南方财经全媒体 记者吴立洋 实习生吴峰 北京报道

近日，多个社交媒体以及安全技术社区均有用户称遭遇“.locked”后缀勒索病毒攻击，计算机文件被病毒加密，用户“中招”后，需支付0.2比特币“赎金”（约2.7万人民币）解锁。

据悉，本次遭遇勒索病毒攻击的对象主要为CRM（Customer Relationship Management客户关系管理系统）厂商，包含“用友”及旗下“畅捷通”等管理软件。

事件发生后，畅捷通分别于8月29日和8月30日紧急发布安全补丁修复该漏洞。其在公告中表示，受到勒索病毒攻击客户的软件服务器“为客户自有部署方式，且未做必要的网络安全防护。”

多位网络安全业内人士和律师在接受21世纪经济报道记者采访时表示，对于采买软件产品存在安全问题而导致经济损失的归责和赔偿问题，供应商和客户通常会在采购合同中加以约定。按照目前的行业惯例，通常遭到第三方恶意攻击时，供应商需按照故障处理尽快提供解决方案，但通常不会对相关损失承担赔偿责任。

安全损失谁之责

8月30日，国家信息安全漏洞共享平台（CNVD）发布了关于畅捷通T+软件存在任意文件上传漏洞的安全公告。未经身份认证的攻击者可利用漏洞远程上传任意文件，获取服务器控制权限。

公告还建议受影响的单位和用户立即将所使用的畅捷通升级至最新版本，联系畅捷通技术支持，采取删除文件等临时防范措施或确认是否具备从备份文件恢复数据的条件及操作方法。

一位遭到该勒索攻击并被锁定文件的畅捷通用户向记者表示，目前除了以一个自称畅捷通工作人员的账号在自己的微博下方进行了回复，表示可以反馈至相应工作人员进行安全加固，此外未有任何官方人员与其进行联系。

“相关文件找专门的第三方公司修复需要三四万。”该网友表示。

上海申伦律师事务所律师夏海龙在接受南方财经全媒体记者采访时表示，如果用户是因第三方恶意侵入系统而遭受损失，则一般应由入侵者承担相关法律责任，判断软件服务商是否需要承担责任取决于其是否存在过错。

西安交通大学法学院助理教授王新雷也表示，根据《民法典》第一千一百六十五条规定，行为人因过错侵害他人民事权益造成损害的，应当承担侵权责任。

但他也指出，勒索软件等网络攻击的法律责任类型很多，涉及民事责任、行政责任和刑事责任。如果网络产品服务提供商提供的网络产品服务不符合有关安全技术标准规范的，可以认为其对被侵权人的损害存在一定过错，将可能相应的赔偿责任。这个过程主要取决于网络产品服务提供商、用户是否严格遵守了网络产品服务的安全义务。

根据我国《网络安全法》和《数据安全法》的规定，当软件服务商发现旗下产品存在漏洞、存在安全风险时，应当立即采取补救措施，同时应当及时告知用户并向有关主管部门报告。

夏海龙指出，如果软件本身存在漏洞或入侵发生后服务商未及时采取补救措施，则软件服务商应当承担一定责任；如果系统遭受入侵是由于用户未能妥善保管账号、密码而发生，则用户就不能仅因此要求服务商承担责任，而只能向侵入者追究责任。

“当发生网络攻击事件时，公安网络安全部门不仅会去追查攻击者，同时会依据《网络安全法》第21条，对被攻击者或者产品服务商履行网络安全义务的情况进行检查。”王新雷表示，检查范围主要为评估企业等相关方是否履行等级保护义务，如果存在违反网络安全等级保护义务的，相关企业及其负责人均可能需要承担行政责任甚至刑事责任。

不过多位网络安全行业从业者告诉记者，当前在监管要求不断完善，企业合规意识提高的大背景下，在发生网络安全问题时，正常履行相关安全义务的企业，除了向有关部门及时报告，只需要尽快进行漏洞修复，而不需要承担民事赔偿责任。

这也是当前行业内的普遍做法。某南京网络安全工程师告诉记者，目前服务商与客户通常会在采购合同中写明发生安全问题时双方所需承担的责任与义务，按照行业惯例，大部分情况下因网络安全攻击而造成的损失会被视作故障，服务商需要及时进行漏洞修复和处理，但无需对攻击造成的损失进行赔偿。

“作为软件服务商，确实很难保证自己的产品完全没有安全问题，就我所知，行业里也没有进行赔偿的先例。”另一位坐标成都的网安从业者向记者表示。

探索治理新框架

随着数字经济的快速发展，网络安全问题对社会生产生活的威胁愈发频繁和严重，网络安全的治理框架也在不断完善中，一方面，以《网络安全法》等“三法一条例”为代表的技术、监管、标准制定等方面的法规和措施正不断落地，另一方面，对于网络安全问题前期防范、中期应对和后期处理的责任要求也在进一步细化。

去年7月，工业和信息化部、国家互联网信息办公室、公安部印发《网络产品安全漏洞管理规定》，网络产品提供者和网络运营者是自身产品和系统漏洞的责任主体，要建立畅通的漏洞信息接收渠道，及时对漏洞进行验证并完成漏洞修补。同时，《规定》还对网络产品提供者提出了漏洞报送的具体时限要求，以及对产品用户提供技术支持的义务。

王新雷指出，软件服务商发现产品存在安全漏洞后，应当履行验证和评估漏洞的危害程度和影响范围、向工信部网络安全威胁和漏洞信息共享平台报送相关信息、及时组织对网络产品安全漏洞进行修补三方面的义务。

同年11月，国家网信办发布关于《网络数据安全管理条例（征求意见稿）》公开征求意见的通知。该征求意见稿第四十四条规定，互联网平台运营者应当对接入其平台的第三方产品和服务承担数据安全管理责任，通过合同等形式明确第三方的数据安全责任义务，并督促第三方加强数据安全管理，采取必要的数据安全保护措施。第三方产品和服务对用户造成损害的，用户可以要求互联网平台运营者先行赔偿。

王新雷表示，“三法一条例”等网络安全法规注重行政监管和公共利益，未来我国需要在“三法一条例”的基础上，继续建立健全配套法规，提高网络安全法规的可操作性，更好地明确网络空间利益相关方的责任边界。

例如，在勒索软件攻击等场景中，通过专门法规、司法解释等形式，明确攻击者、网络产品服务提供者和用户的相应安全义务，依据不同过错情形进行责任分配。

“我们还需要健全跨境网络犯罪的合法侦查手段体系，并倡导和推进打击跨境网络犯罪的国际合作机制。”王新雷说。

更多内容请下载21财经APP