网络犯罪的产业化

独行黑客被成熟的企业所替代

塔玛斯·盖多施

网络犯罪如今已发展成为成熟产业，运作的原则和追求利润的合法企业大致相同。要扼制网络犯罪的激增就要破坏其商业模式，即使用易操作的工具以低风险获得高收益的商业模式。

20 世纪 80 年代末赫赫有名的独行黑客已经不复存在，当时他们黑入他人电脑的主要目的是为了炫耀 99 级的电脑奇才技能。从上世纪 90 年代开始，黑客界逐渐转向盈利模式，形成了如今的网络犯罪产业，这一产业有着所有正常企业的一切特征，包括市场、交易所、专业运营商、外包服务提供商、集成供应链等等。而一些国家已经采用同样的技术研发了高效的网络武器，用于情报搜集、产业间谍活动和破坏对手脆弱的基础设施。

演变

想要成功实施黑客行为并获利而不受到惩罚，需要越来越高超的技术水平，虽然能够做到这一点的技术高超的专业人士并不多，但网络犯罪依然在激增。先进的工具和自动化弥补了缺陷。过去的二十年里，黑客工具有了惊人的发展。20 世纪 90 年代，用所谓的渗透测试在计算机系统中寻找漏洞，这一方法曾在业内风靡一时。当时可用的大多数工具都很简单，通常都是定制的，操作者必须谙熟编程、网络协议、操作系统内部构成以及其他深层技术知识。因此，只有少数专业人才能找到可利用的弱点并加以利用。

随着工具逐渐优化，操作更加便捷化，所要求的技能更低，但却更具吸引力，年轻人——被戏称为“脚本小子”——开始使用这些工具，并小有成就。如今要发起网络钓鱼行动——即以可信发件人的名义发送电子邮件，诱使收信人泄露机密信息的欺诈行为——只要对其概念有一定理解、愿意这样做并有一定资金，那么就可以完成。黑客攻击变得很容易了（见图）。

众所周知，网络风险难以量化。有关数据损失的记录并不多见，而且不可靠，其部分原因在于用户缺乏报告网络损失的动机，尤其是在事件没有成为头条新闻或没有网络保险覆盖的情况下。网络攻击的迅速演变使得历史数据在预测未来损失方面并没有多大意义。

基于场景建模所计算出的那些明确定义的事件对某些经济体造成的影响的成本估计高达数百亿或数千亿美元。据伦敦劳合社估计，云服务中断持续两天半到三天时间，那么对发达经济体造成的损失将达到 530.5 亿美元。IMF 的一项建模结果显示，普通案例平均每年造成的损失总计 970 亿美元，在最坏情况下每年的损失总计有 2500 亿美元。

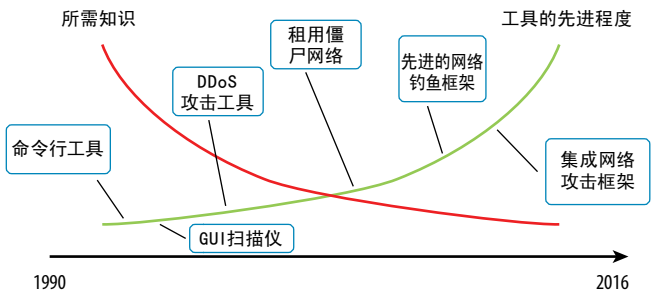
因与果

现实世界中的犯罪——以赚钱为目的——的普遍动机很简单，那就是犯罪获利可能远远高于合法业务的获利，罪犯认为冒着高风险也是值得

设计：ISTOCK/NGURHAN; VANREEEL

轻而易举

随着工具变得越来越先进，黑客所需要的技术知识越来越少，现在实施黑客攻击变得更加容易了。



资料来源：Carnegie Mellon University。
注：DDoS =分布式拒绝服务；GUI =图形用户界面。

的。而网络犯罪中，罪犯可以以更低风险获得同等利润或更高利润：被抓获和成功起诉的几率更小，而且几乎没有被枪杀的风险。据估计，网络钓鱼的盈利能力高出数百个百分点，甚至能超过1000个百分点。我们只能推测最老练的黑客通过窃取知识产权所获得的利润。但基本原理是相似的：有效的工具和企高的风险回报率太有诱惑力了，这也是网络犯罪激增和逐渐产业化的最终原因。

网络犯罪导致了几个行业的系统性风险。虽然不同行业受到的影响不同，但受影响最大的可能是金融业。以破坏性为目的黑客带来了相对新的威胁。在试图破坏金融体系稳定时，这些黑客会选择最有希望被成功攻破的目标。金融市场基础设施是最脆弱的，因为它在全球金融市场中扮演着举足轻重的角色。鉴于金融行业仅仅依赖一套相对较小的金融系统，那么成功的网络攻击导致的违约或交易延迟所带来的连锁效应可能会广泛传播，并可能产生系统性的影响。

考虑到金融行业参与者的内在联系，对支付、清算或结算系统的成功破坏——或窃取机密信息——将导致广泛的溢出效应，并威胁金融稳定。

幸运的是，迄今为止，我们遭遇的网络攻击尚未造成系统性的后果。然而，考虑到近期摧毁了ATM网络的攻击事件，以及对网上银行系统、央行和支付系统的攻击事件，政策制定者和金融监管机构越发谨慎了。

几十年来，金融行业一直依赖于信息技术，在监管规则的要求之下，长期以来一直维持着强有力的信息技术管理环境。尽管金融行业受到网络攻击的风险可能最大，但攻击金融行业的网络犯罪分子面临的风险也更高，部分原因在于执法部门对金融行业的关注更多（就像在过去抢银行一样）。金融行业在支持执法方面也做得更好——比如它们保留着大量对法庭调查有价值的记录。加大预算投入往往能催生有效的网络安全解决方案（最近一个著名的例外是Equifax公司，其被黑客入侵完全就是因为网络监管制度与其风险不相称）。

医疗行业的情况则不同。除最富裕国家以外，其他国家的医疗行业通常都没有用于有效的网络防御所需的资源。这一问题显而易见，今年针对美国的电子健康记录公司Allscripts和其他两家地方医院的计算机系统的勒索软件攻击就是例子。虽然医疗行业也受到严厉监管，也要遵守严格的数据保护规则，但医疗行业对信息技术的依赖程度不像金融行业那么高，因此也没有形成像金融行业一样严格的信息技术管理文化。这也使得医疗行业更容易受到网络入侵。这种缺陷尤其令人担忧，医行业与金融行业不同，如果攻击者攻击的是计算机控制的生命支持系统，那么有人可能会因此而丧生。

公用事业，尤其是电网和通信网络，被普遍认为是下一批大规模网络攻击可能造成严重影响的行业。但在这种情况下，最应该担心的是敌对

网络攻击对全球造成了威胁，而打击和起诉网络犯罪方面的国际合作却远远地落在了后面。

国家直接或通过代理组织对系统进行破坏或渗透。2007 年爱沙尼亚互联网基础设施遭受的大规模攻击——摧毁了在线金融服务、媒体和政府机构——生动证明了经济体越先进、越依赖于互联网，那么网络攻击就越具有破坏性。爱沙尼亚是世界上数字化程度最高的国家之一（见“爱沙尼亚电子化大获成功”,《金融与发展》2018 年 3 月号）。

对策

如果关键基础设施——比如电网或通信和交通网络受到影响，或者是网络攻击使致政府无法征税或提供关键服务，那么这可能会引发严重的混乱，造成系统性的经济后果，还可能会造成公共健康或安全隐患。在这种情况下，全球经济面临的总风险可能超过所有个人风险的总和，因为信息技术网络和平台是全球互联的，而应对结构却是以国家为单位，缺乏有效的国际合作，甚至有些国家也在攻击者之列。

网络攻击对全球造成了威胁，而打击和起诉网络犯罪方面的国际合作却远远地落在了后面。应对网络犯罪的最佳途径是打破其商业模式，即仰赖极高的风险回报率和无效起诉的模式。如此看来，必须大幅提高网络犯罪的商业风险，但这只有在加强国际合作的情况下才能得以实现。

网络犯罪的实施可以跨越几个司法管辖区，因此更加难以被摧毁和起诉。一些司法管辖区在打击网络犯罪方面行动迟缓、效率低下，或者根本不配合。只有加强合作，才可以更快、更有效地追捕和起诉嫌疑人。

在金融行业，监管机构制定了具体的评估标准，确立了可执行的前景和标准，并鼓励企业和监管机构之间信息共享和合作。银行监管机构会进行信息技术审查，将网络安全应对能力纳入压力测试、解决方案制定、安全和健康监督。一些监管机构要求专门针对每个公司模拟网络攻击，利用政府和私营部门的智慧和专业知识，来判断抵御攻击的能力。公司还加大了对网络安全的投资，并将网络安全应对能力纳入风险管理。此外，一些公司还试图通过网络保险转移一些风险。

目前的网络安全格局仍然是分散的、毫不相干的，风险主要被当作局部特殊问题来处理。虽然已有一些合作机制，各国政府和监管机构正在加强这方面的工作，但网络安全的选择很大程度上是由企业需求决定的——“各管各的”。这种情况必须改变，以求普遍增强网络风险应对能力。监管层面、技术层面以及所有行业都需要强有力的预防措施。其中最重要的是遵守网络安全最低标准，由监管机构协调执行。加强网络安全意识培训将有助于防范基本的技术缺陷和用户错误，而这正是大多数网络入侵的根源。

网络攻击和网络安全入侵似乎不可避免，因此我们也要关注检测网络入侵的速度，应对的有效性，以及恢复正常运营的效率。FD

塔玛斯·盖多施（TAMAS GAIDOSCH）是IMF货币与资本市场部高级金融专家、网络安全专业人士，拥有20多年的从业经验，包括调查银行系统以发现网络漏洞。曾担任匈牙利中央银行信息技术监督部负责人。