维也纳, 2020年4月14日

网络犯罪和COVID19（新型冠状病毒肺炎）:风险与应对

关键判断

- COVID19的流行和蔓延使得网络犯罪不断演变和增长。网上诈骗、敲诈勒索和线上儿童性侵主要针对个人，而勒索软件主要危害包括医院在内的系统。政府将继续成为恶意软件的攻击目标。错误信息和不实信息的不断传播将继续迷惑公众，影响科学应对。
- 居家办公增加了潜在的网络犯罪受害者群体。人们在家上网时会面临更大的风险，会无意中将企业IT暴露给网络犯罪分子。网络钓鱼将继续为犯罪分子和其他提前行动者提供恶意访问关键系统的机会。

内容

1. 本简报简要介绍了COVID19背景下的网络犯罪威胁。报告来源于毒品和犯罪问题办公室于2020年4月初在世界各地的执法部门、政府、非政府组织、学术、媒体、开源和私营部门合作伙伴的机密报告。建议载于每一专题部分的末尾。

威胁图景: 演变、增加和利用

2. 目前，世界各地都在实施全面的社会隔离措施。这已导致公共当局、企业和个人在线交流的使用需求显著增加。许多人不熟悉如此大规模的在线技术的使用，这为网络罪犯提供了一个巨大的、有吸引力的、易受攻击的攻击目标。在线技术与远程工作和学

校教育相结合，产生了更多的互联网用户，他们不太了解这种威胁，因而相较于在单位或学校，他们在家里上网可能会比承担更多的风险。

3. 网络罪犯分子已经优化了他们的犯罪行为，以利用与COVID19相关的社会、法律和心理上的细微差别。无论是刚接触互联网的新用户还是曾频繁使用互联网的学龄儿童，均正成为网络性侵犯者的目标。这包括罪犯试图通过更广泛地渗透到在线课程中来对个别儿童进行培训[1]和性侵犯，[2]此处指“Zoom-bombing”。[3]

4. 网络犯罪分子越来越多地利用人们对新冠病毒的恐惧: 在互联网上销售假药，通过销售不存在的洗手液、个人的医学防护用品、药品、卫生用品等进行诈骗。其他欺诈行为包括提供不靠谱的投资建议(包括加密货币)和不正确的医疗建议与诊断。一家主要的网络色情站点向一个国家的用户提供免费订阅服务，增加了恶意软件下载与性勒索的风险。

5. 那些对网络风险往往不大敏感的老年人，能被网络犯罪分子明确锁定为攻击目标，被诱导通过与新冠病毒相关的垃圾邮件下载和转发勒索软件的链接，并在朋友和家人之间传播虚假信息。网络犯罪分子继续试图通过声称知晓并揭露受害者所谓对网络色情的使用来敲诈勒索。

6. 商务电子邮件入侵[4]（利用被盗用的邮件帐户冒充成一位目标组织的高级官员进行欺诈）继续使用社会工程学，通过紧迫感日益增强的流行病加深影响程度，来鼓励资金流向犯罪银行、外汇或虚拟货币，或获得用于包括间谍活动等恶意行为的敏感数据。

7. “黑暗之网”论坛继续出售被盗用的数据—包括知名官员和名人的数据。新接触网络犯罪的犯罪分子正在寻求他人的建议，以更好地利用新冠病毒大流行来牟利。一些网络犯罪分子试图阻止其他网络犯罪分子把医院和疫苗检测实验室作为目标，阻止它们被分布式拒绝服务(DDOS)和勒索软件攻击。掠夺性儿童性侵犯者继续研究哪些社交网络和照片分享网站可能会让他们最容易接触到儿童来实施犯罪。犯罪分子也在继续考虑如

[1] https://www.esafety.gov.au/parents/big-issues/unwanted-contact

[2] https://www.esafety.gov.au/key-issues/image-based-abuse/take-action/deal-with-sextortion

[3] https://tcrn.ch/3buz3gW

[4] https://www.trendmicro.com/vinfo/us/security/definition/business-email-compromise-(bec)

何在网上最好地识别并击败便衣警察。

8. 除了传统的网络犯罪，高级持续性威胁(APT)组织继续演变并利用疾病大流行。高级持续性威胁组织们继续使用恶意软件、勒索软件和分布式拒绝服务来攻击国家关键基础设施，包括医院和疫苗开发实验室。这种攻击背后的动机不仅是简单基于利润，因为恶意软件经常提供登录凭证和其它具有情报价值的敏感信息的访问入口。

9. 许多与新冠病毒相关的网络犯罪的成功依赖于用电子邮件钓鱼攻击作为最初的媒介。当人们点击链接或文档，账户就会泄露。这种泄露可能对受害者是可见的，但更多的情况下，泄露是隐蔽的，使罪犯能够建立和保持对账户、组织和信息关联的长期访问。APT行动者除了收集敏感信息之外，还可以破坏网站、改变文件的细节、删除数据、传播虚假信息和不实信息。

10. 毒品和犯罪问题办公室建议各国政府和私营部门加强具有文化敏感性和易于普及性的公众意识宣传活动。匿名的在线儿童性虐待举报热线是应对的一个关键点。我们还建议继续严格地应用安全更新材料，并定期备份信息。

执法能力和社会应变能力下降

11. 在许多国家，专门打击网络犯罪的执法人员已从调查网络犯罪转为支持政府采取措施，例如隔离执法，以抵御COVID19的爆发。专家官员也生病了。在未来几周内，能力可能会进一步下降，从而削弱各成员国应对新的和日益增加的网络犯罪威胁的能力。

12. 在一些国家，当地采取的公共卫生措施使得相关人员不可能亲身从事相关活动，调查和司法程序因而中断。其他国家已迅速转向在线司法行动。

13. 关于病毒的错误信息和虚假信息主要通过社交媒体和加密消息服务继续传播。社交媒体公司也面临着远程办公，应对错误信息内容的数量、如何始终如一地实施内部政策以及地方立法的影响的挑战。

14. 错误信息、虚假信息和对国家关键基础设施的攻击破坏了公众信任，削弱了公共安全措施的效力。

15. 联合国毒品和犯罪问题办公室建议，司法程序应尽可能继续线上进行，同时应确保国际标准和规范、正当程序和法治仍然有效。

16. 我们还建议社交媒体公司在保护言论自由的同时，采取更多措施来遏制COVID19信息“误报”的传播。COVID19反应的核心必须是基于事实的科学——我们都可以在这方面发挥关键作用。

分析

a. COVID19流行病对全社会构成了前所未有的全球性挑战。许多民众已经把他们的物理性活动转移到线上进行，犯罪分子也一样。随着网络犯罪复杂性和受害者数量的增加，一些国家的执法者却被转派至其他职务。COVID19带来的经济影响为公众和政府增加了一层复杂性。一场极致的潜在网络犯罪风暴即将来临。

b. 当COVID19和与这场危机有关的网络犯罪威胁呈现全球性时，应对措施也必须是全球性的：在一个管辖区打击网络犯罪便有利于降低全球风险。关于新威胁和新犯罪类型的信息，如欧洲刑警组织的COVID19分析和国际刑警组织的网络威胁评估，必须继续进行无延迟国际共享。网络儿童性虐待举报热线也是使公众能够应对这一威胁的重要工具。

c. 鉴于主动和被动执法可能面临的压力，我们评估，积极调查网络犯罪的能力将在短期内受到挑战，特别是在流行病前资源有限的国家。包括高级持续性威胁（APT）组织在内的网络罪犯将继续利用这一点。必须加强对成功逮捕、摧毁企图利用当前危机的网络罪犯的情况的公开报道。极具影响力的行动有利于彰显可见的影响，并提醒网络犯罪分子世界各地的打击行动仍在继续，如荷兰最近在一周内取缔了十五家分布式拒绝服务攻击（DDoS）供应商。[5]必须继续对高风险网络犯罪行为者采取积极的网上卧底行动。与直觉相反，网络罪犯可能会在网上面临更高的风险，因为他们认为被发现的可能性已经降低了。因此，专业执法调查必须继续保持跟进。

d. 公共外交和网络安全意识的提升对预防网络犯罪至关重要，并且必须增强弱势群体在这方面的能力——特别是儿童和老年人。针对错误信息和虚假信息的措施应提供经过评估的、可信的和有用的信息：这意味着这些措施必须以透明和负责任的方式进行。

e. 所有用于打击网络犯罪的措施必须继续是适当的、合法的、负责任的和必要的。许多国家的政府正在使用技术来评估、识别和追踪潜在的COVID19患者。这一基本工作必须

[5] https://www.zdnet.com/article/dutch-police-take-down-15-ddos-services-in-a-week/

继续在明确监督下进行审查，以确保一旦实现疫情控制目标就撤消监测措施这一行动的实现。现在是时候面向公众建立网络信心，共同应对我们这个时代最紧迫的威胁，并从国际层面树立信心。

f. 现在还不是减少对专业网络犯罪执法的投资的时候。打击网络犯罪的能力是保护国家关键基础设施、保障儿童上网安全、增强产业能力、保障医院安全和支持经济从COVID19疫情中复苏的重要组成部分。

g. 联合国毒品和犯罪问题办公室的网络犯罪专家可以每周7天、每天24小时不间断协助全球范围内成员国打击网络犯罪活动。联合国毒品和犯罪问题办公室的公共外交资源可访问https://www.unodc.org/unodc/en/COVID19.html，其中包括与秘书长青年问题特使、联合国工作人员网络保护建议和联合国秘书处网络现场活动的Instagram现场会议链接。