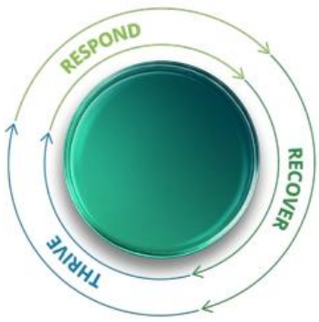
Deloitte. 德勤

全球网络COVID-19高管每周安全简报

本周报重点介绍德勤网络威胁情报中心（CTI）所识别的一些最新网络安全威胁和趋势，并提供近期有关管理网络安全风险的建议，帮助企业在全球COVID-19疫情背景下应对、恢复和持续发展。

***请注意：**第1页关注医疗保健关键基础架构，第2页介绍网络安全对关键基础设施的广义行业影响。*



2020 年 4月 第二期

COVID-19期间对医疗关键基础设施的网络安全影响

当医疗健康机构发现自己遭到不择手段的网络攻击者攻击时，他们正与COVID-19疫情爆发作一线的斗争。因此，在这些机构历史上最具挑战性的时刻，他们正面临双线作战的压力。德勤网络威胁情报中心（CTI）的研究显示，网络敌对者正在全球范围内针对关键医疗基础设施发起网络攻击，医疗健康机构和研究机构对COVID-19的应对措施因此也受到了他们的妨碍。本周，我们重点介绍了**影响全球医疗机构的一些问题和相关的网络威胁**（最初在3月13日至4月10日，CTI发布的详细威胁情报观察报告中已被识别）。

受影响范围:生命科学与医疗保健 | 区域:全球

对计算机系统的攻击影响了COVID-19检测结果

2020年3月13日，由于网络攻击，捷克共和国布尔诺大学医院的计算机系统受到了破坏。 捷克共和国医院拥有最大的冠状病毒检测实验室之一。 由于该攻击，医院的所有计算机都被迫关闭，这导致了COVID-19检测结果的延迟。

建议的首要行动:

1. 避免点击主题包含与COVID-19 或冠状病毒相关信息的电子邮件中的附件或链接。
2. 使用防火墙和入侵检测/防御系统（IDS / IPS）来检测和阻止与恶意软件命令与控制（C2）节点的网络通信。
3. 考虑对包含COVID-19、冠状病毒以及包含不常见文件类型的其他关键字的电子邮件发出警报。

国家健康系统的服务连续性受到安全漏洞影响

2020年3月15日，美国卫生与公共服务部（HHS）成为一场网络攻击的受害者。 这次攻击可能是为了破坏其正常运营，并且是一次针对冠状病毒疫情回应的破坏尝试，这可能是外国黑客的成果。该攻击在数小时内发送数百万次请求使HHS服务器超负荷运行（也就是大家所知的分布式拒绝服务攻击-DDoS）。 政府官员还注意到有关通过文字消息、电子邮件和社交媒体散布的关于全国封锁的虚假信息。 国家安全委员会（NSC）已通过其Twitter帐户警告有关国家封锁的消息是虚假信息。

建议的首要行动:

1. 为缓解DDoS攻击，确认/了解您企业的上游服务供应商，并与其合作制定冗余策略。
2. 配置网络设备使其丢弃来自黑名单区域的数据包。
3. 从专用供应商处购买DDoS缓解服务，并实施基于边界网关协议（BGP）的DDoS清理。

COVID-19疫苗测试中心工作受到勒索软件妨碍

2020年3月23日，一场针对医疗保健供应商Hammersmith Medicines Research的攻击被执行。该机构与英国政府合作，进行了冠状病毒（COVID-19）疫苗的测试。 这家英国医疗机构遭到了Maze勒索软件的攻击。该勒索软件偷走了用户数据进行勒索。 熟悉该攻击的人士表示，勒索软件攻击发生在2020年3月14日。 但是，直到2020年3月23日，该攻击才在新闻中被公布。为了得到声称的勒索金，攻击者尝试收集了一些患者数据并将其发布在网上。 2020年3月18日，Maze勒索软件背后的主谋者宣称，他们不会在疫情期间针对医疗组织发动攻击。 但是，这一承诺并没有阻止他们继续收取赎金。

建议的首要行动:

1. 依靠强大、频繁且冗余的备份恢复被勒索软件或破坏性恶意软件感染的文件。
2. 确定最敏感或最关键的系统和数据，并为它们提供额外的保护，例如网络分段或加密。
3. 映射面向公众的基础架构的攻击面，并确定强化或关闭攻击者潜在入口点的方法。

COVID-19疫情期间医疗健康机构和研究机构在网络安全影响上的七大趋势

- COVID-19疫苗IP知识产权遭窃
- 供应链受损
- 呼吸机和医疗设备损害
- 以COVID-19为主题的恶意网络钓鱼活动
- 高级持续威胁（APTs）
- 远程工作/远程医疗视频会议平台被列为攻击对象
- COVID-19患者的电子病历/个人健康信息

安全加固能力的建议

- 审查和更新云安全策略以支持虚拟和远程医疗创新服务
- 针需提供COVID-19响应需求支持服务的第三对方进行快速安全审查
- 扩展对移除设备的威胁检测和监控的能力

预先做好规范化和规模化的准备

- 通过扩展安全架构，提供对虚拟和远程医疗服务场景的支持
- 为远程设备部署用户和实体行为分析（UEBA）
- 实施或增强危机预案，并开展演练

两个月内的医疗健康领域的网络攻击上升

150%

犯罪分子试图在COVID-19疫情危机期间，利用信息系统的漏洞发动攻击。

参考链接：https://www.medicaldevice-network.com/news/coronavirus-cybersecurity/)

稳健恢复及全面反弹: COVID-19 推动了关键基础设施的下一个常态

许多全球制造企业和物流企业被要求承担更多的角色，他们现在已被列入“公众福利”组织，并已成为国家关键基础设施的一部分。这些企业的供应链现在也已成为国家关键基础设施的一部分（例如，医疗和其他重要物资被生产和分发给医疗工作人员）。因为没有供应商和物流公司，这些医疗机构将无法运作。新的指定人员还包括研究实验室、超市和其他销售必需品的零售商。美国国土安全部（DHS）在COVID-19疫情期间将出租运输部门加入了“关键基础设施工作者”列表。

作为国家关键基础设施的一部分，这些企业现在必须满足各种网络安全和隐私法规的要求。以前，这些企业的网络安全合规性要求最低，而且只需符合ISO质量标准（非政府规定的网络安全标准）。但是现在，作为该国家关键基础设施的一部分，这些企业必须满足各种网络安全和隐私法规的要求。

COVID-19 的影响– 制造企业及物流企业 | 一夜之间从非必需到关键

许多制造企业和物流企业被要求承担更多的角色，他们现在已被列入“公众福利”组织，并已成为国家关键基础设施的一部分。由于COVID-19疫情的爆发，产品和服务是公众福利所必需的（例如，为医疗工作者进行医疗和其他重要物资的生产和分发），因此将其重新分类为“关键”。此前，这些企业网络安全合规要求非常低，并且这些要求是在ISO质量标准的范围内进行的，而不是地方政府规定的网络安全标准。但是现在，作为关键基础设施的一部分，公司现在必须满足各种网络安全和隐私法规。这将需要对制造企业和物流企业的安全基础架构进行大规模的重新架构，以便可以满足政府标准并减少合规报告的成本、时间和精力，从而避免因不合规而导致的罚款。

关键基础设施的新常态

现在知道自己是关键或重要基础设施行业的一部分企业，将需要扩充或重新分配预算，以对必要的数字化转型计划和相应的合规行动进行支持，这些行动侧重于业务弹性和员工能力，以及跟进疫情前的客户合约和创收计划。

全球各地的政府机构设立协会，对关键基础设施服务有关的监管转变提供指导，并对特定行业如何实施针对关键基础设施安全的风险管理框架和方法提供详细说明。

这些新成为关键基础设施的企业采取的行动调整，将使他们不仅能够在未来重大危机中稳健经营，而且还将全面加速反弹，在危机时刻，提供利益相关者所需的基本产品和服务。这可能是关键基础设施常态化成功的新定义。

合规并不等于成熟的安全能力

组织应考虑以下内容，以确保关键应用程序和核心基础架构实施可度量的安全基础架构控制。

- **安全的操作环境应包括：**及时开展关键基础设施和应用程序的漏洞评估和漏洞修复。
- **研究机构网络事件响应的**监视和报告。更新响应预案及业务连续性和灾难恢复计划。
- **发现和保护关键数据资产：**根据公民和员工数据的个人可识别信息保护义务的要求。
- **识别并保护第三方供应商：**即获得审批可以直接访问组织信息系统的第三方，以及通过第三方进行访问的任何第四或第五方。

在COVID-19疫情期间我们将在您身边帮助您

相关德勤参考资料：

- **COVID-19的网络直播：** Responding to COVID-19 with business resilience, trust, and security
- **文章：** Ransoming government
- **文章：** COVID-19 response capabilities for health care organizations
- **文章：** The heart of resilient leadership: Responding to COVID-19

德勤网络安全服务：帮助企业更好地解决复杂的网络问题，从容应对未来的挑战。面向企业、人员和全球有更智能，更快捷，更互联的特点。作为网络安全咨询领域公认的领导者，德勤可以更好地帮助企业将网络安全战略和投资与业务重点保持一致，提高网络威胁意识和可视性，并增强企业在面对网络安全事件时的应对能力。凭借专业洞察力、技术创新能力以及优秀的企业网络安全解决方案，德勤网络安全团队在这个安全无界的时代，帮助企业畅行无限。

德勤中国网络安全服务合伙人


薛梓源
德勤中国网络风险服务领导合伙人
电话：+86 10 8520 7315
电子邮件：tonxue@deloitte.com.cn


江玮
东区
电话：+86 21 2312 7088
电子邮件：davidjiang@deloitte.com.cn


何晓明
北区
电话：+86 10 8512 5312
电子邮件：the@deloitte.com.cn


郭仪雅
南区香港
电话：+852 2852 6304
电子邮件：evakwok@deloitte.com.hk


冯晔
东区
电话：+86 21 6141 1575
电子邮件：stefeng@deloitte.com.cn


石沛恩
东区
电话：86 21 3313 8366
电子邮件：nathanshih@deloitte.com.cn


肖腾飞
北区
电话：+86 10 8512 5858
电子邮件：frankxiao@deloitte.com.cn


Pihkanen, Miro
南区香港
电话：+852 2852 6778
电子邮件：miropihkanen@deloitte.com.hk


Kukreja, Puneet
东区
电话：+86 21 3313 8338
电子邮件：puneetkukreja@deloitte.com.cn


张震
东区
电话：+86 21 6141 1505
电子邮件：zhzhang@deloitte.com.cn


何微
南区大陆
电话：+86 755 3353 8697
电子邮件：vhe@deloitte.com.cn


马国均
南区香港
电话：+852 2852 1086
电子邮件：lukema@deloitte.com.hk

欲了解更多联系信息，请访问Deloitte.com/covid 或 Deloitte.com/cyber