勒索软件：保险市场的视角

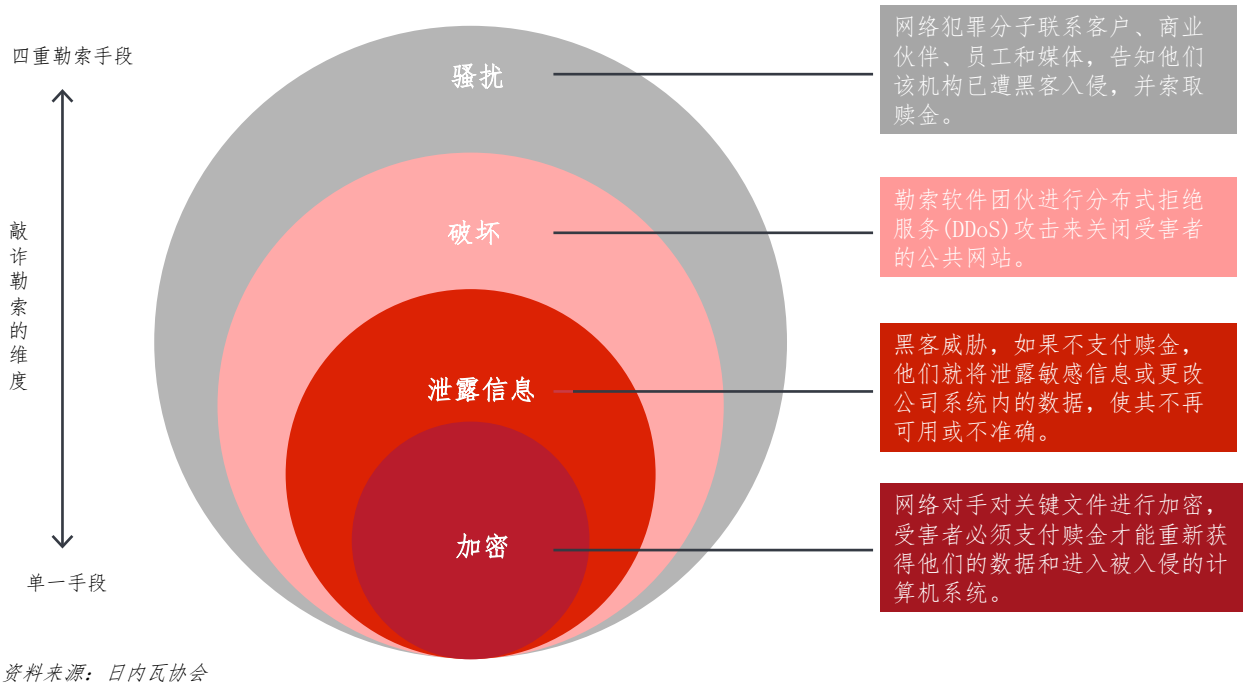
THE GENEVA ASSOCIATION
INSURANCE FOR A BETTER WORLD

Darren Pain，日内瓦协会网络与演化中的责任险专题主管

Dennis Noordhoek，日内瓦协会公共政策和监管专题主管

勒索软件——一种获取文件或系统并阻止用户访问的恶意软件，直到受害者支付赎金以换取解密密钥——和其它相关形式的网络勒索最近已成为一个严重的问题。近年来，试图入侵和成功攻击的数量以及赎金要求的规模都呈急剧上升趋势。网络犯罪分子也在使用复杂的手段来敲诈受害者。勒索软件运营商越来越多地采用额外的勒索手段，而不是单纯地对数据和文件进行加密并要求支付赎金。这些威胁包括：如果不支付赎金，就将公布敏感信息或关闭公司的网站（图 1）。

图1：勒索软件犯罪分子使用的不同勒索方法



资料来源：日内瓦协会

[1]AM Best 2021.

“勒索软件即服务”(RaaS)商业模式的发展，使黑客能够使用现成的勒索软件工具和服务，为这一网络犯罪领域提供了超强的动力，并使威胁者，甚至只是技术能力有限的 IT 人员，能够发起极具破坏性的攻击。一个完整的 RaaS 生态系统已经形成，网络犯罪分子现在各自扮演着特定的角色，他们中的大多数可能与实际发起的攻击无关。这些角色包括：识别未知的漏洞，获得初始访问权，开发恶意软件，处理任何支付的赎金，甚至处理谈判事宜。

对保险业的影响

“明示”的网络保险保单通常涵盖与网络攻击有关的外部费用（例如，取证调查、数据/系统恢复和危机管理费用）、营业中断成本、对受攻击影响的第三方责任以及任何已支付的赎金。勒索软件是导致过去两年网络保险公司承保业绩明显恶化的一个重要因素。总体而言，美国网络保险的损失率从 2019 年的 44.6%上升到了 2020 年的 66.9%，根据贝氏评级(AM Best)的数据，勒索软件占索赔的四分之三。[1]

最近的指标显示，索赔环境没有实质性的改善，勒索软件仍然是一个关键的驱动因素。在索赔压力持续上升的背景下，即便去年网络保险的费率大幅上升，但 2021 年网络保险公司的损失率仍然居高不下。

持续的政策辩论

通过支付赎金，企业也有可能激励勒索软件犯罪分子，并在此过程中增大未来对自己或他人的攻击风险。尽管无论勒索软件攻击的受害者是否投保，这种外部性的经济威胁都会存在，但一些行业外的评论人士表示担心，保险的存在可能会鼓励对已投保的机构进行有针对性的勒索软件攻击，从而使情况变得更糟。例如，2021 年的一项研究显示，70%的受访英国 IT 安全专业人士认为，向支付了勒索软件要求的公司支付保险赔付会加剧问题，并引发更多的攻击。[2]一些政府还暗示了保险可能对利用勒索软件进行勒索产生的非蓄意的影响，指出要求的赎金往往是根据网络保单下的保险金额量身定制的。

这重新引发了一场政策辩论，即政府应在多大程度上进行干预，以减轻与赎金有关的经济外部性——也就是说，利用法律、法规和税收来确保受害者公司意识到，支付赎金可能会助长更多勒索软件的出现，并提高未来的勒索要求。

一些国家正在就完全禁止支付赎金的可能性进行政策辩论。其理由是，如果禁止支付赎金或对赎金支付的保险赔付，勒索软件受害者就不太可能付款给网络犯罪分子。而如果勒索软件受害者不支付或减少他们愿意支付的金额（由于缺乏保险赔付作为潜在的资金来源），黑客要求赎金的动机也会降低。[3]

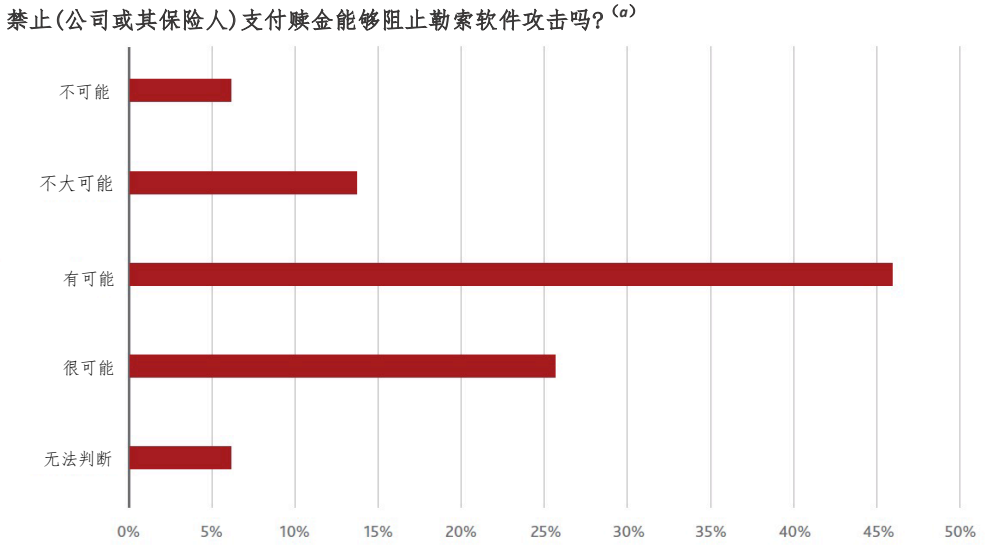
禁止支付赎金并非真正的解决办法

在实践中，针对勒索软件并没有简单的解决方案，而且此类措施往往涉及到重要的权衡，尤其是由于潜在的意外后果。例如，完全禁止支付赎金可能会使这类交易转入地下，并/或鼓励勒索软件攻击者进行新形式的勒索，包括威胁在其要求得不到满足的情况下摧毁财产或造成人身伤害。

日内瓦协会对网络保险与再保险公司的一项调查显示，尽管多数人认为禁止赎金支付或禁止相关的保险赔付可能会阻止一些勒索软件的攻击（图 2），但这种生硬的政策反应可能并不总能得到期望的效果，特别是如果禁令没有在国际层面上得以一致实施的话。仅仅禁止保险公司赔付将是特别无效的，在其它形式的风险融资可能难以组织时，就剥夺了受害者一种重要的保护手段。缺失网络保险对勒索付款的保障，不仅对被保险人不利，而且对遏制助长勒索软件攻击的 RaaS 的增长也毫无帮助。

[2] Talion 2021.
[3] Logue and Shniderman 2021.

图2：再保险人/保险人对禁止赎金的看法



(a) 基于对活跃在全球网络保险市场的15家再保险/保险公司的抽样调查

资料来源：日内瓦协会

意大利在上世纪 90 年代的绑架经验突显了任何赎金禁令的挑战。意大利政府在 1991 年规定支付赎金是非法的，此举被广泛认为是随后绑架率趋于平缓的原因。但这种威胁并没有完全消失，因为被绑架的意大利公民的家人只是停止向当局报告犯罪个案。如果勒索软件的赎金支付被禁止，受害公司可能会寻求掩盖攻击，并通过非官方机制支付赎金以避免被发现。这可能意味着，关于新的勒索软件的学习和培训将在很大程度上被忽视。

网络保险是解决方案的组成部分

虽然勒索赎金经常成为头条新闻，但与勒索软件攻击有关的总损失则远远超过勒索要求。保险在帮助公司应对因勒索软件攻击而导致的各种自身和第三方损失方面发挥着重要作用。在遭受攻击后，网络保险可以作为一种机制，召集合适的专家团队包括法律顾问和计算机取证分析员，以评估事件并对如何及时应对提出建议。这些专家通常具有宝贵的谈判技巧，可以帮助降低实际支付的赎金——这主要是因为他们能够很好地评估威胁的可信度，包括解密密钥的可行性和恢复运营的可能性。

除了为勒索软件受害者提供所需的业务和财务支持以帮助他们尽快恢复外，网络保险还可以为网络风险的整体管理做出重要贡献。保险可以通过促进对勒索软件和其它网络犯罪风险的认识，分享风险管理的专业知识以及鼓励在防范和缓解风险方面进行投资，从而对网络安全标准和最佳实践产生积极的影响。例如，通过直接或与专业网络安全公司合作的方式，为运营商持续监控威胁网络环境的因素，指出公司网络和系统中可能不为投保人所知的漏洞和弱点。同样，通过现有保险保障的条款和条件，保险和再保险公司可以激励投资于良好的网络环境，以大大降低勒索软件和其它网络攻击的机会。保险的这些核心益处需要与为应对网络犯罪分子勒索软件攻击而产生的任何不经意的和不良的激励效应进行权衡。

政府和监管机构必须进一步应对勒索软件攻击

对付勒索软件没有灵丹妙药，需要采取多方面的举措来减少潜在的驱动因素，限制其影响并确保企业的复原力。政府及其监管机构在改善网络空间安全和帮助合法企业在赢得对抗网络对手的先机方面可以发挥重要作用。表 1 列出了保险和再保险公司对保单内容的建议，旨在阻止勒索软件攻击，破坏网络犯罪分子的运营模式，使企业和机构能更好地抵御入侵以及更有效地应对攻击。

表1：再保险/保险公司对政府打击勒索软件可能采取的政策建议

目 标	政 策 建 议
威慑	•确保对实施勒索软件攻击的网络犯罪分子实施更严厉的惩罚。 •促进禁止与被禁实体交易的制裁制度的国际协调，包括分享有关重新命名的勒索软件的情报。
阻止	•要求加密货币交易和点对点(P2P)平台在创建账户和监测交易时遵守尽职调查的标准，包括额外的“了解你的客户”(KYC)和可追溯性要求。 •追究、起诉和公布无证交易所和加密货币交换服务的非法活动。
防备	•推进最低限度的网络安全标准，并建立鼓励最佳实践的机制（例如公共复原力标准，如最低安全准则和事件响应支持，以特别帮助中小企业）。 •加强勒索软件事件的披露机制（可能包括在不会使威胁加剧的时间表内强制向当局报告某些部门或行业的事件），并公布更多的威胁情报，以帮助企业加强网络防御，提高对威胁者新的敲诈手段、技术和程序(TTPs)的认识，并促进信息共享（如解密密钥）。 •加强对云供应商等关键网络基础设施的责任，以提高数字资产的整体复原力。
应对	•开发更强的应对能力，以追究/起诉勒索软件攻击的肇事者，并追回赎金，使执法机构之间的协调和行动更加一致。 •设立政府资助的机构以支持网络犯罪受害者机构，尤其是小公司。 •不断提升公共当局和执法部门打击网络犯罪的专业知识和技能。

资料来源：日内瓦协会

其中许多建议已反映在各国政府已经宣布的措施中，以加强在最近勒索软件侵袭事件出现后的网络安全。特别是，改进跟踪、监测和分享有关勒索软件信息的机制应该是十分有益的。由政府资助的安全机构收集的威胁情报可用于识别和追踪网络罪犯。它还可以就有效的反击措施和解密工具向受害者提供预先警告和指导，以遏制恶意软件的任何传播。

还需要有更严格的加密货币法规来帮助识别和根除非法交易，加强加密货币追踪、取证和其它区块链智能工具以追回被盗资金——特别是为了应对新兴趋势，如采用保护隐私的加密货币和使用去中心化的交易所，这些趋势使调查在线犯罪和执行制裁变得困难。[4]连同高调的公开缉获，这将起到威慑作用：如果网络犯罪分子知道执法部门可以扣押他们的加密货币，可能会降低他们在未来使用它的动机。

政策也可以鼓励企业增强抵御勒索软件攻击的能力。独立保单的网络保险总保费在全球财产和意外险市场的占比尚不足 1%，而一些报告显示，仅有大约三分之一的小企业购买了这种保障。随着网络风险的增加趋势，培育这一小众然而新兴的保险市场的政策措施将有助于确保网络空间的全部社会效益得以实现。

参考文献

AM Best. 2021. Best's Market Segment Report: Ransomware and aggregation issues call for new approaches to cyber risk. https://news.ambest.com/presscontent.aspx?refnum=30762&altsrc=9

Clark, R., S. Kreps, and A.Rao. 2022. Shifting Crypto Landscape Threatens Crime Investigations and Sanctions. Brookings TechStream. 7 March. https://www.brookings.edu/techstream/shifting-crypto-landscape-threatens-crime-investigations-and-sanctions/

K. Logue and A. Shniderman. 2021. The Case for Banning (and Mandating) Ransomware Insurance. https://repository.law.umich.edu/law_econ_current/207/

Talion. 2021. Ransomware Perceptions Report, 2021. https://talion.net/wp-content/uploads/2021/08/Talion-Report_final.pdf

[4] 例如，Monero 利用了一些增强隐私的技术，如模糊 IP 地址，以掩饰那些参与交易者的身份，并提高编码器的可替代性。Clark et al. 2022.