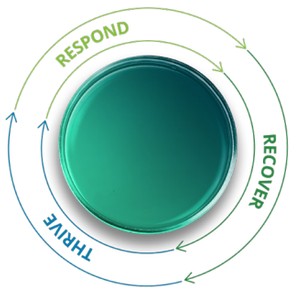
Deloitte.

COVID-19疫情期间3-4月网络威胁增长趋势

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。



2020 年 5月 总第四期

组织投入了大量的资源来应对网络攻击

WORLD

THE FREE PRESS JOURNAL

Updated on : Wednesday, April 22, 2020, 1:07 PM IST

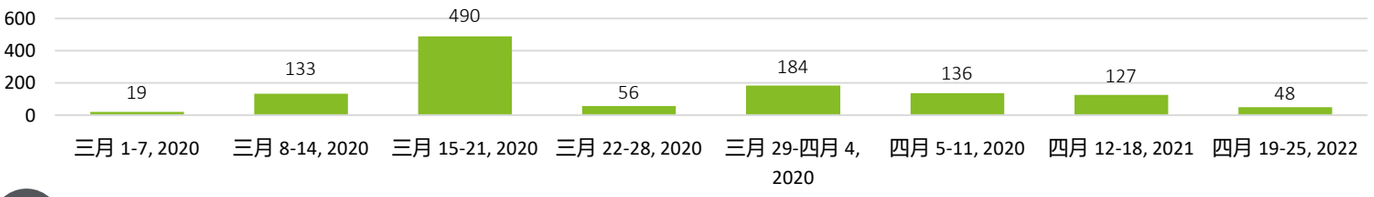
Hack in the time of COVID-19: 25,000 email ids, passwords of WHO, Gates Foundation and NIH employees posted online

By FPJ Web Desk

在过去的30天里，与COVID-19相关的恶意软件和网络钓鱼活动有所增加，包括对WHO和盖茨基金会等著名组织的针对性攻击。 虽然网络威胁总体数并未增加，但是攻击者利用人们对流行病的担忧，将攻击主题转量向COVID-19。从德勤CTI收集的关于COVID-19主题的恶意软件样本的增量中可以明显看出这一点。这些威胁的引诱点主要是疫情地图，其次就是政府资助的个人防护装备。

对于远程办公的员工来说，安全意识薄弱可能会给网络攻击提供方便之门。之后，我们可以推测到，紧接着就会是针对疫情联系人信息追踪和其他相关移动app为主题的攻击……

2020年3月和4月以COVID-19为主题的恶意软件的上涨*(COVID-19相关的恶意软件样本数)*



COVID-19疫情期间移动设备上的恶意软件攻击激增

从4月15日到4月21日，德勤CTI观察到了14次以COVID-19为诱饵的相关垃圾邮件活动。此外，德勤CTI还注意到针对IOS和Android用户的恶意软件以COVID-19主题为诱饵传播间谍软件。本周我们强调的是针对远程办公人员和移动用户不断增加的网络威胁(这个最初在4月18日至4月24日的详细威胁报告中已发现该情况).

来自“冠状病毒最新进展”恶意App的间谍软件威胁

影响范围：所有 |地域：全球

一款名为“冠状病毒最新进展”的恶意应用将间谍软件发给了毫无戒心的用户

2020年4月17日，Deloitte CTI注意到TrendMicro的研究人员发布了一篇报告，报告称一个冒名为 “冠状病毒最新进展”的 恶意应用程序在分发一种名为Project Spy的间谍软件，攻击Android和iOS用户。印度，巴基斯坦，阿富汗，孟加拉国，伊朗，沙特阿拉伯，奥地利，罗马尼亚，格林纳达和俄罗斯已经观察到了该应用程序被下载的实例。这种间谍软件能够通过从用户的设备秘密传输数据，来获取有关他人计算机或移动设备活动的敏感信息。

恶意人员利用仿冒DocuSign和Adobe等流行的服务攻击远程办公

影响范围：所有 |地域：全球

以“未清发票”伪造邮件为诱饵来实施商业电子邮件入侵（BEC）攻击:

随着全球许多组织在COVID-19大流行期间选择远程办公， DocuSign等服务已被广泛用于对敏感文档的访问验证。恶意人员正利用当前这种全球办公现状，通过仿冒流行服务（例如DocuSign，Adobe和其他广泛使用的工具）来实施针对访问凭证的网络钓鱼攻击。2020年4月16日，德勤CTI发现安全供应商MailGuard发布了一则关于通过欺骗DocuSign以获取Adobe Cloud凭据的网络钓鱼活动的报告。MailGuard研究人员发现了其中一封为“未结清发票”的垃圾邮件。

有效监督针对COVID-19恶意软件和网络钓鱼攻击所开展的网络风险管理活动

德勤建议采取以下措施防范网络攻击:

主动部署预案

更新网络事件响应手册?
- 查看网络事件响应手册，调整远程工作中必要的活动或步骤，预测可能的COVID-19攻击场景。

如何协调利益相关方?
- 确定技术、业务和战略层面关键的利益相关者，以便在事件发生期间进行远程协作。确保主要和次要联系人详细信息已更新并且随时可用。
- 针对潜在的攻击手法和COVID-19诱饵对相关人员进行培训教育。

密切监督

如何安全地指导远程协作?
- 指导和监督团队如何进行远程协作，确保员工已被通知并知晓相关工具及其被授权的流程。

如何对运营模式进行监控和实施变更?
- 优化在事件响应范围内执行远程调查和分析活动的能力。
- 对COVID-19为主题的网络钓鱼攻击实施主动的威胁监视和捕捉。
- 利用好为COVID-19设计的最近更新的监控仪板。

及时更新安全控制

如何认证并更新安全访问策略?
- 强制对远程访问技术（例如VPN）和电子邮件服务（例如Office 365）启用多重身份验证。
- 加快所有面向互联网的网站部署。

如何更新安全控制?
- 在疑似攻击的调查期间，对可能采用的调查数据源，优化其日志记录详情和保留期限。
- 审查组织中用于远程访问的工具和技术的安全控制情况，包括但不限于Office 365（电子邮件）和VPN服务。

稳健恢复和全面反弹：社交疏散期间为网络安全应急事件做准备的首要考虑点

在为不可避免的网络安全应急事件做准备时，所涉及的不仅仅是准备做出反应和解除一次性攻击。它涉及有效的、持续的响应能力——包括主动规划预案，大力防御关键系统和数据资产，持续跟踪不断发展的网络威胁以及在发生攻击时能彻底恢复。在COVID-19疫情期间，网络攻击会占用公司大量的资源。适应社交距离限制的强大的网络事件响应（CIR）能力对于企业至关重要。当下，网络攻击者们正在疫情发展不同阶段，择机入侵公司网络。

要像当冠状病毒锁定其城市和国家时，政府部门迅速采取行动改变战略和程序一样，企业也应该审查和调整事件响应手册，协议和安全控制措施以跟上不断增长的网络发展步伐，否则他们可能会面临很多暴露在外几个月甚至几年的漏洞。

为了做好准备，组织可以考虑六个关键领域：

可防御性审查

远程评估并确保业务连续性程序、疫情场景和企业管理实践是可以防御新形态下的外部攻击，并与适用的网络安全和隐私合规要求、诚信义务和行业期望保持一致。

网络安全，危机和疫情事件响应

确保危机管理程序更新，以有效实施和管理远程网络安全、危机和疫情应对措施。首要第一步就是建立远程危机管理办公室并有效管理。

远程培训和评估

对远程办公人员进行培训，让他们了解不断发展的组织流程以及与COVID-19相关的日益增加的网络风险。

第三方风险与供应链管理

了解关键供应商的网络风险和应急计划，并将其纳入公司的应急策略。

威胁管理和态势感知

对公司远程办公的所有基础设施，开展远程评估和部署相关技术措施来提高威胁可见性和防护能力。

威胁情报

监测暗网，以识别组织所暴露的风险，以及针对组织的过往的、活跃中和计划中的攻击。通过情绪分析来改善COVID-19期间员工、供应商和客户之间的沟通。

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


何薇
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