20210123-周报总结

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **小论文进展：** | **🞎阅读文献** | **🞎做实验** | **🞎撰写中** | **🗹其它** |
| **一、本周工作**   1. 看了综述性论文《2021年网络安全发展趋势预测》，了解下前沿知识，关注下2021网络安全的发展趋势。 2. 复习下Python的语句内容，防止遗忘。在Windows下搭建了个Python环境，安装下pycharm。在Windows平台，过一下之前的代码。 | | | | |
| 1. **下周计划** 2. 继续看python内容，主要是函数、文件和类的相关问题，针对性看一下。 3. 看一下，其他的综述性论文，包括外文和中文的。 | | | | |
| 1. **本周工作摘要**   《2021年网络安全发展趋势预测》内容归纳：  由于今年COVID-19疫情大流行、全球经济受损等原因，数据泄露、网络渗透、大量数据盗窃和销售、身份盗窃和勒索软件频频爆发。  本篇摘自全球领先的权限访问管理（PAM）供应商BeyondTrust公司针对2021年网络安全趋势做出的年度预测。此份年度网络安全预测主要基于技术分享、恶意攻击者倾向、文化以及过去数十年的综合经验。  预测1：网络时间协议攻击  网络时间协议（NTP）与基于时间的Windows服务器等协议已经成为黑客群体攻击的新目标。组织大多使用这些协议控制各项事务的时间安排。一旦时间发生问题，从许可服务器到批处理事务都有可能遭遇失败，并导致互联网及组织后端流程中的某些关键基础设施面临拒绝服务攻击。  预测2：机器学习训练数据污染  企业正越来越广泛地利用机器学习去制定自动化决策，攻击者也在着力从中寻求新的可利用因素。恶意攻击者在窃取到原始训练数据副本之后，即可将污染数据注入训练池以操纵由此生成的模型，最终建立起一套与预期训练目标不符的系统。由于整个下游应用程序都将以模型为基础进行自动处理，因此此类操纵造成的影响将被成倍放大，最终破坏掉其他合法处理数据的完整性。  预测3：AI武器化的泛滥  恶意攻击者将利用机器学习（ML）加速针对网络及系统的攻击。机器学习引擎将使用成功攻击中的数据进行训练，借此识别防御体系中的模式，快速查明类似系统/环境中存在的漏洞。以此为基础，所有后续攻击数据都可作为素材继续训练网络攻击引擎。通过这种方式，攻击者能够更快、更隐密地清理攻击痕迹，确保每一次攻击尝试只涉及更少的漏洞，借此避免大面积尝试被安全工具所发现。  预测4：Deepfake全面爆发  Deepfake浪潮很可能全面袭来，令我们难以判断聊天窗口或者视频通话的另一端到底是不是本人或者真人。例如，您可能很快看到由前任总统甚至是已故亲人录制的视频内容。这可能会扰乱我们的认知，更难以做出准确可靠的判断。  预测5：远程办公将成为黑客第一大攻击目标  新的攻击因素可能将矛头指向远程工作人员以及远程访问路径。网络罪犯将不断发起社会工程攻击，并尝试入侵个人设备、进而横向移动至企业网络。社会工程攻击的主要形式为网络钓鱼，具体包括通过电子邮件、语音、文本、即时消息乃至第三方应用程序窃取敏感信息。根据预测，到2021年，偏远地区的办公人员/设备将成为第一大攻击目标。  预测6：数据隐私合规严重过载  2020年，欧盟法院推翻了由欧盟-美国共同制定的治理保护条例“隐私盾（Privacy Shield）”。展望2021年，企业需要努力适应新的、更为严苛的数据隐私法规扩展，同时适应法院系统有可能推翻既定政策的新情况。跨国企业必须快速适应并重新设计客户数据处理方式。而在同一国家内多个州间开展业务的企业，也需要考虑如何遵循各州数据管理规定、如何在集中位置处理数据，并围绕数据删除及违规通报制定新的程序性方法。  预测7：社交媒体攻击因素将在社交隔离时代下继续扩散  除了针对个人之外，攻击者还将利用社会工程手段攻击企业目标。攻击者可能破坏身份认证与验证机制，借此实施社交媒体入侵。恶意二维码或简写URL亦可能被用于混淆恶意网站。由于社交媒体在发布、验证以及控制URL重新定向方面表现不佳，因此预计很可能由此衍生出新的攻击方式。  预测8：网络罪犯利用窃取到的个人身份进行伪装攻击  为了降低攻击成本并提高获利能力，网络罪犯会通过非网络形式的强制手段（贿赂、勒索）侵扰个人，借此在环境中取得初步立足点。这类攻击可能主要针对公众人物（政客、演员、激进主义者、企业高管等）。随着更多个人数据遭到窃取，公众对于伪装性质的恶意行为或者数据/隐私意外暴露的担忧也愈发强烈。  预测9：网络保险成为强制性要求，可能反向催生网络犯罪  网络罪犯将矛头指向制定有保险政策的大型品牌。企业可能更愿意使用保险赔偿支付赎金以找回被盗数据，而非借此投入补救性措施，这最终会给攻击者提供新的、更稳定的收入来源。  预测10：以身份为中心的安全机制的兴起  随着系统与服务逐渐脱离传统网络/数据中心环境，安全保障工作开始更多依赖于身份证明。如今，身份验证正快速成为一切访问活动的唯一“密钥”。到2021年乃至之后，针对身份验证机制的攻击活动将有所增加。  [1]王英哲.2021年网络安全发展趋势预测[J].计算机与网络,2020,46(23):50-51. | | | | |