简译版

新冠疫情将从五个方面改变网络安全

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	Five ways COVID-19 will change cybersecurity		
原文作者	佐勒菲卡尔·拉姆赞（Zulfikar Ramzan）	**原文发布日期**	2020年12月21日
作者简介	佐勒菲卡尔·拉姆赞是RSA首席数字官。		
原文发布单位	Help Net Security		
原文出处	https://www.helpnetsecurity.com/2020/12/21/covid-19-cybersecurity/		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公有方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。		

新冠疫情将从五个方面改变网络安全

佐勒菲卡尔·拉姆赞

2020 年 12 月 21 日

2021 年的主要故事不会再是新冠疫情，而是其疫苗。截至今年 11 月，三种有效、有前景的疫苗正在研发中，新冠肺炎（及其治疗方法）将继续对我们生活的几乎所有方面带来重大影响。

对网络安全领域来说，疫情的影响尤其严重。2020 年，安全行业发生了了重大的转变，我们仍在不断适应中。在 2021 年，新冠疫情及其疫苗将从下述五个方面改变网络安全领域。

1. 重返办公室将带来复杂的网络安全挑战

明年，我们有可能会开始接种疫苗，一些员工很可能会返回办公室办公。大量员工返回办公室，将是 2021 年第一个重要的网络安全趋势，这会带来诸多复杂的挑战。

去年，许多企业迅速转向远程办公以确保业务连续性。截至 6 月，美国全职在家办公的员工数量激增到 42%。疫情使首席信息安全官（CISO）措手不及：在一些重要的情况下，安全团队必须在周末进行远程办公，以遵守当地的“在家办公”命令。

我理解“在家办公”这一决策的必要性，但这些措施将在 2021 年产生严重的后果。

2. CISO 将进行裁员并重建安全策略

明年，CISO 不得不承受他们在 2020 年做出的（或被迫做出的）“远程办公决策”的后果。他们的首要任务之一是改善年初仓促之下确定的远程办公策略，增强远程办公能力。

这种趋势已经开始出现——“零信任”解决方案逐渐受到企业的青睐。这是一种新兴的安全策略，该策略假设一切活动（包括网络、主机、应用程序和服务）都是恶意的。截至 11 月，有 60%的企业报告说他们正在加速进行零信任项目。这在很大程度上归功于 CISO 和 CSO 的裁员决策，以及采取了更加谨慎的方法来确保运营安全。

安全领导者应帮助企业顺利部署零信任策略。他们将意识到，零信任策略必须结合一套完整的功能，包括但不限于：强大的多因子身份鉴别、全面的身份监管和生命周期、有效的威胁检测，以及通过所有关键数字资产的全面可见性促进威胁响应。

数字化转型导致企业数字复杂性日益增长，为了解决这一问题，领先的安全领导者将采用“扩展的检测和响应”（XDR）解决方案，力争在其网络、端点、云资产和数字身份上实现统一的可见性。

3. 接种疫苗的员工携带受感染设备返回办公室

当员工返回办公室办公时，2020 年“紧急转向远程办公”的后果将会凸显。2021 年，越来越多的员工将会接种疫苗，但他们的设备和应用仍会受到感染。6 月，研究人员报告称，源自移动端点的攻击和数据泄露事件激增。

随着更多受感染设备重新进入办公室，与公司资产和系统连接，我们将看到草率的远程办公策略带来的严重影响。

4. 攻击者瞄准 SaaS 应用和云服务

同样，由于许多企业在 2020 年开始依赖远程员工，并通过 SaaS 应用和云服务扩大业务范围，因此攻击者很可能会优先考虑这些目标并找到利用它们的新方法。他们可能会采用两步走的方法：（1）感染终端用户；（2）连接到这些人可以访问的云服务。

5. 攻击者利用伪造的疫苗信息执行网络钓鱼攻击

或许最糟糕的是，2021 年疫苗的可用性将为攻击者提供新的攻击渠道。他们会向攻击目标发送伪造的疫苗信息，执行网络钓鱼攻击。去年疫情期间，网络犯罪分子向我们展示了他们不会放过任何可利用的机会——他们利用疫情相关的信息执行网络钓鱼、木马和流氓应用程序攻击。

攻击者能够迅速调整策略，利用危机：他们会从之前的“疫情救灾供应”和“合同跟踪应用”攻击转向与疫苗相关的网络钓鱼攻击。他们的目标将会是个人消费者以及开发、分发、研究和管理疫苗的组织。

这些攻击可能会损害公众对疫苗的信心，并削弱其效用。鉴于这些疫苗的广泛采用对确保公众健康至关重要，社交媒体公司需要采取更强有力的措施来遏制伪造信息攻击。Facebook、Twitter 和 YouTube 最近的一项对抗疫苗阴谋的联盟就是一个良好的开端，他们必须迅速采取行动，以举报、驳斥和删除伪造信息。

希望企业已经吸取了一些教训

去年，安全行业面临着异常严峻的挑战。网络安全专家努力调整工作，开发新的解决方案，帮助各地的企业继续向依赖他们的人们提供服务，我为他们感到骄傲。

2020 年是残酷的一年，也是很有价值的一年。疫情证明了我们的力量，同时也暴露了我们的一些缺陷和弱点。

希望企业能够从中吸取教训。他们应意识到，下一个颠覆性威胁即将到来。现在，仅仅确保人身安全已经不够了。

从这个意义上讲，2020 年将我们团结了起来，我们朝着一个共同的事业发挥了人类智慧的力量。疫情爆发后，人们迅速开发了新颖的疗法，创建了新的测试方法，加速了疫苗的研究，确定了批量生产个人防护设备的方法，并设计了新的通风机。

我希望，企业关注与疫苗相关的网络安全挑战，更深入地了解攻击者的手段，以应对 2021 年及以后的攻击。

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，始终坚持自主先进的能力导向，依托下一代威胁检测引擎等先进技术和赛博超脑大平台工程能力积累，研发智甲、探海、镇关、捕风、追影、拓痕等系列产品，为客户构建端点防护、流量监测、边界防护、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报的有机结合，协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行，赋能客户筑起可对抗高级威胁的网络安全防线。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全企业、IT 企业选择安天作为检测能力合作伙伴，目前，安天的威胁检测引擎为全球超过八十万台网络设备和网络安全设备、超过十七亿部智能终端设备提供了安全检测能力。安天的移动检测引擎获得国际知名测试机构颁发的 2013 年度权威评测奖项。

安天是中国应急响应体系中重要的企业节点，在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体（如 APT 组织）及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，通过深度分析高级网空威胁行为体的作业能力，安天建立了以实战化对抗场景为导向的能力体系。

安天被行业管理机构、客户和伙伴广泛认可，已连续六届蝉联国家级安全应急支撑单位，是中国国家信息安全漏洞库六家首批一级支撑单位之一，亦是国家网络与信息安全信息通报机制技术支撑单位，国家信息安全漏洞共享平台成员单位。

2016 年 4 月 19 日，在习近平总书记主持召开的网络安全和信息化工作座谈会上，安天创始人、首席架构师作为网络安全领域发言代表，向总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了安天总部，并对安天人说，“你们也是国家队，虽然你们是民营企业”。

安天实验室更多信息请访问： http://www.antiy.com（中文）
http://www.antiy.net（英文）
安天企业安全公司更多信息请访问： http://www.antiy.cn
安天移动安全公司（AVL TEAM）更多信息请访问： http://www.avlsec.com