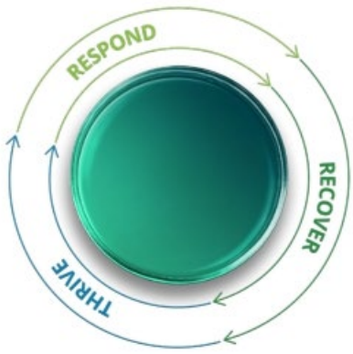
Deloitte.

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。



COVID-19 疫情期间数据保护及隐私

2020 年 5月 总第三期

本周我们重点介绍影响全球消费者、非营利组织和医疗健康机构的相关网络威胁情报（最初在4月11日至4月16日，德勤网络威胁情报中心（CTI） CTI发布的详细威胁情报观察报告中已被识别）。随着COVID-19疫情带来的恐惧，黑客正在利用窃取信息的恶意软件来锁定用户，其目的是获取个人身份信息（PII）、财务信息或以方便进一步访问的凭证。 当前COVID-19疫情的持续，导致针对用户数据和隐私的攻击量增加，从而加剧了此类风险。此外，CTI 的研究表明，黑客们正在全球范围内针对关键医疗基础设施发起网络攻击，导致医疗健康机构和研究中心对COVID-19的抗疫研究受到一定的阻碍。

知识产权（IP）盗窃

影响范围：生命科学|地区：加拿大，日本

木马软件Agent Tesla被利用于盗取医疗研究成果

从2020年3月到4月，德勤CTI观察到一次以“COVID-19”名义的网络钓鱼攻击。该钓鱼攻击，黑客使用Agent Tesla木马针对位于日本和加拿大的医学研究机构开展IP信息窃取。经过德勤CTI研究员分析，在攻击过程中黑客会向攻击对象发送名为“ COVID-19供应商通告”或 “疫情咨询”等钓鱼邮件。这些钓鱼邮件中含有一份伪装为“ COVID-19供应商通告.zip”的木马文件，用户一旦点击该文件，Agent Tesla木马程序会被自动加载到受害者的计算机上。

Agent Tesla木马程序可以执行截屏操作、密码窃取、远程控制摄像头或作为管道下载其它恶意软件。几乎可以肯定的是，这群黑客以这些企业作为攻击目标，通过渗透到内部网络进行侦察，以便展开进一步知识产权盗窃行动。

我们建议的首要行动：

1. 确保正确部署和及时更新反网络钓鱼、防病毒和网络过滤等安全控制措施。
2. 保持警惕，因为垃圾邮件也可能看起来合法或声称来自官方渠道，并且这些邮件可能使用与COVID-19或冠状病毒相关的主题。
3. 邮件接收者应主动采用其它通信方式或安全渠道对发件人进行验证，且不使用可疑邮件中所提供的联系信息。

消费者个人信息盗窃

影响范围:消费者|地区:全球

“骗徒”假扮慈善团体或机构，通过处理虚假捐款，以获取用户个人登录凭证。

德勤CTI高度确信，越来越多利用COVID-19相关主题开展个人身份信息（PII）或财务信息的盗窃活动。 傻瓜式网络钓鱼套件和SaaS式网络钓鱼服务（PhaaS）产品助长威胁数量不断飙升，因为攻击工具简单易用，降低了技术壁垒，黑客们可能仅需考虑是否有资金购买而已。
从2020年2月到2020年4月：

- 涌现了一批网络钓鱼工具被分发，它们仿冒合法的网站或机构来进行欺诈性交易。 用户被诱导提供敏感信息（例如登录凭据）以查看与COVID-19相关的策略。 另外他们可能通过冒充慈善机构或不存在的COVID相关机构，以“捐款”的方式进行欺诈。
- 出现了多个与COVID-19相关的水坑式攻击（watering hole attack），用以窃取如浏览器cookies、浏览历史、支付信息、表单自动填充信息和保存过的登录认证等。水坑式攻击是一种安全漏洞，攻击者试图通过感染已知的用户常访问的网页来达到攻击这一类用户群体的目的。

我们建议的首要行动：

1. 对任何第三方登录和远程用户登录启用双因素身份验证。
2. 监视并限制用户允许进入系统的登录尝试次数。超过阈值后，禁用该帐户，并实施备用验证渠道以重新启用该帐户。
3. 实施访问控制（AC）和身份访问管理（IAM），以限制网络特权和共享驱动器许可来控制终端被勒索软件感染。授予用户在其角色所需的最小权限。
4. 避免点击不明电子邮件消息及其附件或链接，尤其是这些附件或链接的主题中声称包含与COVID-19或冠状病毒相关的信息。

COVID-19疫情期间最需关注的数据保护和隐私考虑事项

在英国，NHS向超市提供了有关弱势患者的数据，以便优先向最需要的人送货。这些信息**至少覆盖了150万人。**

在公共健康领域，应该采取哪些数据保护和隐私措施?

美国正在开展“国家症状监测计划”，该计划是疾病控制与预防中心与各州、地方卫生部门之间的一项自愿合作项目。当中涉及**从超过4000多个医疗机构中获取数据。**

从超过4000多个医疗机构中获取数据。

对电子商务交易的数据分析发现，感冒、咳嗽和流感产品的购买量**增长了198%，**而止痛药的在线购买量**增长了152%。**

处理高度敏感的数据会产生什么后果

苹果和谷歌发布了一系列工具，这些工具可以让智能手机用户知道自己是否与患有COVID-19的人有过接触。

这项技术可以为接触者追踪提供有价值的新支持。一名公共卫生行政人员认为，该策略对于让人们在遏制疫情蔓延期间同时重返工作和恢复正常生活而言至关重要。

如果要追踪公民行为，应采取什么措施以进行匿名追踪?

对于不法分子来说，PHI比其他行业的PII更有价值，因为它包含更多详细信息，比如出生日期和社会保障号码。PHI中的详细信息有助于进一步的身份盗用行为，例如信用额度申请欺诈、保险欺诈和处方药获取欺诈等。

来自非医疗健康组织的PII记录，至少可以获取：

$0.10 *美元/每条*

然而，PHI信息可以卖到：

$5 *美元/每条*

稳健恢复和全面反弹：在确保安全的同时保护隐私的注意事项

当社会进入全面复工阶段，企业领导者应该重点关注哪些围绕数据隐私的问题

随着疫情持续好转，当政府认为全面复工的时机已成熟，传统企业将面临不少难题，例如：考虑如何更快让员工复工和与客户恢复业务往来，是否对员工及访客量体温及进行核酸检测，是否需要其披露健康状况？无论企业采取何种行动，都将围绕数据隐私问题作出决策。

在全球范围内，围绕隐私和疫情管理的话题一直存在争议。有关数据收集、分析和隐私方面的道德问题也被广泛关注。围绕员工和客户的数据隐私，企业应考虑哪些问题？我们建议从以下几点出发：

数据生命周期	企业“应对及稳健恢复”阶段的考虑事项	企业“复工”后的考虑事项－常态化
创建或收集	**匿名化**–为了抗击COVID-19，您的组织可收集哪些非身份信息（例如，如地理位置、人口统计信息）？	**同意管理**–有效的同意是与客户 / 员工建立信任的基本要素。如今，在收集数据需求激增的情况下，您的组织如何确保有效的同意，并如何清晰描述这些数据在COVID-19疫情期间和复工之后的使用、存储和销毁?
存储和处理	**盘点**–您是否有动态的方法来盘点为COVID-19相关活动而收集的客户/员工数据?	**安全的数据存储**–企业收集的数据越多，企业就越容易成为外部恶意攻击者的目标。企业应如何在预防和管理COVID-19传播的必要措施下限制个人信息的收集、使用和披露，并采取合理的措施来保护个人信息安全?
分析和使用	**分析方法**–COVID-19 增加了数据分析策略的复杂性。企业如何根据分析技术确定数据的准备情况？ 是否有关于数据使用的道德标准?	**使用**–是否按照公开的承诺、企业处理的法律依据和国际法规使用数据？ 企业是否具有用于数据使用和分析的治理模型?
共享或传输	**安全的数据共享**–COVID-19促进了科研机构与国际组织之间的数据共享，例如共同支持疫苗的研发。 组织应如何考虑检查其汇总数据中是否包含机密或受限制的信息，以及如何确保这些数据的安全传输?	**监控数据传输**–在COVID-19疫情期间和复工之后如何监控机密的知识产权(IP)、PII和PHI数据的使用和传输?
保留并销毁	**保留和数据变现**–如果您的企业计划将COVID-19中收集的数据变现，那么您的组织是否有与您的数据保留框架相一致的数据变现策略?	**数据保留**– 是否应保留在COVID-19期间收集的数据以便在复工后进行数据挖掘、建模等价值利用，或在计划的时间段后销毁？

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：

- Responding to COVID-19 with business resilience, trust, and security
- COVID-19 Government Response Portal
- Privacy and Data Protection in the Age of COVID-19
- GDPR: How to make your business more resilient against data protection breaches in light of the COVID-19 crisis?

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