简译版

2021 年网络安全趋势和新兴威胁

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	Cybersecurity Trends and Emerging Threats in 2021		
原文作者	道格拉斯·邦德鲁（Douglas Bonderud）	**原文发布日期**	2021 年 3 月 3 日
作者简介	道格拉斯·邦德鲁是一位自由撰稿人。		
原文发布单位	Security Intelligence		
原文出处	https://securityintelligence.com/articles/cybersecurity-trends-and-emerging-threats-2021/		
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。		

2021 年网络安全趋势和新兴威胁

道格拉斯·邦德鲁

2021 年 3 月 3 日

2021 年带来了更加光明之未来的希望——但是前路漫漫。在本文中，我们将深入探讨 2021 年会导致严重风险的五种网络安全趋势，并提供实用建议以帮助各实体降低总体风险。

2021 年第一季度，企业在网络安全方面走到了十字路口——他们可能会将部分员工调回办公室办公，同时还要管理远程办公的风险和回报，这给攻击者打开了一扇攻击之门。从常见的攻击向量到新兴威胁，攻击者一直在寻找规避 IT 告警和防御措施，以及利用新漏洞的方法。

2020 年的网络安全趋势奠定了基础

2020 年的一些威胁并不新鲜。根据 IBM Security X-Force 的数据，截至 2020 年 9 月修复的攻击活动中，25%与旧的勒索软件有关。

此外，居家办公为攻击者提供了另一种攻击向量，带来了新的信息安全威胁。从特权凭证泄露到个人和专业网络的混用，攻击者总能迅速加以利用，将其作为攻击入口点。

与此同时，IT 团队通过改善身份和访问管理（IAM）、增强数据加密和转向托管服务等方法，来防御潜在漏洞和减少新风险。

2020 年的网络安全趋势为 2021 年奠定了基础。公司和网络犯罪分子都已了解 IT 行业的“新常态”，接下来会发生什么呢？

居家办公攻击

2021 年的第一个重要网络安全趋势始于 2020 年。虽说居家办公并非今年新出现的威胁，但攻击者同时攻陷多个不安全的家庭网络，以大规模破坏关键系统和服务是迟早的事。这说得通——很多员工不仅将家庭宽带用于个人用途，还将其用于办公用途，这导致公司的攻击面大大增加。

要想解决这一问题，企业应部署身份识别与访问管理（IAM）解决方案，以及能够智能分析用户活动、资源请求和公司联系习惯的工具，以便在保证安全的情况下精简登录过程。

一旦检测到潜在问题，则需要进行额外的身份验证。

暴力破解攻击

暴力破解攻击重受攻击者青睐。他们认识到，分布式拒绝服务攻击（DDoS）在摧毁公司网络方面颇具潜力。2020 年下半年，DDoS 攻击增加了 12%，尤其是那些使用简单服务交付协议（SSDP）和简单网络管理协议（SNMP）的攻击。

通过使用僵尸网络群，攻击者能够发送大量 IP 请求，导致企业网络崩溃，从而减慢企业的响应甚至完全拒绝服务。SNMP 协议连接并管理常见的公司设备，包括调制解调器、打印机、交换机、路由器和服务器，因此 SNMP 漏洞利用更加令人担忧。通过攻击 SNMP 服务，攻击者能够跨越企业防火墙，使所有企业服务都面临风险。

在 2021 年，要想对抗 DDoS 威胁，企业需要敏捷、适应性强的工具，以便在此类攻击发生时及时进行检测、隔离和修复。

无文件恶意软件

2021 年，无文件恶意软件和勒索软件攻击将会继续困扰企业。这些威胁旨在绕过熟悉的检测控制，并“靠山吃山地”（使用公司网络中已存在的受认可平台或软件工具）渗透到关键系统中。

通过这种方法，攻击者可以绕过常见的检测方法（扫描恶意文件附件或对新创建文件进行分类）。此外，使用现有系统工具意味着攻击者不必自己设计攻击框架，这减少了他们开发恶意软件所需的时间。2021 年，攻击者很可能会使用无文件恶意软件来感染服务提供商而非特定群体。之后，他们就可以使用现有的基础架构来攻击下游客户端。

要想应对此类攻击，保持警惕是关键。企业可以通过清点网络安全措施来防御无文件威胁，重点是及时更新软件和系统，以确保安全工具按预期运行。此外，企业应部署有效的访问控制措施（例如多因子身份鉴别[MFA]），以降低潜在风险。

旧的网络安全趋势仍然存在

即使攻击者开发了新威胁，勒索软件、木马和僵尸网络等旧威胁仍然存在。为了应对这些熟悉的威胁，企业必须确保员工拥有迅速发现这些攻击所需的工具和知识。例如，企业应对员工开展关于常见攻击向量（例如恶意电子邮件附件和链接）的培训。此外，企业还应监

控员工电子邮件账户，提醒员工注意安全标准，并在检测到潜在威胁时自动通知员工。

网络钓鱼攻击

2021 年最大的新闻是新冠疫苗。人们经常搜索疫苗接种信息，包括疫情的当前状态、何时何地分发疫苗、谁被批准获得疫苗等。这将影响 2021 年的网络安全趋势。因此，公司必须做好准备以应对相关的网络钓鱼活动。这类钓鱼信息会立即引起读者的兴趣，因此非常危险。

我们已经检测到利用疫苗信息的钓鱼攻击。英国国家卫生局（National Health Service）最近发布了有关假疫苗接种预约电子邮件的警告。IBM X-Force 发现了一起针对疫苗供应方的攻击，该攻击旨在破坏疫苗冷链。

这类攻击增加的原因很简单。尽管我们经常谈论此类攻击，且企业 IT 安全团队不断努力，但网络钓鱼诈骗仍然很有效。居家办公期间，此类攻击更加令人担忧。居家办公的员工不仅要应对严重的生活和工作压力，还要应对大量的钓鱼邮件，被此类攻击攻陷也不足为奇。

为了应对这种攻击，企业应改进身份管理。他们要确认，只有正确的人能够在正确的时间正确地访问正确的资源，这样可以降低上钩的风险。此外，创建安全文化也很重要——企业应鼓励员工上报其发现的可疑内容。这样一来，在与网络钓鱼攻击作斗争时，企业就能缓慢而稳定地取得胜利。

使用经过验证的工具应对当今的威胁

随着企业朝着新常态迈出第一步，攻击者也在试图利用这一趋势。为了应对当今的网络安全趋势，包括新的攻击向量和旧的威胁框架，企业需要制定攻击防御计划，将新兴工具与久经考验的最佳实践结合起来。

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