门的网络中窃取了近250 GB的未加密文件，该数据库包括情报简报、调查报告、纪律处分和逮捕数据。

【参考链接】

https://ti.nsfocus.com/security-news/4qYG0

34. Android恶意软件冒充Chrome应用传播病毒

【概述】

针对Android设备的攻击会自我传播，并可能造成一系列损害。在过去几周内，一个冒充Chrome应用的新Android恶意软件已经蔓延到数十万人。这款恶意应用程序被用作一场复杂网络攻击活动的一部分，威胁行为者从受感染设备每周发送超过2,000条的SMS消息，旨在利用移动网络钓鱼窃取个人感敏信息和凭证。

【参考链接】

https://ti.nsfocus.com/security-news/ruT9

35. 黑客针对使用Adobe Reader的Windows用户

【概述】

Adobe 2021年5月的安全更新在Experience Manager、InDesign、Illustrator、InCopy、Adobe Genuine Service、Acrobat和Reader、Magento、Creative Cloud Desktop、Media Encoder、Medium和Animate中至少解决了43个CVE。上述缺陷中的5个是通过ZDI程序报告的。其中一个问题被追踪为CVE-2021-28550，它是一个影响Adobe Reader for Windows的免费使用后内存损坏缺陷，该缺陷已在有限的攻击中被广泛利用。

【参考链接】

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

36. Avaddon勒索软件攻击增加

【概述】

据联邦调查局FBI和澳大利亚网络安全中心ACSC称，攻击者正在使用Avaddon勒索软件攻击美国、澳大利亚和其他地方的不同组织。这些机构警告说，正在进行的活动针对制造商、航空公司、医疗保健机构和其他机构。Avaddon勒索软件最初是在俄语黑客论坛上作为一种勒索软件即服务产品进行推广的，随后被用于网络犯罪活动，该勒索软件通过网络钓鱼和恶意垃圾邮件活动进行传播，这些活动提供了恶意的JavaScript文件。

【参考链接】

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

37. WallStreetBets论坛成员因加密货币诈骗损失200万美元

【概述】

WallStreetBets (WSB)论坛的部分成员成为加密货币诈骗活动的受害者，威胁行为者诱使购买一种称为WSB Finance的新型加密货币代币，要求将Binance Coins（称为BNB）或以太币发送至指定加密货币钱包，然后与Telegram上的“代币机器人”联系，接收WSB Finance，接下来在Telegram上告诉已经汇款的人，由于机器人问题，需要再次汇出相同的金额，否则将会失去最初的投资?。此次诈骗活动是一些用户蒙受200美元的损失。

【参考链接】

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

38. 恶意垃圾邮件活动使用Hancitor下载Cuba勒索软件

【概述】

威胁行为者正积极使用Hancitor来部署Cuba勒索软件，从而初步进入目标网络，一旦受害者的设备被成功入侵，如果赎金要求没有得到满足，就会利用Cuba勒索软件专门的数据泄露网站发布被泄露的数据。古巴勒索软件至少从2020年1月起就开始活跃，其运营商拥有DLS网站，他们在该网站上发布了拒绝支付赎金的受害者的敏感数据，主要来自自航空、金融、教育和制造业公司的敏感信息。

【参考链接】

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

39. XcodeGhost恶意软件影响1.28亿iOS用户

【概述】

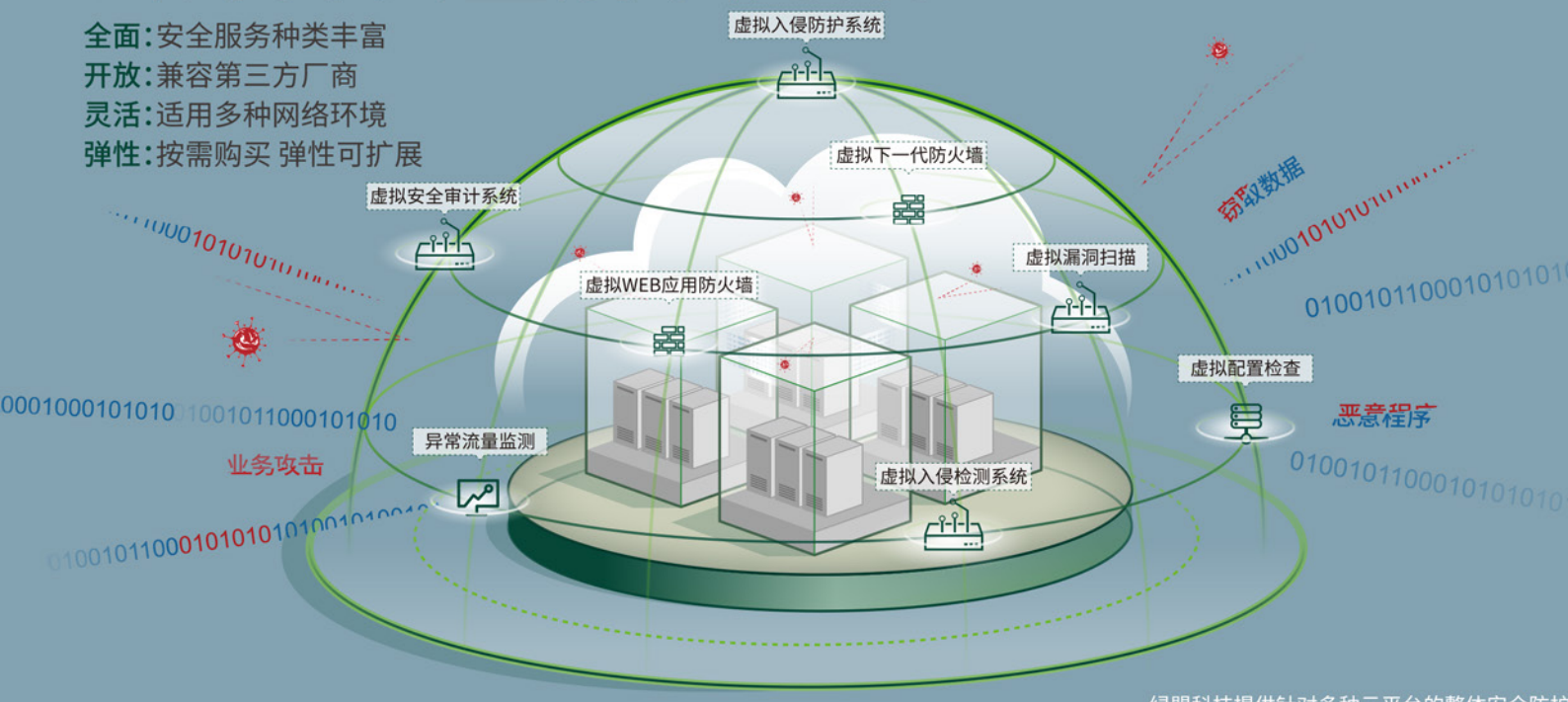
自2015年以来一直活跃的臭名昭著的XcodeGhost恶意软件大规模感染已影响了1.28亿iOS用户。大规模黑客入侵是由于App Store中提供了4000个恶意应用程序，结果发现这些应用程序包含XCodeGhost恶意软件。威胁行为者使用XcodeGhost来接管受害者的移动设备，能够窃取凭据、劫持用户的流量并窃取iCloud密码。

【参考链接】

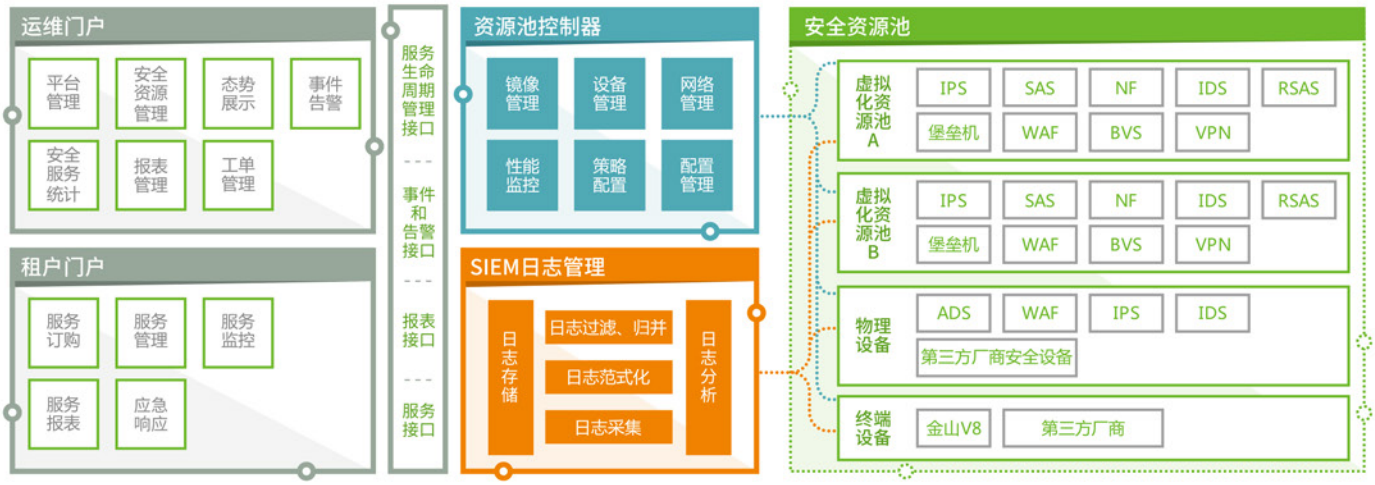
https://ti.nsfocus.com/security-news/ruTc

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/