高校群发邮件“吓坏”校友，“幕后黑手”竟是惯犯

作者：writer 来源：科学网

本文原地址：https://www.iikx.com/news/progress/38669.html

高校群发邮件“吓坏”校友，“幕后黑手”竟是惯犯。

编译｜赵婉婷

2025年10月的一天，“Stefan988”（网名）的邮箱弹出一封母校发来的邮件：“我们遗憾地通知，基于对你的审查，我们将永远停止你在西悉尼大学的学习，你于此前获得的任何证书或奖项将被撤回。”

“Stefan988”倒吸一口凉气，彼时他已经毕业数年，这样的通知犹如一场噩梦。“毕业后学校再未与我联系”“我根本不知道学校在对我进行审查”“邮件中我的学生证号的确是正确的”……他满心迷惑，并在社交媒体发帖询问网友的看法。

原帖截图

评论区很快热闹起来。不止一位已毕业多年的校友和正在就读的学生留言称，自己也收到了这样的邮件。他们在交流中推测，这应该是虚惊一场，大概是学生服务中心的系统出了故障。

实际上，这并非一次系统故障，其背后是一连串性质严重的网络攻击事件。据媒体近日报道，嫌疑人Birdie Kingston为原澳大利亚西悉尼大学学生（其具体毕业时间尚无公开信息），她不仅是这次虚假邮件事件的幕后黑手，还连续三年违规入侵该校信息系统、在网络上出售该校相关人员的个人敏感信息，甚至向校方索取赎金。

2025年年底，Kingston已被澳大利亚新南威尔士州执法部门逮捕，目前正在狱中等待庭审。目前的公开信息并未明确解释她的作案动机。参与案件调查的警司Jason
Smith表示，Kingston对大学的长期不满，可能是其犯罪行为背后的主要动机。

01 多次违规入侵学校系统

Kingston的黑客行为始于2021年。

彼时，Kingston就读于西悉尼大学的电气工程专业。为了少交校内停车费，她“ 黑 ”入停车系统，篡改了自己的停车费用账单。

Kingston没有止步于此。在之后的三年里，她的行为变本加厉，升级为复杂且恶劣的网络攻击。Kingston长期在教职工、学生和管理这三类账号之间来回切换操作，一路收集了教职工和学生的门户信息、学术数据库、云存储等大量数据。

2024年1月，该校首次发现系统漏洞，并上报至相关部门。2024年5月，该校向约7500名受影响的个人和大学社区成员正式发出通知，告知其所使用的Microsoft Office 365环境遭到入侵。

警方于同年6月锁定了嫌疑人Kingston，并突袭了她的大学宿舍，但当时未对她提出任何指控。

Kingston没有就此收手。一个月后，学校再次通报，该校信息系统Isilon（一款数字内容智能集群存储系统，该校依托其托管校内桌面“ 我的文档 ”信息、各部门共享文件夹以及部分备份和存档数据）中的个人信息也遭到未经授权的访问。

同年11月，一封匿名邮件出现在学校邮箱，内容直白：以加密货币的形式支付4万美金，否则将在网络论坛公开所盗取的信息，任人。

Kingston造成的最严重的黑客攻击事件发生于2025年1月至2月间。当时，她攻破了该校的单点登录系统（SSO）。SSO的攻破意味着攻击者可通过单一凭证获得多项服务访问权限。被盗数据于6月初在网上出现。学校在相关泄露帖子发布后8小时监测到该情况，并协调将被盗数据下架。

6月底，Kingston首次被捕。她获得了附带严格条件的保释，包括禁止持有可上网的手机、未注册设备，禁止与大学联系，以及每天向警方报到。

但警方随后表示，网络攻击并未因此停止。6月19日至8月22日期间，Kingston涉嫌窃取数据并向

西悉尼大学服务器输入代码，并通过学校系统发送了109745封欺诈性电子邮件。

同年10月，Kingston利用盗窃数据伪造“学位撤销”邮件。“Stefan988”等一众校友收到的“虚惊一场”邮件，就发生于此时。

2025年年底，新南威尔士州警察与澳大利亚联邦警察再次逮捕了这位27岁的嫌疑人。这一次，她没有获得保释的机会。警方表示，Kingston持有一部经过改装的手机，可以作为电脑终端实施犯罪，她还涉嫌捏造、发布材料为自己开脱罪责。

依据新南威尔士州相关法律，Kingston面临20项与未经授权访问大学系统和基础设施相关的刑事指控。据称，这一案件将于今年进入庭审阶段。

02 信息泄露后

自2024年出现网络攻击事件后，西悉尼大学官方开设了“Cyber Incidents”网站更新该网络安全事件的发展进度，并介绍该校应对此事的策略。

根据网站公告，受影响的数据包括邮件地址、电话号码、姓名、出生日期、学生证或教职工证、雇佣和薪资详情、银行账户详情、税务档案号码、驾驶执照详情、投诉/案件、健康等重要信息。

该校表示与澳大利亚国家身份和网络安全支持服务机构建立了长期合作关系，且会向学校师生提供免费的咨询和支持。

校方称，已投入大量资金聘请专家服务，以确保建立强有力的网络安全防护措施。已采取的部分措施包括但不限于：重置和重新颁发系统凭证、密钥和访问令牌，并加强对外部技术提供商的监督；加强身份和访问安全保障，包括更严格的身份验证和对特权帐户更严格的控制；提升供应链网络安全审查和模拟的治理与保障水平等。

据报道，西悉尼大学开展的修复工作中，仅承包商费用就超5300万美元。

该校同时建议用户考虑更改密码并设置多因素身份验证、更换驾照等证件。但学生似乎对这些建议并不满意。“改密码？仅此而已？真是太可笑了。”一学生在社交平台表示。

“学生将数据托付给了他们。这家机构收取了无数学生甚至非学生的学费，显然这些钱根本没花在网络安全上，更别提数据处理政策了。我毕业都十多年了，他们根本无权把我们的信息保存这么久，更何况他们还用这种有问题的方式存储信息。”另一位学生留言道。

从事网络安全与创新战略及咨询的Glenn Murray在领英撰文评论道，当一所大学被入侵，不只意味着技术失败，还会爆发信任危机。“学生开始怀疑学历能否被篡改；员工担心人事档案、绩效评估、医疗信息在网上流传；家长重新审视招生页面；监管机构拿着泄露通知函步步紧逼。”

“即便信息被盗后尚未泄露，损害也已发生。因为信任不只是‘有没有泄露’，还在于‘还可能泄露什么’，以及其反映的相关机构对重要事物的保护能力。”Murray写道。

03 大学网络攻击事件频发

高校的网络系统究竟存在多少漏洞？事实上，西悉尼大学受到的网络攻击事件并非个例。

通过梳理媒体报道发现，仅2025年，就有多起高校数据泄露事件发生。例如，3月，一个名为Funksec的勒索组织发布消息，声称已从法国索邦大学服务器中窃取了20GB的文件；7月，美国哥伦比亚大学表示，86万曾注册或曾在该校学习者的信息被黑客泄露；10月，宾夕法尼亚大学SSO账户遭入侵，攻击者在网络论坛上发布了数千页校内文件，包括内部谈话、捐赠者及家属备忘录、银行交易收据；11月，哈佛大学监测到其校友事务平台在一次钓鱼电话后遭未授权访问，电子邮件地址和电话、家庭和工作地址、活动出席记录、大学筹款等信息遭泄露。

Funksec发布的勒索信息

精英教育机构已然成为网络犯罪分子的主要目标之一。当敏感信息被窃取，可能会发生什么？

网络安全媒体Cybernews的副主编Vilius Petkauskas指出，泄露的社会安全号码、出生日期和个人信息的组合使攻击者能够尝试“身份盗窃”。“攻击者可能会以他人名义创建虚假账户——这是网络犯罪分子常用来掩盖非法活动的手段。”

此外，Petkauskas强调，攻击者可能针对知名人士发起复杂的网络钓鱼攻击并进行勒索。一些知名的毕业生也会因其财富和影响力，成为“最有价值”的目标。

随着一系列网络入侵事件频发于高等教育机构，大学对于社区敏感数据的保护，或许是开展教育工作的前提。

参考信息：

https://www.academicjobs.com/au/higher-education-news/wsu-cyber-attacks-former-student-charged-or-academicjobs-au-7142

https://www.abc.net.au/news/2025-12-05/western-sydney-university-hacking-arrest-birdie-kingston/106105756

https://www.linkedin.com/pulse/blog-19-ctrlaltdeceit-curious-case-birdie-kingston-murray-phd-k6cec/

https://7news.com.au/news/former-western-sydney-university-student-charged-after-allegedly-hacking-system-for-personal-gain-over-years-c-19164802

https://www.westernsydney.edu.au/news/cyber-details/october-23-2025

https://www.reddit.com/r/UWS/comments/1nzeqpy/is_this_legit/

https://www.huit.harvard.edu/cyberincident

https://cybernews.com/news/sorbonne-university-paris-claim-funksec-ai-ransomware-attack/https://cybernews.com/security/columbia-university-data-breach-students-exposed/

https://www.cuit.columbia.edu/cyber-incident

https://www.acronis.com/en/blog/posts/ivy-league-universities-under-siege-the-cyberattacks-targeting-harvard-princeton-and-penn/

作者：赵婉婷 来源：科学网微信公众号