第2章

谁是对手？

一直追溯到早期的分时系统，我们的系统人员将用户和他们编写的任何代码视为我们和彼此的死敌。我们就像暴力贫民窟中的警察。

罗杰·李约瑟

虚假的面孔必须隐藏虚假的心所知道的

– 麦克白

2.1 简介

理论家可能会按照他们希望的方式处理世界，但工程师会按原样处理世界。如果你要保护系统免受攻击，你首先需要知道你的敌人是谁。

在计算的早期，我们大多没有真正的敌人；虽然银行和军队必须保护他们的系统，但大多数其他人并没有真正费心。第一个计算机系统是孤立的，为单个公司或大学服务。学生可能会尝试破解系统以获得更多资源，而系统管理员会试图阻止他们，但这主要是一场游戏。当拨号连接开始出现时，恶作剧者偶尔会猜测密码并留下笑话信息，就像他们在大学时所做的那样。早期的互联网是一个友好的地方，居住着学者、科技公司的工程师和一些业余爱好者。我们知道恶意软件是可能的，但几乎没有人认真对待它，直到 1980 年代后期出现 PC 病毒，随后是 1988 年的 Internet 蠕虫。（即使那是从实验室逃脱的学生实验；我在第 21.3 节中讲述了这个故事。 2.）

一旦每个人都开始上网，情况就发生了变化。 20 世纪 90 年代中期出现了第一批垃圾邮件，1990 年代后期出现了第一次分布式拒绝服务攻击，互联网繁荣时期邮购业务的爆炸式增长引发了信用卡欺诈。首先，在线欺诈是一种家庭手工业；同一个人

会窃取信用卡号并用它们购买商品,然后再出售,或者伪造信用卡以在商店中使用。随着地下市场的出现,情况在 2000 年代中期发生了变化。这些让坏人专业化 一个团伙可以编写恶意软件,另一个团伙可以获取银行凭证,还有一些团伙可以想出套现的方法。这使他们能够做好自己的工作,扩大规模并走向全球化,就像 18 世纪后期制造业所做的那样。 2000 年代还见证了世界各国政府努力“掌握互联网”(正如美国国家安全局所说) 研究如何大规模收集数据并将其编入索引,就像谷歌所做的那样,以供分析师使用.

它还看到了社交网络的出现,这样每个人都可以在网上拥有一个家 而不仅仅是拥有创建自己的手工网页技能的极客。当然,一旦每个人都在线,这不仅包括间谍和骗子,还包括混蛋、变态、种族主义者和恶霸。

在过去十年中,这种威胁形势已经稳定下来。我们对此也了解很多。感谢埃德·斯诺登和其他举报人,我们对西方情报部门的能力和手段有了很多了解;我们还了解了很多有关中国、俄罗斯和其他民族国家威胁者的信息。我们对网络犯罪了解很多;按数量和价值计算,网络犯罪现在约占所有犯罪的一半。有大量基于恶意软件和僵尸网络的犯罪基础设施,我们一直在与之抗争;还有一个庞大的诈骗生态系统。许多传统的犯罪活动都在网上进行,一家典型的公司不仅要担心外部欺诈者,还要担心不诚实的内部人员。

一些公司不得不担心敌对政府,一些公司担心其他公司,还有一些公司担心活动家。许多人不得不应对网上的敌意,从在学校遭受网络欺凌的孩子到骚扰民选政客的人,再到被前伴侣跟踪的人。由于网络极端主义的发展,我们的政治可能会变得更加两极分化。

安全工程师在处理新问题时需要做的第一件事就是确定可能的对手。尽管您可以设计一些特定的系统组件(例如密码学)来抵御所有合理的对手,但对于复杂的现实世界系统而言,情况并非如此。您无法保护它免受所有可能的威胁,并仍然期望它以合理的成本完成有用的工作。那么对手将拥有什么样的能力,以及什么动机呢?您对此评估的确定程度如何,它在系统的生命周期内会发生怎样的变化?在本章中,我将根据动机对在线威胁和电子威胁进行分类。首先,我将讨论政府出于国家原因进行的监视、入侵和操纵,从网络情报到网络冲突行动。其次,我会处理以金钱为主要动机的罪犯。第三种是研究人员,他们为了乐趣或金钱而发现漏洞,或者出于社会良知而报告漏洞 迫使公司修补他们的软件并清理他们的运营。最后,我将讨论出于个人原因且主要对人实施犯罪的不良行为者,从网络恶霸到跟踪狂。

微软、谷歌和 Facebook 等大型服务公司不得不担心所有四类威胁。大多数公司和大多数个人只会关心其中的一些。但是对于安全工程师来说,了解大局很重要,这样您就可以帮助客户确定他们自己的威胁模型应该是什么,以及他们应该计划预防什么样的攻击。

2.2 幽灵

政府拥有一系列用于网络被动监视和计算机系统主动攻击的工具。数百家公司出售用于窃听、无线电拦截以及利用各种漏洞接管计算机、电话和其他数字设备的设备。然而，各国政府在规模、目标和能力方面存在显着差异。我们将从潜在对手的角度讨论四个具有代表性的类别 美国及其盟友、中国、俄罗斯和阿拉伯世界。即使 spooks 不在您今天的威胁模型中，他们使用的工具迟早也会经常落入骗子手中。

2.2.1 五眼联盟

正如某个年龄段的每个人都记得约翰·列侬被枪击时他们在哪里，自 2013 年以来从事我们行业的每个人都记得当年 6 月 7 日星期五得知斯诺登泄密事件时他们在哪里。

2.2.1.1 棱镜

我当时在加利福尼亚州帕洛阿尔托的一家旅馆里，在计划访问谷歌之前在线阅读《卫报》，我在 2011 年曾作为科学访问者访问过谷歌，帮助开发适用于 Android 手机的非接触式支付。标题是“NSA 棱镜计划利用苹果、谷歌和其他公司的用户数据”；这篇由 Glenn Greenwald 和 Ewen MacAskill 撰写的文章描述了一个名为 Prism 的系统，该系统收集非美国公民或永久居民用户的 gmail 和其他数据，并根据 FISA 法院的命令执行 [817]。早餐后我开车去了 Googleplex，发现我以前的同事和我一样困惑。他们对棱镜一无所知。 gmail 团队也没有。怎么会建立这样的窃听器？是否已向 Eric Schmidt 发出命令，如果是，他如何在邮件和安全团队不知情的情况下执行命令？日子一天天过去，人们不再说话了。

事实证明，Prism 是 NSA 的一个访问通道的内部代号，已提供给 FBI 以进行有保证的窃听。美国法律允许对美国公民进行窃听，前提是一个机构说服法院根据“可能的原因”证明他们没有做好事；但外国人可以自由窃听。因此，对于像我这样的外国目标，NSA 情报分析师所要做的就是点击一个标签，说他认为我是非美国人。查询将通过 FBI 基础设施自动路由，并将我的 Gmail 传送到他们的工作站。文章称，该项目于 2007 年在微软启动；雅虎曾在法庭上与之抗争，但败诉，并于 2008 年底加入；谷歌和 Facebook 于 2009 年加入，苹果终于在 2012 年加入。人们认为该系统正在为执法部门提供有针对性的、有保证的窃听服务，但它正在为外国情报目的提供大规模访问，根据泄露给卫报的幻灯片显示，它

是“ NSA 报告中最常用的 SIGAD1 ”。

第二天,我们得知故事的来源是爱德华·斯诺登,一位决定举报的美国国家安全局系统管理员。故事是他用记忆棒从夏威夷的一个设施中走私了 50,000 多份机密文件,并在香港会见了卫报记者 [818]。

6 月 21 日,他试图飞往拉丁美洲寻求庇护,但在美国政府取消他的护照后,他被困在莫斯科,最终在俄罗斯获得庇护。一个报纸联盟协调了一系列故事,描述了“五眼联盟”国家 美国、英国、加拿大、澳大利亚和新西兰 的信号情报能力,以及这些能力如何不仅被使用而且被滥用。

基于泄露文件的第一个故事实际上比棱镜故事早两天出现;这是关于 FISA 法院如何在当年 2 月命令 Verizon 将所有通话数据记录 (CDR) 移交给 NSA [814]。这并没有引起安全专业人员的太多关注,因为我们知道这些机构无论如何都会这样做。但它肯定引起了律师和政治家的注意,因为它在隐私法学者会议期间被打破,并表明美国国家情报总监詹姆斯克拉珀在作证说国家安全局收集美国人的国内通讯时向国会撒谎“只是不经意 。接下来发生的事情改变了一切。

2.2.1.2 时间

6 月 21 日,媒体刊登了有关 Tempora 的报道,这是一个从国际光纤电缆收集情报的程序 [1199]。这并不完全出乎意料;记者 Duncan Campbell 在 1988 年描述了一个名为 Eche lon 的系统,该系统利用 Intelsat 卫星网络,将语音通话保存在磁带上,同时使元数据可用于搜索,以便分析人员可以选择与感兴趣的电话号码之间的通话 [373、374]（我将在第 26.2.6 节中提供更多历史背景）。斯诺登向我们介绍了这项技术的最新情况。仅在康沃尔,就有 200 根跨大西洋光纤被挖掘出来,并且可以同时收集到 46 根。由于其中每一个都承载 10Gb/s,每天的总数据量可能高达 21Pb,因此传入的数据馈送经历了大规模的缩减,丢弃了视频、新闻等。然后使用选择器选择材料 不仅是电话号码,还有更通用的搜索词,如 IP 地址 并存储 30 天,以备感兴趣时使用。

与之前的 Echelon 一样,Tempora 计划有大量英国参与。
英国拥有大约四分之一的互联网骨干网的物理接入,因为现代电缆往往走在过去电话线所在的地方,而且它们通常铺设在与 19 世纪电报电缆相同的终端站之间。因此,英国的主要情报资产之一原来是它为控制其 19 世纪帝国而建造的通信基础设施的遗产。

这项资产确实意义重大:到 2012 年,来自 GCHQ 的 300 名分析师和来自 NSA 的 250 名分析师每天分别使用 40,000 和 31,000 个选择器筛选 6 亿“电话事件”。

1SIGINT（信号情报)活动指示符

2.2.1.3 肌肉发达

在 Tempora 之上运行的应用程序之一是 Muscular。 10 月 30 日透露,它收集了在雅虎和谷歌等大型服务公司的数据中心之间流动的数据 [2016]。您的邮件在发送到服务前端的途中可能已使用 SSL 加密,但随后在每个公司的数据中心之间以明文形式流动。在《华盛顿邮报》上发布了关于“谷歌云利用”的 NSA PowerPoint 幻灯片后（见图 2.1）,公司争先恐后地加密其网络上的所有内容。云服务公司的高管和工程师将笑脸视为一种人身攻击。

它提醒业内人士,即使你遵守了搜查令,间谍也会对你进行黑客攻击。它让行业外的人停下来思考:谷歌通过搜索、邮件、地图、日历和其他服务积累了如此多的访问我们所有生活的机会,以至于不受限制的情报服务访问其记录（以及 Facebook 和微软的记录)是一个重大隐私泄露。

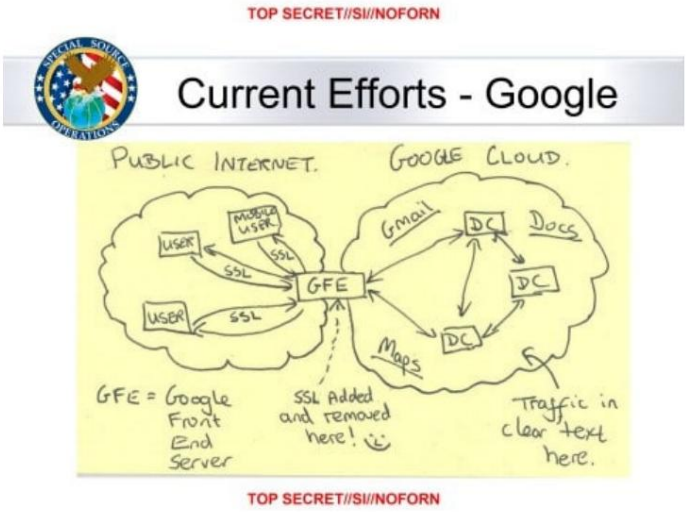

图 2.1:肌肉发达　幻灯片

两年后,在斯诺登以远程呈现机器人的形式参加的普林斯顿会议上,他指出许多看似加密的互联网通信实际上并非如此,因为现代网站使用内容分发网络 (CDN)例如 Akamai 和 Cloudflare;虽然从用户的笔记本电脑或手机到 ISP 的 CDN 存在点的网络流量是加密的,但它在回程上没有加密,除非他们支付额外费用　他们中的大多数人不支付额外费用 [86]。因此,客户认为该链接是加密的,并且可以防止随意窥探　但不是来自可以读取骨干流量的国家或公司。

2.2.1.4 专项征集

美国国家安全局和中央情报局联合运营特别收集服务 (SCS),其最明显的活动可能是美国和盟国屋顶附近的塑料板

世界各地的大使馆;这些隐藏的天线用于收集蜂窝通信（称为“Stateroom”的程序）。除此之外,SCS 还在外国电信公司、互联网交换中心和政府设施中植入收集设备。这可能涉及经典的间谍技术,从放置监控语音或电子通信的窃听器,到在目标组织中招募间谍,再到在目标国家秘密部署天线以窃听内部微波链路。此类技术不仅限于国家目标:墨西哥贩毒集团电话头目“El Chapo”Guzman 在美国特工收买他的系统管理员后被捕。

近距离访问操作包括 Tempest 监视:收集由计算机监视器和其他设备的电磁辐射泄露的信息,如 19.3.2 中所述。斯诺登泄密事件披露了从许多国家的大使馆和联合国代表团（包括印度、日本、斯洛伐克和欧盟)收集的计算机屏幕数据和其他电磁辐射。2。

2.2.1.5 Bullrun 和 Edgehill

特殊收集越来越多地涉及供应链篡改。 SCS 会例行拦截从美国出口的路由器等设备,添加监控植入物,用工厂封条重新包装,然后将它们发送给客户。供应链篡改的一种极端形式是美国国家安全局秘密收购了瑞士公司 Crypto AG,该公司是冷战期间向不结盟国家提供加密设备的主要供应商;我稍后将在第 26.2.7.1 节中更详细地讲述这个故事。

Bullrun 是 NSA 的代号,而 Edgehill 是 GCHQ 的代号,意为“启用加密货币”,这是一项每年 100 美元的计划,旨在篡改堆栈各级的供应和供应商。这始于 o 试图指导或误导学术研究3;它继续将受信任的人置于标准委员会中,并利用 NIST 的影响力来采用弱标准。一个引人注目的事件是 Dual EC_DRBG 崩溃,其中 NIST 标准化了一个基于椭圆曲线的随机数生成器,结果发现它包含一个 NSA 后门。然而,大部分实际损害是由于对加密密钥长度的限制造成的,与对盟国实施出口管制的外交压力相吻合,因此需要出口许可证的公司可能会被迫使用“适当的”标准,并且是与加密战争纠缠在一起（我在第 26.2.7 节中讨论）。结果是今天使用的许多系统被迫使用弱加密,导致从酒店和汽车门锁到 VPN 的一切都存在漏洞。除此之外,供应链攻击将隐蔽的漏洞引入广泛使用的软件中;许多民族国家和一些私人演员一起玩这个游戏 [890]。我们将看到由监视和加密策略合二为一的漏洞

2如果 NSA 需要使用高科技收集来对付你,因为他们无法获得软件
植入你的电脑,这可能是一种恭维！

3 在 1990 年代,当我申请在剑桥大学艾萨克牛顿研究所开展一个关于编码理论、密码学和计算机安全的研究项目时,GCHQ 的一位高级官员向该研究所提供了 50,000 英镑的捐款,但他说“密码学中没有发生任何有趣的事情,女王陛下政府希望这种情况继续下去”。他被领到了门口。

一章又一章,并返回本书的第 3 部分,更详细地讨论政策历史。

2.2.1.6 Xkeyscore

拥有如此庞大的数据集合,您需要好的工具来搜索它。五眼联盟使用 Xkeyscore 搜索计算机数据,
Xkeyscore 是一个分布式数据库,使分析师能够远程搜索收集的数据并汇总结果。

2013 年 7 月 31 日公开的美国国家安全局文件将其描述为“影响最广泛”的情报发展系统;它使分析师能够搜索电子邮件、短信、聊天、地址簿条目和浏览历史记录 [815]。 2008 年的训练套牌中的例子包括“我的目标说德语,但在巴基斯坦。我怎么才能找到他?” “向我展示来自伊朗的所有加密 Word 文档”和“向我展示伊朗的所有 PGP 使用情况”。通过搜索异常行为,分析师可以找到嫌疑人并识别强选择器(例如电子邮件地址、电话号码或 IP 地址)以进行更常规的收集。

Xkeyscore 是一个联合系统,其中一个查询扫描所有站点。它的组件在收集点缓冲信息 2008 年,150 个站点有 700 台服务器。
有些似乎是被黑客入侵的海外系统,NSA 恶意软件可以从中泄露与提交的查询相匹配的数据。唯一需要的司法批准是提示分析师输入他们认为对话的一方不居住在美国的原因。这些卷使得 trac 数据保留 30 天,但内容仅保留 3-5 天。任务项目被提取并发送给任何请求它们的人,并且有一个通知系统(Tracthief),用于在他们的目标做任何感兴趣的事情时提示 o 分析师。提取基于指纹或插件 后者允许分析师使用检测器快速响应隐写术和自制加密等新挑战。

Xkeyscore 也可用于目标发现:训练查询之一是“显示 X 国所有可利用的机器”(机器指纹由名为 Mugshot 的爬虫编译)。例如,2015 年,GCHQ 和 NSA 入侵了世界领先的 SIM 卡供应商,法国-荷兰公司 Gemalto,以破坏拦截(如果需要欺骗)数亿流量所需的密钥手机 [1658]。黑客使用 Xkeyscore 来识别公司的系统管理员,然后他们被钓鱼了;代理人还能够破坏计费服务器以抑制 SMS 计费和身份验证服务器窃取密钥;另一种技术是在从 Gemalto 到移动服务提供商的传输过程中收集密钥。根据 2014 年对斯诺登的采访,Xkeyscore 还可以让分析师为任何目标的在线活动建立指纹,以便在全球范围内自动跟踪他们。据称,该系统的成功包括抓获 300 多名恐怖分子;在一个案例中,基地组织的 Sheikh Atiy atallah 通过谷歌搜索自己、他的各种别名、一名同伙和他的书名 [1658],从而暴露了他的身份。

Xkeyscore 上有一组套牌,其中包含 Morgan Marquis 的一项调查
Boire, Glenn Greenwald 和 Micah Lee [1230];仔细阅读甲板

可以作为探索斯诺登宝藏的良好起点4。

2.2.1.7 长途

批量密钥盗窃和供应链篡改并不是破解密码学的唯一方法。 Xkeyscore training deck 给出了一个例子：“给我看看 X 国所有的 VPN 初创公司,并给我数据,这样我就可以解密和发现用户”。 VPN 似乎很容易被击败;名为 Longhaul 的解密服务提取密文并返回明文。密码分析技术的详细描述被保存为极端隔离信息 (ECI),在斯诺登的论文中找不到,但其中一些谈到了密码分析的最新突破。这些可能是什么？

泄漏确实显示了用于设置 VPN 加密的协议消息的勤奋收集,因此一些密码学家在 2015 年建议，“Logjam 攻击”的某些变体对于民族国家攻击者来说是可行的,以针对大多数 VPN 使用的 1024 位素数以及许多使用 Die-Hellman 密钥交换的 TLS 连接 [26]。其他人指出 NSA 密码学家参与了相关标准,以及后来发现的协议缺陷;然而其他人指出,即使在数论或协议漏洞利用方面取得了进步,美国国家安全局也有足够的资金通过蛮力简单地破解 1024 位 Die-Hellman,如果许多人使用相同的少量素数模数,这将很容易证明是合理的– 他们这样做 [853]。我将在第 5 章更详细地讨论密码分析。

2.2.1.8 量子

对协议的攻击由来已久,可以通过各种方式进行欺骗、重放和操纵。 （我们将在第 4 章详细讨论这个主题。）记录最详尽的 NSA 对 Internet trac 的攻击代号为 Quantum,涉及对通信端点之一的动态利用。因此,为了将加密的 SSL/TLS 会话接入网络邮件提供商,Quantum 系统会触发一个利用浏览器的“攻击”。

有多种口味;在“Quantuminsert”中,注入的数据包将浏览器重定向到“Foxacid”攻击服务器。其他变体攻击软件更新和代码在手机应用程序中运行的广告网络 [1995]。

2.2.1.9 CNE

计算机和网络利用 (CNE) 是 NSA 的通用黑客攻击术语,它不仅可用于窃取密钥或 TLS 会话劫持;它也可用于获取对 trac 的访问权限。 Operation Socialist 是2010-11 年比利时主要电信公司 Belgacom5 遭到黑客攻击的 GCHQ 代号。

GCHQ 攻击者使用 Xkeyscore 识别出三个关键的 Belgacom 技术人员 ,然后在他们访问 LinkedIn 等网站时使用 Quantuminsert 接管他们的 PC。然后攻击者使用他们的系统管理员权限安装恶意软件

4该系列还有一个搜索引擎,网址为 https://www.edwardsnowden.com。
5 它现在被称为 Proximus。

在数十台服务器上,包括用于进一步访问的身份验证服务器、用于掩盖其踪迹的计费服务器,以及公司的核心 Cisco 路由器 [734]。这使他们能够访问大量移动漫游流量,因为当 Belgacom 的用户在欧洲漫游时,他们会向许多外国提供商提供服务。一个北约和欧盟成员国将对另一个国家的关键基础设施进行网络攻击的想法让许多人感到意外。

这次攻击还让 GCHQ 可以访问欧洲委员会和其他欧洲机构的电话系统。鉴于这些机构为英国和其他成员国制定了许多法律,这几乎就像美国州长让他的州警入侵 AT&T,以便窃听国会和白宫一样。

Belgacom 的工程师在 2012 年开始怀疑出了什么问题,并在 2013 年春天意识到他们遭到了黑客攻击;一家反病毒公司发现复杂的恶意软件伪装成 Windows 文件。这个故事于 2013 年 9 月公开,德国新闻杂志 Der Spiegel 发布了斯诺登文件,显示 GCHQ 对此负有责任。经比利时检察官2018年2月通报后,我们得知此次袭击一定是得到了时任英国外交大臣威廉·黑格的授权,但没有足够的证据起诉任何人;调查在技术和政治方面受到各种阻碍;该软件在被发现后几分钟内开始自行删除,而欧洲刑警组织（其负责人是英国人)等机构拒绝提供帮助。负责电信的比利时部长 Alexander de Croo 甚至暗示,比利时自己的情报部门可能已经非正式地为该行动开了绿灯 [735]。欧洲刑警组织后来通过了一项政策,它将帮助调查“涉嫌犯罪”的黑客行为;它与政府的黑客行为无话可说。

CNE 上的 GCHQ 幻灯片解释说,它用于通过重定向 trac 和“启用”（破解)加密来支持传统的信号;它必须始终是“英国可否认的”;并且它也可以用于“效果”,例如降低通信质量或“更改极端主义网站上的用户密码”[735]。其他论文表明,这些机构经常以中东、非洲乃至全世界的电话公司和 ISP 的管理员为目标危害关键技术人员“通常是进入网络的入场券”[1139]。正如一位电话公司高管所解释的那样,“移动网络运营商当时对网络安全一无所知。大多数网络都向其供应商开放,以使用 ID 和密码进行远程维护,而中国或印度的技术人员不知道他们的 PC 已被黑客入侵”。

美国国家安全局及其盟友使用的黑客工具和方法现在已广为人知;有些与执法部门共享。斯诺登文件揭示了一个内部商店,分析师可以在那里获得各种工具； Shadow Brokers（被认为是俄罗斯军事情报机构,GRU)在 2016-7 年的一系列泄密事件中披露了一些实际的 NSA 恶意软件样本,NSA 的 Tailored Access Operations 团队的黑客使用这些样本发起攻击 [238]。

（其中一些工具被俄罗斯人重新用于发射 NotPetya 蠕虫病毒,而朝鲜人则将其用于 Wannacry,我将在后面讨论。)最好的文件可能是关于中央情报局使用的一个单独的好东西的存储,披露在 2017 年的“Vault 7”泄漏中向 Wikileaks 提供了一些细节。其中包括可用于安装远程访问木马的工具手册

在你的机器上,带有用于定位它和泄露文件（包括 SSH 凭据）、音频和视频的组件;一种通过感染拇指驱动器来跳过气隙的工具;一种感染 wifi 路由器的工具,因此它们会进行中间人攻击;甚至还有一个给文件加水印的工具,这样泄露文件的举报人就可以被追踪到。许多工具不仅适用于 Windows,也适用于 OSX 和 Android;一些感染固件,使它们难以删除。也有用于入侵电视和物联网设备的工具,以及阻碍法医调查的工具。如果您对现代政府恶意软件 [2019] 的规范和手册感到好奇,那么 Vault 7 文档很有用。作为执法部门使用此类工具的一个例子,2020 年 6 月,里尔的法国警方自 2018 年以来在数千部运行 EncroChat 的 Android 手机上安装了恶意软件,EncroChat 是一种受犯罪分子青睐的加密消息系统,导致逮捕了在法国、荷兰、英国和其他地方逮捕了 800 名犯罪嫌疑人,并逮捕了几名因腐败而被捕的警察,并没收了数吨毒品 [1332]。

2.2.1.10 分析师的观点

因此,情报分析师拥有一大袋工具。如果他们试图找到组织中的关键人物 无论是为关键决策提供建议的决策者,还是参与洗钱寡头利润的律师 他们都可以使用 Xkeyscore 中的 trac 数据来绘制联系网络。有各种简洁的工具可以提供帮助,例如“Cotraveler”,它可以标记一起旅行过的手机。通过我们自己对网络犯罪的研究,我们对这一过程有了一些了解,我们从地下论坛中收集了数千万条消息并对其进行分析,以了解新旧犯罪类型。可以将这一过程描述为“自适应消息挖掘”。正如您在进行 Web 搜索时使用自适应文本挖掘,并根据您找到的内容样本不断优化搜索词一样,通过消息挖掘,您还拥有元数据 因此您可以关注线程、跨论坛跟踪参与者、进行聚类分析并使用各种其他技巧来“找到更多像这样的消息”。在阅读单个消息获得的详细视图和分析批量集合获得的统计视图之间来回切换的能力非常强大。

一旦分析师从搜索阶段进入收集阶段,他们就可以使用 Prism 查看目标在 Facebook、谷歌和微软的账户,而 Xkeyscore 将让他们看到他们访问了哪些网站。 Trac 数据分析还提供了更多信息:尽管加密技术的使用越来越多,但进出家庭的通信揭示了用户在何时使用了哪些应用程序或设备以及使用了多长时间6。这些机构正在推动访问 WhatsApp 等端到端消息系统;在英国、澳大利亚和中国等国家,立法者已经授权这样做,尽管尚不清楚哪些美国公司可能会遵守（我将在第 26 章讨论政策）。

鉴于高价值目标,分析师可以直接在他们的笔记本电脑或手机上安装一大袋工具。他们可以对其进行物理定位,将其变成房间窃听器,甚至将其用作远程摄像头。他们可以下载

6 例如,Hill 和 Mattu 窃听了现代智能家居来衡量这一点 [900]。

目标的地址簿和联系人历史记录,并将其输入 Xkeyscore 以递归搜索他们的直接和间接联系人。同时,分析师可以窃取消息应用程序的漏洞,通过在通话内容被解密后收集通话内容来击败端到端加密。他们可以设置警报,以便在目标发送或接收感兴趣的消息或更改位置时通知他们。

覆盖范围相当完整。到了杀戮时刻,目标的手机可以用来引导炸弹或导弹。难怪埃德·斯诺登坚持要采访他的记者把手机放在冰箱里!

最后,分析师还有一个代理,他们可以通过代理秘密访问互联网 通常是僵尸网络上的一台机器。它甚至可能是您家中的 PC。

2.2.1.11 攻击性操作

美国国家安全局局长还领导美国网络司令部,该司令部自 2009 年以来一直是美国国防部的十个统一司令部之一。
它负责攻击性的网络操作,其中真正与众不同的是 Stuxnet。这是一种蠕虫,旨在破坏伊朗的铀浓缩离心机,以旨在造成机械损坏的模式加速和减速它们,由美国和以色列联合开发 [325, 826]。它在技术上非常复杂,使用四个零日漏洞和两个被盗的代码签名证书通过 Windows PC 混杂传播,直到它发现伊朗纳坦兹浓缩工厂使用的西门子可编程逻辑控制器类型 然后它会在那里安装一个 Rootkit,可以发出破坏性命令,而 PC 向操作员保证一切都很好。它显然是使用 USB 驱动器引入的,以弥合与伊朗系统的气隙,并在副本以某种方式传播到中亚和印度尼西亚后于 2010 年曝光。随后发现了另外两种恶意软件(Flame 和 Duqu)使用类似的技巧和通用代码,对中东和南亚的许多公司进行监视;最近的代码分析工具追踪了恶意软件的血统,可以追溯到 2002 年 (Flowershop),并一直运行到 2016 年(使用 Equation Group 工具)[2068]。

Stuxnet 为其他政府敲响了警钟,它们急于获得“网络武器”并制定攻击性的网络学说 一套关于网络战士可能做什么的原则,在制定时考虑了一些理由,战略、战术和合法性。哦,零日漏洞的价格急剧上涨。

2.2.1.12 攻击缩放

计算机科学家知道算法扩展的重要性,对于攻击来说也是如此。窃听一部手机很难。您必须在嫌疑人身后驾驶无线电和密码分析设备,冒着被发现的风险,并希望当他们从一个牢房漫游到另一个牢房时,您设法捕捉到嫌疑人的信号。或者你可以用假的在他们后面开车

基站 7并希望他的手机能漫游到它,因为信号比真正的手机大;但是你也有电子检测的风险。两者都是高技能和低收益的工作:您可能有四分之一的时间会丢失信号。

因此,如果您想经常窃听巴黎市中心的某个人,为什么不窃听所有人呢?将天线放在大使馆的屋顶上,收集所有信息,将解密的电话和短信写入数据库,然后以电子方式重建会话。如果你想黑掉法国的每一个人,那就黑掉电信公司,或许可以通过破坏它使用的设备来实现。在每个阶段,资本成本都会上升,但每个水龙头的边际成本都会下降。五眼战略本质上是收集世界上的一切;建立和维护基础设施可能要花费数十亿美元,但一旦它在那里,你就拥有了一切。

这同样适用于进攻性网络行动,这更像是破坏活动。战时,你可以派遣突击队员炸毁敌方雷达站;但是如果你这样做不止一两次,你的小伙子们就会开始遇到很多哨兵。因此,我们以不同的方式扩大动能攻击 : 通过建造数百架轰炸机、大炮或 (现在)数千架无人机。那么,如何扩大网络攻击的规模,不仅要摧毁一个发电站,还要摧毁对手的整个电网?五眼联盟就是这样。就像谷歌在几千台服务器上保留了一份互联网副本,所有内容和链接都被编入索引,美国网络司令部保留了一份互联网副本,索引了世界上所有机器使用的软件版本 Mugshot 系统上面提到过 所以五眼网络战士可以立即看到哪些目标可以被哪些攻击接管。

因此,对于竞争国家来说,一个关键问题不仅仅是他们可以在多大程度上创造一些通常不受五眼联盟限制的电子空间。这是他们可以在多大程度上扩大自己的情报和进攻能力,而不必依赖美国。我们在网上看到的扫描和探测数量表明,美国国家安全局并不是唯一一个试图制造可扩展网络武器的公司。并非所有人都是民族国家。有些人可能只是军火商或雇佣军。这会引发一系列政策问题,我们将在第 3 部分中返回这些问题。现在我们将继续关注功能。

2.2.2 中国

中国现在是美国的主要竞争对手,不仅在国内生产总值方面排名第二,而且在技术强国方面也排名第二。中国人缺乏美国国家安全局的联盟网络和全球基础设施 (尽管他们正在努力工作) 。然而,在中国本土,他们要求不受限制地访问本地数据。一些美国服务公司曾经在那里经营,但麻烦接踵而至。

在 2002 年雅虎的系统被用来陷害异议人士王小宁之后,阿里巴巴于 2005 年接管了雅虎在中国的业务;但当王的妻子于 2007 年在美国法院起诉雅虎并表明雅虎在此事上误导了国会时,仍然存在争执 [1760]。2008 年,中国可用的 Skype 版本被修改,扫描消息中的敏感关键字,如果找到,用户的文本将上传到

7 这些设备在美国被称为 Stingray,在欧洲被称为 IMSI-catcher;他们进行了我们将在 22.2.1 节中详细讨论的那种中间人攻击。

服务器在中国 [1959]。 2009 年 12 月,谷歌发现了对其公司基础设施的中国攻击,这被称为“极光行动”;中国特工侵入了用于为 FBI 进行窃听的谷歌系统（见上文 Prism）,以发现他们在美国的哪些特工受到监视。谷歌已经因为为中国用户运营审查版的搜索引擎而受到批评,几个月后,他们退出了中国。此时,Facebook、Twitter 和 YouTube 已经被屏蔽。一种完全控制国内的中国战略正在出现,并通过越来越积极的海外收款得到加强。

大约从 2002 年开始,发生了一系列针对美国和英国国防机构和承包商的黑客攻击,代号为“泰坦雨”并归因于中国武装部队。根据美国对外军事研究办公室 (FMSO) 2004 年的一项研究,中国的军事学说认为该国处于与西方的战争状态;我们正在通过攻击中国来继续冷战,试图通过在互联网上向其输出颠覆性思想来推翻其共产主义政权 [1881]。中国领导人认为美国服务公司、新闻网站和匿名工具,如 Tor（国务院资助,以便中国人和其他人可以击败审查制度)与美国监视卫星和观察其军事防御的飞机是一体的。

雅虎和谷歌因此被视为公平竞争,就像洛克希德马丁和 BAe 一样。

我们自己的小组与中国人的第一次接触是在 2008 年。达赖喇嘛向我们寻求帮助,他意识到中国人在当年北京奥运会前夕入侵了他的操作系统。我的一名研究生 Shishir Nagaraja 碰巧在德里等待他的英国签证续签,所以他自愿前往位于达兰萨拉的西藏总部并进行一些取证。他发现西藏流亡政府办公室的50台PC中,大约有35台被黑;信息被窃取到中国,IP 地址位于三个负责西藏事务不同方面的中国国家安全机构附近。攻击者似乎是通过向其中一名僧侣发送一封看似来自同事的电子邮件而进入的;当他点击附加的 PDF 时,出现了 JavaScript 缓冲区溢出,利用 Adobe Reader 中的漏洞接管了他的机器。

这种技术称为网络钓鱼,因为它通过提供诱饵使某人咬住来起作用;当它针对特定的个人（如本例)时,称为鱼叉式网络钓鱼。然后他们破坏了藏人的邮件服务器,这样每当办公室里的一个人向另一个人发送 .pdf 文件时,它就会带有嵌入式攻击。邮件服务器本身在加利福尼亚。

当你停下来想一想时,这是非常发人深省的。您从十英尺外的一位同事那里收到一封电子邮件,您问他是否刚刚发送了邮件 当他说是时,您点击了附件。你的机器突然被你在一万英里外的一个友好国家租用的服务器感染了。我们在关于“Snooping Dragon”[1374] 的技术报告中写下了这一点。它出来后,我们不得不处理一段时间对我们设备的攻击,以及中国人在会议上的质问,他们声称我们没有证据表明这些攻击是他们政府造成的。多伦多 Open Net Initiative 的同事紧随其后,最终通过对黑客工具仪表板的分析发现,同一个间谍网络已将 103 个国家/地区的 1,295 台计算机作为目标 [1223]

– 从印度驻华盛顿大使馆到纽约的美联社,再到泰国、伊朗和老挝的外交部。

随后出现了一系列关于中国政府黑客攻击的进一步报道,从 2009 年与力拓就铁矿石价格发生的复杂纠纷,到同年墨尔本国际电影节放映一部关于维吾尔族领导人的电影时遭到黑客攻击 [1898]。 2011 年,在伊朗人追踪到中央情报局的秘密通信系统后,中国人入侵了该系统,并处决了大约 30 名特工 尽管直到后来才为公众所知 [578]。

第一个闪光灯时刻是 2013 年泄露的五角大楼报告,称中国黑客窃取了 F35 联合攻击战斗机以及一系列其他武器系统的部分机密 [1379]。与此同时,中国和香港占美国港口查获的所有假冒商品的 80% 以上。奥巴马政府誓言要将窃取商业机密的调查和起诉作为重中之重,并于次年对五名中国人民解放军成员进行了缺席起诉。

在 2015 年 6 月有消息称中国人入侵了人事管理办公室 (OPM) 后,白宫不得不再次采取行动,获得了 2200 万现任和前任联邦雇员的高度个人数据,从指纹到敏感信息来自安全许可访谈。申请最高机密许可的员工被命令泄露所有可能被用来敲诈他们的信息,从青少年吸毒到公开的同性恋关系。过去五年内的所有性伴侣都必须申报,以获得正常的绝密许可;为了获得 Strap 许可(处理信号情报材料),候选人甚至必须报告他们经常在教堂遇到的任何外国人。所以这次泄密影响了超过 2200 万人。从表面上看,这种侵入式数据收集是为了降低情报机构工作人员被勒索的风险。 (愤世嫉俗者认为这也是为了让举报人名誉扫地。)无论出于何种动机,将所有此类信息放在一个地方都非常愚蠢;这是一个真正的“废墟数据库”。

对于中国人来说,获得所有担任敏感政府工作的美国人的所有妥协信息令人瞠目结舌。 (英国也搞砸了;2008 年,一名海军军官丢失了一台笔记本电脑,其中包含 600,000 名加入皇家海军或试图加入 [1072] 的人的个人数据。)在当年 9 月的一次峰会上,奥巴马总统和习近平总统同意避免为商业利益而利用计算机窃取知识产权8。尽管关于军事机密或联邦特工的性生活,但在公开场合什么也没有说。

2000 年代的中国攻击使用了聪明的人和简单的工具;对西藏人的攻击使用俄罗斯犯罪软件作为远程访问木马。
国家还拉拢了一群“爱国黑客”,或者可能利用他们来推诿;一些分析人士注意到与中国大学学期相关的针对西方公司的天真攻击浪潮,并想知道学生是否被要求将黑客攻击作为课程作业。英国警方和安全部门在 2007 年向英国公司发出警告。到 2009 年,据报道中国对美国电力公司进行了多项调查,到 2010 年,中国的鱼叉式网络钓鱼攻击已经成为

8中国人信守诺言;据在中国开展业务的美国公司称,知识产权现在在关注事项列表中排名第六,低于 2014 年的第二 [704]。无论如何,“知识产权盗窃”一词一直是一种简化,用于将机密信息防御承包商的盗窃与其他希望进入中国市场的公司强制技术转让以及假冒附带问题这一更大的问题混为一谈。

报告了美国、波兰和比利时的政府目标 [1304]。与西藏人的袭击一样,这些袭击通常使用简陋的工具,而且操作安全性极差,以至于很清楚他们来自哪里。

到 2020 年,攻击变得更加复杂,威胁情报公司跟踪了一系列高级持续威胁 (APT)。一场针对维吾尔人手机的黑客攻击活动涉及多次零日攻击,甚至是针对 iPhone 的攻击,这些攻击是通过受感染的维吾尔人网站 [393] 进行的;这不仅针对中国的维吾尔人,也针对散居海外的维吾尔人。中国还从事工业和商业间谍活动,西方机构声称他们利用托管服务提供商 9。另一种方法是攻击软件供应链。一个名为 Wicked Panda 或 Barium 的中国组织破坏了计算机制造商华硕的软件更新、一个 PC 清理工具和一个韩国远程管理工具,以及三个流行的计算机游戏,在数百万台机器上安装了它的恶意软件;它没有启动银行木马或勒索软件,而是用于间谍活动 [810]。就像在 GCHQ 的社会主义行动中一样,这种间接策略提供了一种在你不是主权国家的领土上扩大攻击规模的方法。而中国也在玩社会主义游戏:2019 年传出,有人在过去 7 年里入侵了至少 10 家西方手机公司,并泄露了通话数据记录 肇事者似乎是 APT10 团伙,与中国军方[2017]。

自 2018 年以来,关于中国公司是否应被允许在北约国家销售路由器和 5G 网络硬件的政治争论一直存在,特朗普政府于 2019 年 5 月将华为列入黑名单。此前曾有过关于另一家中国公司中兴通讯的口角; 2018 年,GCHQ 警告说,中兴设备“将给英国国家安全带来无法有效或切实缓解的风险”[1475]10。特朗普总统以中兴通讯违反对朝鲜和伊朗的制裁为由对其下禁令,但态度有所缓和并允许其设备在安全控制下返回美国 11。

华为曾尝试过安全控制路线,该公司于 2010 年在牛津郡设立了一个中心,作为该公司获准在英国销售的条件,GCHQ 可以在那里研究其软件。虽然分析师没有发现任何后门,但他们 2019 年的报告对华为的软件工程实践提出了一些严厉的批评 [931]。华为复制了很多代码,无法修补他们不理解的地方,尽管承诺了多年,但在解决许多问题方面没有取得任何进展。 OpenSSL 的版本数量多得难以管理,包括已知漏洞和不受支持的版本:4 个不同 OpenSSL 版本的 70 个完整副本,以及 14 个版本的 304 个部分副本。中国人不仅可以破解华为系统;任何人都可以。他们的设备被排除在外

9这在 2019 年公开,声称他们已经入侵了 Wipro 并用它来危害他们的客户 [1093];但后来发现,Wipro 遭到了一个以营利为目的的犯罪团伙的攻击。

10 唯一真正被发现在其代码中带有恶意后门的路由器供应商是美国公司 Juniper,该公司不仅使用 NSA 的 Dual-EC 后门使 VPN trac 可被利用,而且以一种其他人可以利用的笨拙方式进行它也是 而且至少有另一方这样做了 [413]。

11前国家安全顾问约翰·博尔顿表示,这是对习主席的帮助,他宣称自己对习主席干涉刑事诉讼感到“震惊”[156]。

几年来自英国骨干路由器和用于窃听的系统。
英国要求“在多个版本和多个产品范围内持续改进的证据”，然后才会更加信任它。随后，包括澳大利亚和新西兰在内的许多国家彻底禁止使用华为设备，2019 年加拿大逮捕了华为的首席财务官（她也是其创始人的女儿），此前美国要求引渡她密谋就华为与华为的关系诈骗全球银行一家在伊朗经营的公司。作为报复，中国以虚假的间谍罪名逮捕了两名加拿大人，其中一名是休假的外交官，并以毒品罪名判处另外两人死刑。美国反击禁止美国供应商向华为出售芯片、软件或支持。英国从 2020 年底开始禁止购买他们的电信设备，并表示将在 2027 年之前将其从英国网络中移除。同时，中国正在帮助许多欠发达国家实现网络现代化，这种访问可能有助于他们与五眼联盟竞争 范围在适当的时候。贸易政策、产业政策和网络防御战略在新冷战中交织在一起。

从战略上讲，问题可能不仅仅是中国是否可以使用华为路由器大规模窃听其他国家，而是他们是否可以在紧张时期使用华为路由器发起 DDoS 攻击，通过破坏 BGP 路由来破坏互联网。我在第 21.2.1 节中更详细地讨论了这一点。多年来，中国的“和平崛起”学说意味着在其他大国足够强大之前避免与它们发生冲突。总体态势是一种主要是防御性的信息战，结合了家庭的无处不在的监视、比其他任何人都更好地防御网络攻击的围墙花园家庭互联网，以及相当大且不断增长的能力，主要用于勤奋的情报-聚集支持国家战略利益。他们开始以各种方式欺负其他国家，有时还涉及在线操作。 2016 年，在与越南就南海部分岛屿发生争端期间，他们入侵了河内和胡志明市的机场系统，显示侮辱性信息并强制乘客手动办理登机手续[1195]。 2020 年，欧盟谴责中国传播有关冠状病毒大流行的破坏性假新闻 [1577]，澳大利亚谴责自其呼吁对大流行的起源进行国际调查以来发生的网络攻击 [935]。这些信息行动展示了一流的公开和隐蔽的虚假信息能力，并遵循了之前在香港和台湾开展的更为有限的活动 [564]。外交评论员指出，中国的贸易政策虽然咄咄逼人，但与 1970 年代的日本无异，也不如美国那样咄咄逼人；新冷战与上一次冷战一样误入歧途，同样可能造成浪费和危险；中国仍然维护国际秩序而不是扰乱它；并且它比美国自二战以来所做的更一贯地支持它 [704]。中国对外宣传的目的是向世界展示自己是一个积极的社会经济榜样，因为它正在争夺准入和影响力，并成为美国和欧洲的竞争对手。

2.2.3 俄罗斯

俄罗斯和中国一样,缺乏美国的平台优势,并通过使用鱼叉式网络钓鱼和恶意软件的黑客团队来弥补。与中国不同的是,它走低调路线,经常充当搅局者,试图扰乱国际秩序,有时还通过其主要出口产品石油价格上涨直接获利。

历史学家蒂莫西·斯奈德 (Timothy Snyder) 描述了普京的上台以及他对寡头、正统基督教、恐同症和法西斯理论家伊万·伊林的拥护,尤其是自 2012 年被操纵的选举以来。这使得俄罗斯国家需要与威胁纯洁性的外部敌人进行永久性斗争俄罗斯人民[1798]。它在网络上的战略姿态在四个方面与中国不同。首先,它是网络犯罪的主要中心;地下市场于 2003-5 年首次出现在俄罗斯和乌克兰,我们将在下一节讨论网络犯罪。其次,虽然俄罗斯正试图变得像中国一样更加封闭,但其国内互联网相对开放并与西方的互联网交织在一起,包括 VK 和 Yandex [605] 等主要服务公司。第三,俄罗斯将自己重新确立为地区大国的战略比中国更加激进,直接对格鲁吉亚和乌克兰等邻国进行军事干预。这些干预措施涉及网络攻击和“小绿人”(制服上没有俄罗斯徽章的军队)的混合策略,以及否认的政治策略。第四,1989年苏联解体时,俄罗斯曾被美欧羞辱,至今仍感到被包围。自 2005 年左右以来,其目标一直是削弱美国和欧盟,并提倡威权主义和民族主义,以替代基于规则的国际秩序。自 2013 年以来,这方面的努力得到了加强;斯奈德讲述历史 [1798]。随着英国脱欧,随着匈牙利、土耳其和波兰威权政府的出现,以及意大利、斯洛伐克和奥地利联合政府中威权主义者的出现,这一战略似乎正在取得胜利。

2007 年,爱沙尼亚将塔林一座备受憎恨的苏联时代雕像移到了一个不太显眼的地方,俄罗斯人因此感到受到了侮辱,俄罗斯的网络攻击在 2007 年变得引人注目。针对政府机构、银行和媒体公司的 DDoS 攻击迫使爱沙尼亚在数周内对其外部互联网访问进行速率限制 [692]。俄罗斯拒绝引渡肇事者,其中大多数是俄罗斯人,但一名俄裔爱沙尼亚少年被罚款。怀疑论者表示,这些攻击似乎是业余爱好者所为,而且之所以奏效,是因为爱沙尼亚人没有像美国服务提供商那样强化他们的系统。尽管如此,爱沙尼亚还是向北约求助,结果之一就是塔林手册,其中规定了网络冲突法 [1664]。我将在电子和信息战一章的 23.8 节中更详细地讨论这个问题。次年,在俄罗斯和格鲁吉亚之间爆发短暂战争后,俄罗斯黑客建立了一个网站,其中列出了格鲁吉亚的目标,供俄罗斯爱国者攻击 [1990]。

爱沙尼亚和格鲁吉亚只不过是乌克兰的热身赛。在基辅 Maidan 广场举行反对亲俄总统亚努科维奇的示威活动,以及 2014 年 2 月俄罗斯雇佣军射杀约一百名示威者的干预后,亚努科维奇逃离。俄罗斯人于2月24日入侵乌克兰,吞并了克里米亚,并在乌克兰东部的顿巴斯地区建立了两个傀儡国。他们的战术结合了俄罗斯 spe

穿着便服的官方力量,一大堆宣传声称说俄语的乌克兰人发动叛乱,或俄罗斯帮助保卫人民免受乌克兰法西斯分子的侵害,或捍卫俄罗斯的纯洁性以对抗同性恋者和犹太人;所有这一切都与各种网络攻击相协调。例如,在 5 月,俄罗斯人入侵了乌克兰选举委员会的网站,并操纵它显示一条消息,即获得不到 1% 选票的民族主义者获胜;这被发现并被阻止,但俄罗斯媒体无论如何都宣布了虚假结果 [1798]。

第二年,随着冲突的持续,俄罗斯在半小时内关闭了三个不同配电系统上的 30 个变电站,导致 230,000 人数小时断电。它们涉及数月内植入的多个不同的攻击向量,而且由于它们是在乌克兰对克里米亚的配电设施发动攻击之后 并在本可以摧毁它的情况下将设备切换到其他地方 似乎是为了作为警告 [2067]。与冲突的其他影响相比,这次袭击仍然微不足道,其中包括击落马来西亚航空公司的客机,机上人员全部遇难;但这是第一次破坏主电源的网络攻击。终于在 2017 年 6 月 27 日发生了 NotPetya 攻击 迄今为止最具破坏性的网络攻击 [813]。

NotPetya 蠕虫最初是使用 MeDoc 的更新服务分发的,MeDoc 是乌克兰大多数企业使用的会计软件。然后,它使用 EternalBlue 漏洞在 Windows 文件共享的组织中横向传播,这是一个具有有趣历史的 NSA 漏洞。从 2016 年 3 月开始,一个中国团伙开始使用它来攻击越南、香港和菲律宾的目标,这可能是找到它并对其进行逆向工程的结果(据说你不会发射网络武器;你会分享它)。它在 2017 年 4 月被一个名为“影子经纪人”的团伙泄露,连同中国人没有部署的其他 NSA 软件,然后在 6 月被俄罗斯人使用。

NotPetya 蠕虫将 EternalBlue 与从 Windows 内存中恢复密码的 Mimikatz 工具结合使用。蠕虫的有效载荷伪装成勒索软件;它对受感染计算机的硬盘进行加密,并要求支付 300 美元的比特币作为赎金。但是没有机制来解密支付赎金的计算机所有者的文件,因此它确实是一种破坏性的服务拒绝蠕虫。唯一的解决方法是重新安装操作系统并从备份中恢复文件。

NotPetya 攻击导致银行、电信公司甚至前切尔诺贝利核电站的辐射监测系统瘫痪。更重要的是,它从乌克兰传播到在那里拥有办事处的国际公司。全球最大的集装箱航运公司马士基不得不更换大部分计算机,并为延迟装运的客户提供补偿,成本达 3 亿美元; FedEx 也损失了 3 亿美元,而 Mondelez 损失了 1 亿美元。 Mondelez 的保险公司以这是“战争行为”为由拒绝赔付,因为乌克兰、美国和英国政府都将 NotPetya 归因于俄罗斯军事情报机构 GRU [1232]。 2016年以英国英国脱欧公投和美国总统在美国的选举为标志,在这两者中都有大量的俄罗斯干预。在前者中,主要的干预措施是为休假活动提供财政支持,后来发现这些活动也因花费过多而违法

很多 [1265];这得到了社交媒体上密集活动的支持[363]。在后者中,奥巴马总统在竞选期间谴责俄罗斯的干涉,导致重新实施经济制裁,随后美国情报界也谴责了俄罗斯的干涉。前联邦调查局局长罗伯特·穆勒 (Robert Mueller) 的一项调查发现,俄罗斯通过其互联网研究机构“巨魔农场”以及 GRU 开展的虚假信息和社交媒体活动进行了非常广泛的干预,该活动黑掉了民主党全国委员会和竞选委员会的电子邮件,大多数尤其是克林顿竞选主席约翰·波德斯塔 (John Podesta) 的那些人。特朗普的一些助手因各种罪名入狱。

正如我将在第 26.4.2 节中讨论的那样,很难评估此类干预措施的效果。一方面,一份提交给美国参议院外交关系委员会的报告阐述了自普京上台以来俄罗斯一贯的政策,以破坏民主国家和基于规则的国际秩序的影响,促进威权政府左派和右派,尽可能地制造麻烦。它指出,欧洲国家采取广泛的防御措施,包括就选举行为和提高选民媒体素养达成两党协议;它建议美国也采用这些方法 [385]。 On the other hand, Yochai Benkler cautions Democrats against believing that Trump s election was all Russia s fault;民众对政治精英不满的根源要久远得多 [227]。俄罗斯与西方的信息战早于普京;它延续了旧苏联通过各种民族解放运动和恐怖组织煽动冲突来削弱西方的战略（我在第 23.8.3 节中讨论了信息战方面的问题）。蒂莫西·斯奈德 (Timothy Snyder) 将这一切置于现代俄罗斯历史和政治的背景下 [1798];他的分析还概述了针对民主的破坏性信息战的剧本。这不仅仅是关于黑进变电站,而是关于黑进选民的思想;关于破坏对机构甚至事实的信任,利用社交媒体并将政治重塑为演艺事业。普京是一名柔道运动员;柔道是利用对手的力量和势头来绊倒他们。

2.2.4 其余

世界其他国家的政府拥有相当广泛的网络能力,但有共同的主题,包括其工具的性质和来源。阿拉伯之春起义严重动摇了中东政府,有些政府甚至关闭了一段时间的互联网,例如 2010 年 4 月至 7 月的利比亚,当时叛军使用谷歌地图为美国、英国和法国战机生成目标文件.从那时起,阿拉伯国家制定了结合间谍软件和黑客攻击高调目标的策略,通过巨魔农场在公共论坛上发表辱骂性评论,并进行人身胁迫。

2019 年,举报人 Lori Stroud [247] 描述了阿拉伯联合酋长国的行动。作为一名美国国家安全局分析师 埃德·斯诺登的前任老板 她于 2014 年被马里兰州的一家承包商猎头,以雇佣军的身份在迪拜工作,但在阿联酋的行动开始以美国人为目标后离开了。

阿联酋的主要技术是使用 Windows 恶意软件进行鱼叉式网络钓鱼,但他们最有效的工具 Karma 使他们能够破解外国政治家和当地持不同政见者的 iPhone。他们还针对批评的外国人

政权。在一个案例中,他们对一名英国研究生进行社会工程,让他在他的 PC 上安装间谍软件,借口是这会使他的通信难以追踪。情报小组由几十人组成,既有雇佣军也有阿联酋人,他们在迪拜的一座大别墅里。独立观察员记录了阿联酋政府对 iPhone 恶意软件的使用 [1219]。

2018 年,沙特阿拉伯政府在其驻伊斯坦布尔领事馆内杀害了《华盛顿邮报》记者 Jamal Khashoggi。邮报发起运动,揭露沙特王储穆罕默德·本·萨勒曼是下令的人,2019 年 1 月,国家询问者发表了一份特刊,其中包含的文字显示邮报的所有者杰 ·贝佐斯有风流韵事。

贝索斯抢先宣布他和妻子正在离婚,并聘请了一名调查员来寻找泄密的源头,从而抢在《国家问询报》之前。 《国家询问者报》曾试图用它也获得的一些照片勒索贝佐斯;它希望他和调查人员都声明该报没有依赖“任何形式的电子窃听或黑客在他们的新闻收集过程中”。贝索斯改为公开上市。据调查人员称,他的 iPhone 已被沙特阿拉伯政府入侵 [199];造成损害的恶意 What sApp 消息是从王储本人的手机 [1053] 发送的。美国司法部后来指控两名前 Twitter 员工从事间谍活动,向沙特披露批评其政府的人的个人账户信息 [1500]。

一个更令人不快的例子是叙利亚,在那里,暴行的工业化是扩大信息收集规模的第三种方法。从 2012 年开始就有针对持不同政见者的恶意软件攻击的报道,最初使用了各种鱼叉式网络钓鱼诱饵。随着内战的进行,逮捕嫌疑人的警察会当场强奸女性家庭成员,除非嫌疑人透露他的邮件和社交媒体密码。然后,当他被带上面包车前往酷刑室时,他们会用鱼叉式网络钓鱼他所有的联系人。

这种基于受害者的攻击扩展方法不仅在叙利亚而且在美国和欧洲导致许多机器受到损害。随着战争的发展,这些活动变得越来越复杂,带有虚假标记攻击,但仍保留了一些显示斩首视频的工具的残酷优势 [737]。

感谢 John Scott-Railton 及其在多伦多的同事,我们有许多进一步记录的在线监视、计算机恶意软件和电话攻击被用来针对持不同政见者的例子;许多在中东和非洲国家,但也在墨西哥,实际上在匈牙利 [1219]。这里真正的问题是公司的生态系统,这些公司主要在美国、欧洲和以色列,它们向令人讨厌的国家提供黑客工具。这些工具的范围从电话恶意软件,到您在自己的网络上针对持不同政见者使用的大规模监视工具,再到使您能够通过滥用信号系统跟踪和窃听海外电话的工具 [488]。这些工具被独裁者用来追踪和监视他们在美国和欧洲的敌人。

非政府组织已尝试阻止这种网络武器贸易。在一个案例中,非政府组织争辩说,叙利亚政府从一家英国公司的德国子公司购买大规模监控设备的能力应该受到出口管制,但英国当局不愿阻止。 GCHQ 确定,如果要在阿萨德总统的网络上安装大量监控设备,它们应该是英国设备,而不是

乌克兰人。 （我将在后面的 26.2.9 节中对此进行更详细的描述。）因此，围绕常规武器销售的道德问题在网络时代仍然存在；事实上，它们可能会更糟，因为这些工具被用来对付美国人、英国人和其他人，他们坐在家里，但不幸的是，他们被列入了一个令人不快的政府不喜欢的人的联系人名单。在过去，向远方的独裁者出售武器不会让你自己的居民受到伤害；但网络武器可以产生全球影响 。

多年来因制裁而孤立无援的伊朗利用当地黑客论坛开发了一种本土网络能力。与叙利亚一样，它的主要重点是情报行动，特别是针对国内外持不同政见的伊朗人。它也是美国和其他攻击的目标，其中最著名的是 Stuxnet，之后它追踪了中央情报局的秘密通信网络并围捕了许多特工 [578]。它在海外发起了间谍活动和攻击。前者的一个例子是它对荷兰 Diginotar CA 的黑客攻击，使其能够监控持不同政见者的 Gmail；而其 Shamoon 恶意软件损坏了沙特阿拉伯国家石油公司 Aramco 的数千台 PC。 Collin Anderson 和 Karim Sadjadpour [49] 讲述了伊朗网络能力的历史。

最近，它于 2020 年 4 月袭击了以色列的水处理厂；以色列在接下来的一个月对伊朗的阿巴斯港 [229] 发动了袭击。

最后，值得一提的是朝鲜。 2014 年，在索尼影业开始制作一部关于暗杀朝鲜领导人阴谋的喜剧之后，一个黑客组织破坏了索尼的大部分基础设施，发布了令人尴尬的电子邮件，导致其最高电影执行官艾米帕斯卡辞职，并泄露了一些未发行的电影.随后威胁说，如果这部喜剧全面上映，电影院将遭到恐怖袭击。该公司将这部电影限制上映，但当奥巴马总统批评他们屈服于朝鲜的讹诈时，他们改为全面上映。

2017 年，朝鲜再次受到关注，因为他们的 Wannacry 蠕虫病毒感染了全球超过 200,000 台计算机，加密数据并要求比特币赎金 尽管它与 NotPetya 一样没有选择性解密的方法，因此实际上只是一种破坏性的蠕虫病毒。它使用了 NSA 永恒之蓝漏洞，如 NotPetya，但在恶意软件研究人员发现终止开关时被阻止。与此同时，它扰乱了汽车制造商日产和雷诺以及台湾芯片代工厂台积电的生产，还导致英国国民健康服务体系的几家医院关闭了他们的急救室。 2018 年，美国司法部就这两起事件以及一系列电子银行抢劫案对一名朝鲜政府黑客提出了起诉，其中包括从孟加拉国银行 [1653] 盗取 8100 万美元。 2019 年，一份泄露的联合国报告进一步指责朝鲜特工从加密货币交易所盗窃了超过 10 亿美元 [346]。

2.2.5 归属

人们常说网络是不同的，因为很难归因。作为一般命题，这是不正确的；在线匿名比您想象的要难得多。

即使是聪明人也会在操作安全方面犯下错误,从而暴露他们,威胁情报公司已经收集了大量数据,使他们能够在许多情况下以合理的概率归因于甚至错误的标记操作 [180]。然而有时这可能是真的,人们仍然指向气候门事件。在 2009 年哥本哈根气候变化峰会召开前几周,有人发布了超过一千封电子邮件,其中大部分发送给或来自英国东安格利亚大学的四位气候科学家。气候怀疑论者抓住了其中一些,讨论了如何最好地呈现全球变暖的证据,作为全球阴谋的证据。官方调查后来证实,这些电子邮件是断章取义,但损害已经造成。

人们想知道肇事者是俄罗斯人还是沙特人,甚至是一家能源公司。然而,一项更有说服力的分析表明这是内部泄漏,甚至是事故;只有一个存档文件被泄露,它的文件名 (FOIA2009.zip) 表明它可能已经准备好在任何情况下进行信息自由披露。这里真正有趣的事情可能是这些电子邮件是如何被谈论成阴谋论的。

另一个可能的国家行动是 Equifax 黑客攻击。最初的故事是,2017 年 3 月 8 日,Apache 警告 Apache Struts 存在漏洞并发布了补丁;两天后,一群人开始寻找易受攻击的系统； 5 月 13 日,他们发现 Equifax 的争议门户没有打补丁,于是就进去了。后来的诉讼是,Equifax 使用门户的默认用户名和密码“admin”[358]。无论哪种方式,违规行为都是可以预防的;入侵者发现了一个明文密码文件,可以访问 51 个内部数据库系统,并花了 76 天的时间帮助自己获取至少 1.455 亿美国人的个人信息,直到 7 月 29 日报告入侵并在第二天阻止访问。高管们在 9 月 7 日通知公众之前就卖出了股票;国会被激怒了,首席执行官里克史密斯被解雇了。到目前为止,还很普通。但是,没有任何被盗信息被用于犯罪,这导致当时的分析人士怀疑肇事者是一个民族国家行为者,大规模寻求美国人的个人数据 [1444];在适当的时候,四名中国军人因此被起诉 [552]。

无论如何,情报界和犯罪界长期以来一直纠缠在一起,而且在网络时代,它们似乎越来越纠缠不清。接下来我们转向网络犯罪。

2.3 骗子

网络犯罪现在约占所有犯罪的一半,无论是数量还是价值,至少在发达国家是这样。它是略多于还是少于一半取决于定义（现在在线提交纳税申报表是否包括税务欺诈？）以及您提出的问题（您是否将骚扰和网络欺凌计算在内？） 但即使是狭义的定义,还差将近一半。然而,世界执法机构通常只将不到百分之一的预算用于打击它。直到最近,大多数司法管辖区的警察部队都尽力忽视它;在美国,它被视为“身份盗窃”并单独计算,而在英国,受害者被告知向银行而不是警察投诉

从 2005-15 年。结果是,随着网络犯罪,就像其他一切一样,网络部分没有被计算在内,犯罪似乎在下降。不过,最终,真相在那些开始在定期受害调查中询问欺诈问题的国家浮出水面12。

我和我的同事经营着剑桥网络犯罪中心,我们在那里收集和整理数据供其他研究人员使用,范围从垃圾邮件和网络钓鱼到恶意软件和僵尸网络命令和控制跟踪,再到帖子集合到地下犯罪论坛。本节借鉴了我们在 2019 年进行的一项关于网络犯罪成本及其随时间变化的调查 [91]。

自 1960 年代以来,计算机欺诈就一直存在,一个值得注意的早期案例是 Equity Funding 保险公司,该公司从 1964 年到 72 年创建了 60,000 多份伪造保单,并将其出售给再保险公司,并创建了一个特殊的计算机系统来跟踪所有这些保单。自 1980 年代以来,针对支付系统的电子欺诈就一直存在,而当 1990 年代互联网向所有人开放时,垃圾邮件也随之而来。然而,早期的诈骗大多是家庭手工业,个人或小团体收集信用卡号,然后伪造卡在商店使用,或使用卡号购买邮购商品。现代网络犯罪可能可以追溯到 2003-5 年,当时地下市场的出现使犯罪分子能够专业化并擅长于他们的工作,就像工业革命在实体经济中发生的那样。

要理解网络犯罪,首先考虑共享基础设施,然后再考虑以营利为目的的主要网络犯罪类型。与我们在上一节中考虑的国家犯下的罪行以及我们将在下一节中考虑的个人针对其他个人犯下的罪行有很大的重叠;但演员的动机是一个有用的初级过滤器。

2.3.1 犯罪基础设施

大约从 2005 年开始,地下市场的出现导致人们专门成为犯罪基础设施的提供者,最著名的是僵尸网络放牧者、恶意软件编写者、垃圾邮件发送者和提现运营商。我将在 21.3 节中更详细地讨论该技术;在本节中,我的重点是参与者和他们在其中运作的生态系统。虽然这个生态系统可能由几千人组成,收入在几千万到几亿之间,但他们给行业和社会带来了数十亿美元的成本。

既然网络犯罪已经产业化,现在大多数“工作”都扮演着无聊的角色,例如客户支持和系统管理,包括所有涉及逃避执法行动的繁琐设置工作 [453]。

他们为专业工作的“公司”;企业家和技术专家可以赚到真钱。 （此外,在冠状病毒大流行期间,网络犯罪行业一直在蓬勃发展。）

12美国、英国、澳大利亚、比利时和法国

2.3.1.1 僵尸网络牧民

第一个僵尸网络 受感染的计算机网络 可能是在 1996 年对纽约的 ISP Panix 的攻击中出现的,它使用医院中受感染的 Unix 机器进行 SYN 洪水攻击 [368]。下一个用途是垃圾邮件,到 2000 年,Earthlink 垃圾邮件发送者发送了超过一百万封网络钓鱼电子邮件;它的作者被 Earthlink 起诉。一旦网络犯罪分子开始组织起来,规模就会显着扩大。我们开始看到专业构建和维护的僵尸网络可以被坏人出租,无论是垃圾邮件发送者、网络钓鱼者还是其他人;到 2007 年,Cutwail 僵尸网络每分钟从超过 100 万台受感染的机器发送超过 5000 万封垃圾邮件 [1832]。机器人最初会联系命令和控制服务器以获取指令;这些将被威胁情报公司关闭或接管,用作监视受感染机器的污水坑,并将它们的列表提供给 ISP 和企业。

垃圾邮件发送者的第一反应是点对点僵尸网络。 2007 年,Storm 突然增长到占所有 Windows 恶意软件的 8%;它主要通过电子邮件附件中的恶意软件感染机器,并让它们使用 eDonkey 对等网络来查找其他受感染的机器。它不仅用于垃圾邮件,还用于 DDoS、拉高出货股票诈骗和获取银行凭证。防御者让很多同行加入这个网络来收集机器人地址列表,这样机器人就可以被清理掉,到 2008 年底,Storm 的规模已经缩减到原来的十分之一。紧随其后的是 Kelihos,这是一个类似的僵尸网络,也窃取了比特币;它的创造者是一名俄罗斯国民,2017 年在西班牙度假时被捕,并被引渡到美国,他于 2018 年在那里认罪 [661]。

Conficker 僵尸网络带来了下一个犯罪创新:域生成算法 (DGA)。 Conficker是一种利用Windows网络服务漏洞传播的蠕虫;它每天生成 250 个域名,受感染的机器会尝试所有域名,希望 botmaster 设法租用其中一个。防御者一开始只是简单地购买域,但后来的变体每天生成 50,000 个域,一个行业工作组与注册商达成协议,这些域将被简单地停止使用。到 2009 年,Conficker 已经变得如此庞大,拥有大约一千万台机器,以至于人们认为它对最大的网站甚至可能对国家构成威胁。与 Storm 一样,它对随机化的使用被证明是一把双刃剑;防御者可以坐在域的一个子集上并收集受感染机器的提要。到 2015 年,受感染机器的数量已降至 100 万以下。

无论是否可以通过逮捕 botmaster 或技术手段来摧毁命令和控制系统,僵尸网络感染的普遍解决方法是清理受感染的机器。但这引发了许多规模和激励问题。虽然 AV 公司提供工具,Microsoft 提供补丁,但许多人并不使用它们。只要您受感染的 PC 只是偶尔发送垃圾邮件,但在其他方面运行良好,您为什么要费心去做任何事情呢?但是带宽会让 ISP 花钱,所以下一步是一些 ISP,特别是像康卡斯特这样的有线电视公司,会识别受感染的机器并将他们的用户限制在“围墙花园”内,直到他们承诺清理。到 2019 年

变得不那么普遍了,因为人们现在在他们的 wifi 上有各种各样的设备,其中许多没有用户界面;与人类用户的交流变得更加困难。

2020 年,我们发现许多拥有数万台机器的僵尸网络对于大多数防御者来说太小而无法关心,加上一些往往是多层的大型僵尸网络 通常在底部具有点对点机制,使footsoldier 机器人与一些控制节点进行通信,这些控制节点又使用域生成算法来找到 botmaster。将步兵分割成许多小型僵尸网络使得防御者很难渗透到所有这些僵尸网络中,而控制节点可能位于防御者难以到达的地方。 2020 年此类僵尸网络的大笔资金似乎来自点击欺诈。

自 2016 年 10 月以来的最新创新是 Mirai,这是一个利用物联网设备的僵尸网络家族。第一个 Mirai 蠕虫病毒感染了小米制造的闭路电视摄像机,该摄像机具有已知的无法更改的出厂默认密码。 Mirai 僵尸网络会扫描 Internet 的 IPv4 地址空间,寻找其他易受攻击的设备,这些设备通常在启动后几分钟内就会被感染。第一次攻击是针对 DynDNS 的,在美国东部沿海地区导致 Twitter 瘫痪了六个小时。从那时起,已经出现了 1000 多种变体,研究人员研究这些变体以确定发生了什么变化,并找出可能使用的对策。

在任何时候,都可能有六个大型僵尸网络牧民。例如,Mirai 运营商似乎是两个或三个可能涉及几十人的小组。

2.3.1.2 恶意软件开发者

除了为世界情报机构及其承包商编写恶意软件的数百名软件工程师之外,可能还有数百人为犯罪市场编写恶意软件;没有人真正知道（尽管我们可以在黑客论坛上监控 trac 来猜测数量级）。

在这个社区中有专家。有些人专注于将漏洞转化为漏洞利用,这对于使用堆栈金丝雀、ASLR 和其他技术的现代操作系统来说是一项不平凡的任务,我们将在第 6.4.1 节稍后讨论。

其他人专门研究利用漏洞安装的远程访问木马;其他人构建用于弹性命令和控制通信的点对点和 DGA 软件;还有一些人为银行欺诈设计专门的有效载荷。最高价值的操作似乎是不断升级以应对反病毒公司最新对策的平台。

在每个专业细分市场中,通常都有几家运营商,因此当我们逮捕其中一家时,会在一段时间内产生影响。一些供应商位于不引渡其国民的司法管辖区,例如俄罗斯,俄罗斯犯罪软件不仅被俄罗斯国家行为者使用,也被其他国家使用。

随着 Android 取代 Windows 成为最常用的操作系统,我们发现 Android 恶意软件数量有所增加。在中国和拥有大量二手和旧手机的国家/地区,这可能是使用

未修复的 Android 手机 root 漏洞;美国和欧洲有很多未打补丁的手机（因为一旦手机停售,许多原始设备制造商就会停止提供补丁）,但通常只是应用程序在做坏事,例如窃取用于验证银行交易的短信。

2.3.1.3 垃圾邮件发送者

1990 年代中期互联网向公众开放时,垃圾邮件小规模出现,到 2000 年,我们看到 Earthlink 垃圾邮件发送者通过发送网络钓鱼诱饵赚取了数百万美元。到 2010 年,垃圾邮件每年花费全球 ISP 和科技公司约 10 亿美元的反制措施,但它为其运营商带来的收入可能只有其中的 1%。主要受益者可能是 Yahoo、Hotmail 和 Gmail 等网络邮件服务,由于规模大,它们可以运行更好的垃圾邮件过滤器;在 2010 年代,数亿人转而使用他们的服务。

垃圾邮件现在是一项高度专业化的业务,因为要通过现代垃圾邮件过滤器需要一整套不断变化的技巧。如果您想使用垃圾邮件来安装勒索软件,您最好为现有服务付费,而不是尝试从头开始学习。一些垃圾邮件涉及工业规模的电子邮件妥协,这对受害者来说代价高昂;在大规模妥协后,雅虎以 48 亿美元的价格被出售给 Verizon,损失了约 3.5 亿美元 [771]。

2.3.1.4 批量账户泄露

一些僵尸网络不断尝试通过猜测密码和密码恢复问题来侵入电子邮件和其他在线帐户。大型电子邮件服务提供商可能每天要恢复数万个帐户。有高峰,通常是当黑客在一个网站上泄露数百万个电子邮件地址和密码,然后在所有其他网站上进行尝试。

在 2019 年,这种凭据攻击仍然占尝试帐户泄露数量最多 [1882]。受损帐户被出售给以各种方式利用它们的人。主要电子邮件帐户通常具有其他帐户的恢复信息,如果攻击者幸运的话,包括银行帐户。它们也可用于诈骗,例如滞留旅客,受害人通过电子邮件向所有朋友发送电子邮件,称他们在国外某个城市遭到抢劫,并寻求紧急经济帮助以支付酒店账单。如果所有其他方法均失败,则受感染的电子邮件帐户可用于发送垃圾邮件。

该主题的一个变体是按安装付费服务,它在手机或 PC 上植入恶意软件以进行大规模订购。这可能涉及各种环境中的一系列网络钓鱼诱饵,从要求您安装特殊查看器的免费色情网站到体育用品供应和有关热门事件的新闻。它还可以使用更多技术手段,例如路过式下载。此类服务通常由僵尸网络提供,需要它们维护自己的号码;在美国和欧洲,他们可能会向第三方客户收取每千台受感染机器 10-15 美元的费用,而在亚洲可能会收取 3 美元。

2.3.1.5 目标攻击者

我们已经看到了黑客雇佣操作员的出现,他们会尝试破坏特定的目标帐户并收取费用,通常为 750 美元 [1882]。他们会调查目标,进行多次鱼叉式网络钓鱼尝试,尝试密码恢复程序,看看他们是否可以通过相关账户闯入。这延续了私家侦探的传统,他们传统上帮助离婚案件,也代表红顶报纸跟踪名人 尽管现在可以在线匿名购买服务,道德约束更少。 John Scott-Railton 及其同事揭露了 Dark Basin 的运作,这是一家针对埃克森美孚的批评者和网络中立倡导者的黑客雇佣公司,并将其追溯到印度的一家公司 [1692]。

近年来,针对小企业主和大公司财务人员的目标攻击也被大规模使用,以实施各种支付欺诈,我将在下面 2.3.2 中讨论。

2.3.1.6 套现团伙

回到二十世纪,盗取信用卡号码的人必须不厌其烦地购买商品,然后将其出售才能套现。如今,有些专家在地下市场购买受损的银行凭证并加以利用。价格揭示了犯罪链中的真正价值所在;信用卡号和到期日的组合售价不到 1 美元,要获得一美元,您需要 CVV、持卡人的姓名和地址等。

套现技术每隔几年就会发生变化,因为通过世界洗钱控制发现了路径,并且调整了法规以阻止它们。一些套现公司组织了一群骡子,他们将部分风险转移给他们。回到 2000 年代中期,骡子可能是吸毒者,他们会用偷来的信用卡去商店购买商品;然后有一段时间,不知情的骡子被广告招募,这些广告向“代理人”承诺高额收入以代表外国公司,但他们被用来通过他们的个人银行账户汇出被盗资金。洗衣工接下来使用拉脱维亚的俄罗斯银行,俄罗斯骡子会出现在这些银行提取现金。然后,总部位于哥斯达黎加的一种未经许可的数字货币 Liberty Reserve 风靡一时,直到它被关闭并且其创始人于 2013 年被捕。比特币接管了一段时间,但随着其价格变得越来越高,它在网络犯罪社区中的受欢迎程度有所下降波动性很大,因为美国财政部开始对比特币交易进行干预,以识别他们的客户。

与垃圾邮件一样,套现是一种不断发展的攻防游戏。我们使用 CrimeBB 对其进行监控并分析趋势,CrimeBB 是一个数据库,我们在地下黑客论坛中收集了数千万个帖子,网络犯罪分子在这些论坛上买卖服务,包括提现 [1499]。它似乎也有利于可以扩大规模的团伙,直到他们变得足够大以引起执法部门的认真关注:2020 年,谢尔盖·梅德韦杰夫 (Sergey Medvedev) 承认在 2010-15 年期间造成超过 5.68 亿美元的实际损失 [1928] .

2.3.1.7 勒索软件

加密货币下降的一个原因可能是勒索软件的增长,并且随着参与其中的团伙转向受害者更容易使用的支付方式。到 2016-17 年,美国受害者遇到的勒索软件中有 42% 要求提供亚马逊礼品卡等预付代金券； 14% 的人要求电汇,只有 12% 的人要求加密货币;许多针对消费者的低端勒索软件现在实际上是恐吓软件,因为它实际上根本不加密文件 [1742]。自 2017 年以来,我们看到了勒索软件即服务平台;使用这些平台的运营商往往是业余爱好者,即使你愿意付钱也无法解密。

与此同时,一些更专业的团伙渗透系统,安装勒索软件,等待几天或几周的备份数据被加密,并索取大量比特币。这种情况在 2019-20 年间增长迅速,美国最引人注目的勒索软件受害者是公共部门机构;数百个地方政府机构和少数医院都遭遇了服务失败 [358]。在大流行期间,更多的医院成为目标;加州大学旧金山分校的医学院支付了超过 100 万美元 [1480]。不过,这是一种国际现象,许多私营企业也成为受害者。

勒索软件运营商还一直威胁要大规模泄露个人数据,以胁迫受害者付款。

2.3.2 对银行和支付系统的攻击

对卡支付系统的攻击始于丢失和被盗的卡,大规模伪造出现在 1980 年代;在 1990 年代,互联网繁荣进一步加剧了这种情况,因为许多企业开始在线销售,但对如何检测欺诈一无所知;正是信用卡欺诈在 2000 年代中期催生了地下市场,因为犯罪分子想方设法买卖被盗的卡号以及相关设备和服务。

另一个重要组成部分是发行前欺诈,在美国称为“身份盗窃”[670],犯罪分子以您的名义获取信用卡、贷款和其他资产,然后让您来收拾烂摊子。我在括号中写下“身份盗用”,因为它实际上只是老式的冒充行为。回到二十世纪,如果有人去银行,冒充我,向他们借钱然后消失,那是银行的问题,而不是我的问题。在 21 世纪初,银行开始声称被盗的是您的身份而不是他们的钱 [1727]。现在这种责任倾销的情况有所减少,但联邦调查局仍将许多网络犯罪记录为“身份盗用”,这有助于将其排除在美国主流犯罪统计之外。

信用卡欺诈生态系统现在相当稳定。 2011 年和 2019 年的调查显示,虽然信用卡欺诈在十年间翻了一番,但损失占交易价值的百分比略有下降 [90、91];随着系统的发展,该系统变得越来越高效。许多卡号是在对零售商的黑客攻击中获取的,一旦他们支付通知受影响的客户并偿还银行重新发行的卡,这对他们来说可能是非常昂贵的。与犯罪基础设施一样,总成本可能比犯罪分子实际逃脱的成本高出两个数量级。

随着大规模网络钓鱼攻击的到来,2005 年对网上银行的攻击愈演愈烈;看似来自银行的电子邮件将客户驱使到窃取其密码的仿冒银行网站。银行以双因素身份验证等技术作为回应,或者一次只要求密码中几个字母的低成本替代品;大约从 2009 年开始,骗子的反应就是凭证窃取恶意软件。 Zeus 和后来的特洛伊木马潜伏在 PC 上,直到用户登录到他们认可其网站的银行;然后,他们向 mule 账户付款并向用户隐藏他们的活动 即所谓的“浏览器中间人攻击”。 (一些特洛伊木马甚至实时连接到人类操作员。)Zeus 和后来的 Dridex 银行恶意软件背后的骗子于 2019 年 12 月被美国调查人员点名起诉,并被指控窃取了大约 1 亿美元,但他们仍然逍遥法外俄罗斯 [795]。

其他团伙已被瓦解,人们因此类骗局而被捕,这些骗局每年在全球范围内继续净赚数亿至数十亿美元。

公司还必须注意商业电子邮件泄露,其中骗子破坏了商业电子邮件帐户并告诉客户他们的银行帐号已更改;或骗子冒充首席执行官并命令财务总监付款;以及伪装成您银行人员的社会工程攻击,他们说服您发布代码以授权付款。大多数针对公司支付系统的攻击在理论上都可以通过大多数大公司已有的控制程序来阻止,因此典型的目标是经营不善的大公司,或者有足够资金值得窃取的中型公司没有足够的控制来锁定一切。

我将在第 12 章讨论此类欺诈的技术细节,以及越来越多的仅直接影响银行、银行监管机构和零售客户的犯罪。我还将在第 20 章中讨论加密货币,它促进了从勒索软件到股票欺诈的网络犯罪。

2.3.3 部门网络犯罪生态系统

银行业以外的许多部门都有自己既定的网络犯罪现场。一个例子是旅行欺诈。有一个完整的生态系统,出售以欺诈方式获得的机票,有时只是用偷来的信用卡号购买,有时直接通过操纵或入侵旅行社或航空公司的系统获得,有时由这些公司的腐败员工预订,并且有时通过窃取他们的航空里程直接从公众那里被骗。由此产生的降价票直接使用垃圾邮件或通过各种联属营销骗局出售。使用它们飞行的一些乘客知道他们是可疑的,而另一些则是受骗的 这使得仅仅通过在登机口逮捕人来解决问题变得困难。 (骗子还在最后一刻提供门票,所以警报通常来不及了。)

有关旅行欺诈的说明和分析,请参见 Hutchings [936]。越来越多的其他业务部门也有自己的阴暗面,我将在后面的章节中谈到其中的一些。

2.3.4 内部攻击

自企业开始招聘员工以来,内部人员欺诈一直是个问题。员工欺骗公司,合伙人互相欺骗,公司欺骗股东。主要防御是簿记。复式簿记的发明,我们最早的记录来自一千年前的开罗,它使企业能够扩大规模,超越拥有它们的家族。整个生态系统随着技术的发展而发展,其设计由四大会计师事务所驱动,他们对审计客户提出要求,进而推动会计软件和配套安全机制的发展。我在第 12 章详细讨论了所有这些。还有涉及举报的内部攻击,我将在下面讨论。

2.3.5 CEO犯罪

公司互相攻击,他们的客户也是如此。从 1990 年代开始,打印机供应商使用密码术来锁定他们的客户使用专有墨盒,正如我在第 24.6 节中描述的那样,而销售笔芯的公司一直在破解密码。游戏机制造商一直在与售后市场供应商玩完全相同的游戏。密码学在配件控制中的使用现在很普遍,甚至在冰箱的滤水器滤芯上也能找到[1071]。许多客户觉得这很烦人,并试图规避控制。美国法院在 Lexmark v SCC 案中裁定这没问题:打印机供应商 Lexmark 起诉 SCC,这家公司将其安全芯片的克隆产品出售给独立的墨水供应商,但败诉了。因此,在位者现在可以聘请他们能找到的最好的密码学家来锁定他们的产品,而挑战者可以聘请他们能找到的最好的密码分析员来解锁他们的产品 客户可以以任何方式破解他们的产品。在这里,冲突是合法和公开的。与国家行为体一样,企业有时会组建拥有多个博士学位、数百万美元资金和电子显微镜等资本资产的团队 13。

我们稍后将在 24.6 节中对此进行更详细的讨论。

并非所有公司攻击都是公开进行的。也许最著名的秘密黑客攻击是大众汽车对欧盟和美国排放测试计划的攻击;如果检测到标准排放测试条件,汽车中销售的柴油发动机被编程为清洁运行,否则有效。为此,大众的首席执行官在美国被解雇并被起诉(德国不会将他引渡到美国),而奥迪的首席执行官在德国被解雇并入狱[1084]。大众已拨出 250 亿欧元用于支付刑事和民事罚款及赔偿金。其他汽车制造商也在作弊;戴姆勒于 2019 年在欧洲被罚款 8.6 亿美元 [1466],并于 2020 年在美国达成和解,其中包括来自四个政府机构的 15 亿美元罚款以及 7 亿美元的集体诉讼 [1856]。其他制造商和其他国家/地区的和解协议正在酝酿之中。

有时,产品旨在破坏整个保护系统等级,例如第 12 章稍后描述的覆盖 SIM 卡。这些 SIM 卡有两个面且厚度仅为 160 微米,您可以将其贴在手机的 SIM 卡顶部提供第二信任根;他们是

13 全面披露:我们的硬件实验室和我们的非政府组织活动有时会收到此类参与者的资助。

旨在使中国人能够克服 2010 年代初高昂的漫游费用。覆盖 SIM 实质上是对真实 SIM 进行中间人攻击,并且可以在 Javacard 中进行编程。一个副作用是这样的 SIM 使得进行某些类型的银行欺诈变得非常容易。

因此,在为您的系统构建威胁模型时,请停下来想想您的竞争对手中或与您所依赖的产品供应商竞争的公司中可能有哪些有能力的动机对手。显而易见的攻击包括工业间谍活动,但如今它比这复杂得多。

2.3.6 举报人

情报机构和秘密公司可能会沉迷于“内部威胁”。但在 2018 年,巴克莱银行的首席执行官因试图追踪银行的举报人而被罚款 642,000 英镑,并被勒令偿还 500,000 英镑的奖金 [698]。因此,让我们把它转过来,从另一个角度 举报人的角度 来看待它。许多人试图做正确的事,通常是在相当平凡的层面上,例如举报一位经理从供应商那里收受贿赂或性骚扰员工 。在银行业等受监管的行业中,他们可能有法律责任报告不当行为,并享有法律豁免权,免受雇主违反保密义务的指控。即便如此,他们也经常因为实力不平衡而输掉比赛;他们被解雇了,问题还在继续。许多安全工程师认为对泄密者的正确对策是技术性的,例如数据丢失防护系统,但员工报告不当行为的稳健机制通常更为重要。一些组织,如银行、警察部队和在线服务,有员工举报犯罪的机制,但没有有效的程序来提出对管理决策的道德问题 14。

但即使是基本的举报机制也常常是事后才想到的;他们通常会将投诉人带到人力资源部,而不是董事会的审计委员会。外部机制可能好一点。一家大型服务公司在 2019 年为其客户开通了“举报热线”;但是网页代码有来自 LinkedIn、Facebook 和谷歌的跟踪器,它们可以因此识别不满意的员工,还有来自 CDN 的 JavaScript,散落着来自更多 IT 公司的 cookie 和推荐人。精通技术的泄密者不会使用这样的服务。在生态系统的顶端,一些报纸为举报人提供了使用加密电子邮件进行联系的方式。但这些机制往往很笨拙,宣传它们的网页并不总是向潜在泄密者说明监视风险或可能对付它们的操作安全措施。我将在第 25 章中更详细地讨论有关举报的可用性和支持问题。

这主要是一个政策问题,而不是技术问题。很难设计一种技术机制,让诚实的员工能够揭发组织文化中根深蒂固的滥用行为,例如普遍存在的性骚扰或财务不当行为。在大多数情况下,谁是举报人一目了然,所以关键因素是举报人是否愿意

14Google 员工于 2018 年因处理性骚扰丑闻而罢工。

获得外部支持。例如,他们会找到另一份工作吗?这不仅是一个正式的法律保护问题,也是一个文化问题。例如,哈维·韦恩斯坦 (Harvey Weinstein) 被判强奸罪使许多妇女能够抗议性骚扰和歧视;希望 Black Lives Matter 抗议活动将同样赋予有色人种权力 [31]。

不过,匿名确实有帮助的一个例子是 2008-9 年的英国议会开支丑闻。在一场关于公众是否可以获得议会成员的费用报销的漫长法庭案件中,有人找到保存记录的个人电脑,将它们复制到 DVD 中,然后将其卖给了《每日电讯报》。该报在整个 5 月和 6 月期间分期发布了这些有趣的内容,当时议员们放弃了并在议会网站上发布了这些内容。六位部长辞职;七名国会议员和同僚入狱;在随后的选举中,数十名国会议员下台或失去席位;对于向纳税人收取的某些费用,既有欢笑也有愤怒。举报人在技术上可能犯了罪,但他们的行为显然是为了公共利益;现在所有的议会开支都是公开的,本来就应该如此。如果一个国家的立法者掌握了收银机,还有什么可以清理这个系统?

即使在埃德·斯诺登的案例中,他也应该有一个强有力的方式来向政府的适当部门(可能是国会委员会)报告 NSA 的非法行为。但他知道,之前的一名举报人比尔·宾尼 (Bill Binney) 在试图这样做后遭到逮捕和骚扰。事后看来,这种咄咄逼人的做法是不明智的,正如奥巴马总统的国家安全局审查小组最终承认的那样。在商业公司的较低级别,如果您的一名员工偷了您的钱,而另一名员工想告诉您这件事,您最好设法解决。

2.4 极客

我们的第三类攻击者是像我这样的人 研究漏洞并报告漏洞以便修复漏洞的研究人员。学术界出于好奇寻找新的攻击,并获得专业赞誉的回报 这可以导致教授晋升,帮助我们的学生找到工作。

为安全公司工作的研究人员也在寻找具有新闻价值的漏洞利用;在 Black Hat 等会议上进行宣传可以赢得新客户。 Hobby hack ers 将闯入 stu 视为一种挑战,就像人们爬山或下棋一样;黑客行动主义者这样做是为了惹恼他们认为是邪恶的公司。无论是否遵守法律,我们都倾向于成为好奇的内向者,他们需要掌控一切,但接受挑战并寻求“快感”。我们的回报通常是名声 无论是通过学术出版物、为安全咨询业务赢得客户、赢得学术团体或政府机构颁发的奖章,甚至是在社交媒体上。有时我们会因为恼怒而破坏 stu ,这样我们就可以规避一些阻止我们修复我们拥有的东西的东西;有时还有利他主义的因素。例如,过去有人来找我们抱怨他们的银行卡被盗并用于购买 stu ,银行不给他们退款,说他们的 PIN 码肯定被用过了,但实际上没有.我们调查了其中一些案例并发现

对芯片和 PIN 系统的 No-PIN 和预播放攻击,我将在关于银行业务的章节中描述（坏人实际上已经发现了这些攻击,但我们复制了它们并为一些受害者伸张了正义）。

发现漏洞并向软件供应商或系统运营商报告漏洞的安全研究人员过去常常冒法律威胁的风险,因为公司有时认为这比修复问题更便宜。因此,一些研究人员开始在邮件列表中匿名披露错误;但这意味着坏人可以立即使用它们。到 2000 年代初,IT 行业已经发展出负责任的披露做法,研究人员可以在披露之前几个月向维护人员披露错误。许多公司运营漏洞赏金计划,为漏洞提供奖励;因此,独立研究人员现在可以通过出售漏洞大赚一笔,而且现在不止一位勤奋的研究人员这样做已经赚了超过 100 万美元。自 Stuxnet 蠕虫病毒以来,各国政府竞相储备漏洞,我们现在看到一些公司从研究人员那里购买漏洞以将其武器化,然后将其出售给网络武器供应商。一旦被使用,它们就会传播,最终被逆向工程和修补。我将在有关经济学和保证的章节中更详细地讨论这个生态系统。

一些更传统的部门仍然没有采用负责任的披露。
大众汽车起诉了伯明翰大学和奈梅亨大学的研究人员,他们对一些在线汽车盗窃工具进行了逆向工程,并记录了他们的远程钥匙输入系统有多糟糕。公司输了,自欺欺人并宣传他们车辆的不安全性（我将在第 4.3.1 节中讨论技术细节,在第 27.5.7.2 节中讨论政策）。最终,随着软件渗透到一切,软件行业的工作方式也将变得更加普遍。与此同时,我们可以预料到动荡。掩盖危害其客户的问题的公司将不得不考虑内部告密者或外部安全研究人员可能会查明正在发生的事情,并且当这种情况发生时,通常会建立一个负责任的披露流程来调用。这将给未能将其商业模式与它保持一致的公司带来成本。

2.5 沼泽

我们的第四类是虐待,我们通常指的是对人而不是对财产的侵犯。这些范围从学校的网络欺凌一直到国家赞助的 Facebook 广告活动,这些活动让人们以死亡威胁淹没立法者。我将首先处理规模庞大的违法行为,包括政治骚扰和儿童性虐待材料,然后处理不涉及的围栏,从学校欺凌到亲密伴侣虐待。

2.5.1 黑客行动主义和仇恨运动

宣传和抗议随着技术的发展而发展。古代社会不得不靠史诗来凑合。通过在论坛上发表演讲,城市使人们能够直接与数百人交流;书写的发明使规模进一步扩大。十六世纪印刷术的普及导致了

到第十七世纪的宗教战争,第十八世纪的日报和第十九世纪的大众市场报纸。活动家们学会了在大众媒体中争夺注意力,并随着广播和电视的出现磨练自己的技能。

互联网时代的激进主义开始于使用网络媒体动员人们进行常规游说,例如写信给立法者； Indymedia 和 Avaaz 等组织在 2000 年代开发了这方面的专业知识。

2011 年,Wael Ghonim 等活动家利用社交媒体引发了阿拉伯之春,我们将在第 26.4.1 节中对此进行更详细的讨论。从那时起,政府开始严厉打击,激进主义蔓延为在线仇恨运动和激进化。许多仇恨运动是由政府或反对党秘密资助的,但绝不是全部:单一问题的运动团体也是参与者。如果你能激励数百人发送愤怒的电子邮件或推文,那么接收端的公司或个人就会遇到真正的问题。拒绝服务攻击可能会中断运营,而 doxxing 可能会造成真正的品牌损害,并给高管和员工造成困扰 。

激进主义者的目标、组织一致性以及违法程度各不相同。有一个完整的范围,从完全守法的非政府组织,这些非政府组织让他们的支持者给立法者发电子邮件,再到稍微急躁的非政府组织,他们可能通过让机器人点击新闻报道来操纵新闻,玩弄媒体分析并让编辑更加关注他们的问题。然后,还有前往受人尊敬的报纸的告密者、在 Twitter 帐户的温和匿名背后骚扰人们的政治党派、闯入目标公司并破坏其网站甚至对它们进行 doxx 的黑客。上面 2.2.5 中描述的 Climategate 丑闻可能是黑客行动主义者进行人肉搜索的一个例子。在最顶端,有一些铁杆分子最终因恐怖主义罪行入狱 。

在 1990 年代,我很高兴地使用电子邮件和 usenet 来动员人们反对通过英国议会的监控法案,我将在后面的第 26.2.7 节中描述。 2003 年,当动物解放阵线以我的大学为目标时,我发现自己处于黑客行动主义的接收端,因为计划建造一个猴舍,供灵长类动物用于研究。在线部分包括发送给工作人员的数千封电子邮件,其中包含令人痛苦的猴子大脑中有电线的图像;这是“结盟”的早期例子,数百人在网上联合起来攻击一个目标。我们通过关闭他们的电子邮件帐户来轻松应对在线攻击。但他们坚持进行身体示威和媒体骚扰;我们的副校长决定减少损失,猴舍转而去了牛津。一些领导人后来因袭击当地一家药物检测公司的员工并在医学研究人员的汽车下放置炸弹 [21] 而因恐怖主义罪名入狱。

在线羞辱已成为一种流行的抗议手段。它可以是自发的,当事件像病毒一样传播时,会形成一群自发的义务警员。
一个早期的例子发生在 2005 年,当时首尔的一位年轻女士在她的狗在地铁车厢内排便后未能清理干净。另一名乘客拍下了这一事件并上传到网上;几天之内,“狗屎女孩”就被迫躲藏起来,放弃了她的大学课程 [418]。此后还有许多其他案例。

Twitter 等平台的力量在 Gamergate 中变得显而易见,这场风暴是由前男友在 2014 年 8 月公开对一名女性游戏开发者的辱骂性评论引发的,并逐渐演变成对游戏行业女性和批评该行业男性主导文化的女权主义者。许多人被人肉搜索、殴打或赶出家门 [1932 年]。骚扰是在 4Chan 等匿名留言板上协调进行的,攻击者会联合起来攻击一个特定的目标 然后这些目标也受到主流保守派记者的批评 [1130]。这场运动似乎群龙无首,而且不断演变,其中一个持续的主题是对“社会正义战士”的咆哮。它似乎促进了影响两年后 2016 年大选的另类右翼运动的发展。

越来越多的人认识到愤怒的网络暴徒的力量,导致政客们在各个层面煽动他们,从试图破坏他们的竞争对手的地方政客到试图左右敌对州选举的民族国家。愤怒的暴民是发达国家现代政治中一个令人不快的特征;在欠发达国家,情况变得更糟,在印度等国家发生了真正的私刑(执政的印度人民党至少从 2011 年开始就一直在组建一支巨魔军队,以骚扰政治对手和民间社会批评者 [1637])。公司成为目标的频率较低,但确实会发生。与此同时,社交媒体公司面临着审查在线内容的压力,而且由于人工智能程序很难区分外国政府的笑话、辱骂、阴谋论和信息战,他们最终不得不雇用越来越多的版主。我将在下面的 26.4 中回到这方面的法律和政策方面。

2.5.2 儿童性虐待材料

当互联网在 1990 年代引起政府的注意并且他们想知道如何处理它时,首先要监管的是 2001 年布达佩斯公约中的儿童性虐待 (CSA) 图像。我们几乎没有数据关于 CSA 材料的真正流行,因为法律限制使得执法部门以外的任何人都很难进行任何研究。在许多国家,对 CSA 材料的处理方法对实际减少危害的重视程度低于其应有的水平。事实上,许多关于网络性犯罪的法律设计得很糟糕,而且似乎更多地是为了利用愤怒而不是为了尽量减少受害者的数量和他们所遭受的伤害。 CSA 可能是一个案例研究,说明如何由于取证失败、删除失败、武器化和法律规范差距而不进行在线监管。

最臭名昭著的取证失败是英国的矿石行动,我在 26.5.3 中对此进行了更详细的描述。简而言之,数千名男子在滥用网站上发现他们的信用卡号码后因涉嫌 CSA 违法行为而被捕,其中可能有一半最终成为信用卡欺诈的受害者。数百名无辜的人的生命被毁了。然而,巴西和印度尼西亚的儿童受害者没有采取任何措施,当局仍然无法有效地关闭托管 CSA 材料的网站。在大多数国家,CSA 的取缔要么是警察的垄断,要么是根据公共部门规则运作的受监管机构(美国的 NCMEC 和美国的 IWF)

英国），需要几天到几周的时间;如果政府使用银行用来处理网络钓鱼站点的私营部门承包商，事情会进展得更快 [938]。公共部门的垄断源于许多国家/地区的法律，这些法律将拥有 CSA 材料定为严格责任
ence。

这不仅使得使用通常的滥用渠道处理此类材料变得困难，而且还允许将其武器化:抗议者可以将其发送给目标，然后向警方报案。这也让家长和老师很难明智地处理青少年使用约会应用程序或建立远程关系时发生的事件。整件事一团糟，是立法者想在不了解技术的情况下强硬说话造成的。 （CSA 材料现在对一些立法者的工作人员来说是一个很大的烦恼 ，也使得一些报纸的记者不愿公开他们的电子邮件地址。）

随着色情短信在青少年中越来越受欢迎，法律与规范之间出现了差距。不管喜欢与否，当智能手机于 2008 年问世时，向伴侣（真实的和预定的)发送亲密照片已成为许多国家青少年的正常行为。这距布达佩斯公约仅七年，其签署者可能无法想象性图片18 岁以下的人可能不是虐待。由于该公约，现在拥有 18 岁以下任何人的私密照片在已批准该公约的 63 个国家中的任何一个国家都可能被判入狱。青少年嘲笑学校老师不拍摄或分享此类照片，但最终的结果是真正的伤害。孩子们可能会被欺骗或被迫分享他们自己的照片，即使最初的分享是双方同意的，接收者以后也可以用它来勒索或只是传来笑去。收件人 - 即使是无辜的 - 也犯下了刑事罪行仅仅将照片放在手机上，这样孩子们就可以陷害其他孩子并谴责他们。这导致了一般的欺凌问题和更具体的亲密伴侣虐待问题。

2.5.3 学校和职场欺凌

网络骚扰和欺凌是现代社会生活中的一个事实，不仅在学校如此，在工作场所也是如此，因为人们在争夺地位、朋友和资源。
从媒体报道的青少年因网络虐待而自杀的报道来看，您可能认为网络欺凌现在是问题的主要原因 至少在学校是这样 但数据显示，这一比例还不到一半。英国的一项年度调查显示，大约四分之一的儿童和青少年经常受到欺凌（13% 的口头欺凌、5% 的网络欺凌和 3% 的肢体欺凌），而大约一半的人有时会受到欺凌（分别为 24%、8% 和 9%)[565] .我所知道的唯一一项针对所有年龄段的全国调查是法国全国受害调查，自 2007 年以来，该调查不仅收集了有关入室盗窃等身体犯罪和欺诈等网络犯罪的数据，还收集了有关骚扰的数据 [1458]。这是基于对 16,000 户家庭的面对面访谈，2017 年的调查报告了 200 万起威胁行为，其中 7% 是通过社交网络进行的，另外 9% 是通过电话进行的。但社交媒体让情况变得更糟了吗?研究表明，社交媒体的使用对青少年幸福感的影响是微妙的，充其量是很小的，并且取决于分析方法 [1473]。

然而，媒体上有关于青少年自杀率上升的说法，一些评论员将其与社交媒体的使用联系起来。值得庆幸的是，经合组织的死亡率统计数据显示

这也是不正确的:在 1990-2015 年期间,15-19 岁的自杀率从每 100,000 例中的约 8 例略微下降到约 7 例 [1477]。

2.5.4 亲密关系虐待

正如我在上一节结束时讨论举报人 对公司的内部威胁 我将以亲密关系虐待、对家庭和个人的内部威胁结束本节。 Gamergate 可能是一个闪光灯的例子,但保护自己免受前亲密伴侣和其他家庭成员的伤害是一个大规模存在的真正问题 大约一半的婚姻以离婚告终,而且并非所有分手都是友好的。 27% 的女性和 11% 的男性遭受过亲密伴侣虐待。跟踪当然不仅限于前合作伙伴。名人尤其可能会被素未谋面的人跟踪 偶尔会有悲剧性的结果,例如约翰·列侬 (John Lennon)。但对于男性伴侣来说,其中大部分是罪魁祸首,而且大多数国家的执法部门历来不愿对他们采取任何有效措施。技术使受害者的处境更糟。

一个子问题是发布未经同意的亲密图像 (NCII),曾被称为“报复性色情” 直到加州检察长卡玛拉·哈里斯反对称这是网络剥削和犯罪。她的信息传达给了大型服务公司,这些公司自 2015 年以来一直根据受害者的要求取下此类材料 [1690]。这是继 2012 年早些时候的一份报告之后,哈里斯记录了越来越多地使用智能手机、在线市场和社交媒体迫使弱势群体从事包括卖淫在内的不受监管的工作 这引发了关于如何使用技术联系和帮助犯罪受害者的更广泛问题[866]。

一个女人离开一个虐待和控制的丈夫所面临的问题是信息安全领域中最困难的问题之一。所有通常的建议都是错误的:你的对手不仅知道你的密码,而且拥有如此深厚的背景知识,以至于他可以回答你所有的密码恢复问题。通常分为三个阶段: 物理控制阶段,滥用者可以访问您的设备并可能安装恶意软件,甚至破坏设备;当您试图寻找新家、工作等时,这是一个高风险的逃避阶段;和一个生活分开的阶段,你可能想屏蔽位置、电子邮件地址和电话号码以避免骚扰,并且可能会有终生的担忧。平均需要七次逃脱尝试才能重获新生,断开在线服务可能会导致其他虐待行为升级。越狱后,可能要限制孩子上网,断绝关系;让您的孩子张贴任何东西都可能泄露学校位置并导致施虐者出现。你可能不得不改变职业,因为如果你不能再做广告,就不可能以个体经营者的身份工作。

为了支持这样的用户,负责任的设计师应该认真考虑在高压力和高风险时期的可用性;他们应该允许用户拥有多个帐户;他们应该设计一些东西,这样查看你的历史的人就不能告诉你删除了任何东西;他们应该推送双因素身份验证、异常活动通知和隐身模式。他们还应该考虑幸存者如何收集证据用于离婚和监护案件以及可能的刑事诉讼,同时最大限度地减少

外伤 [1248]。但这不是我们在现实生活中发现的。许多银行并不想真正了解家庭内部的纠纷或金融剥削。一些国家的一个大问题是跟踪软件 旨在监控合作伙伴、前合作伙伴、儿童或员工的应用程序。 Citizen Lab 的一份报告详细说明了这些应用程序在信息安全方面的不良做法，它们是如何明确地向施虐者推销的，以及它们是如何在欧洲和加拿大触犯法律的；至于美国和澳大利亚，超过一半的施虐者使用跟踪软件追踪女性 [1495]。然后是 Absher 应用程序，它使沙特阿拉伯的男性能够以发达国家无法接受的方式控制女性；它在应用程序商店中的可用性导致了世界其他地方对苹果和谷歌的抗议，但截至 2020 年，它仍然存在。

亲密虐待对于设计师和其他人来说很难处理，因为它与伴侣之间、朋友和同事之间、父母和年幼的孩子之间，以及后来的孩子和年迈的父母之间的正常人类照顾纠缠在一起。许多关系在很大程度上是有益的，但也有一些虐待方面，参与者往往不同意哪些方面。我所知道的最好的分析是 Karen Levy 和 Bruce Schneier，讨论了多种动机的结合、导致技术漏洞的共同存在以及导致关系漏洞的权力动态 [1154]。技术助长了人际关系中的多种隐私侵犯，从偶然到严重的虐待；设计师需要意识到家庭不是单位，设备不是个人，设备的购买者不是唯一的用户。我预计在未来几年内，对亲密虐待的担忧将扩大到对朋友、老师和父母虐待受害者的担忧，并且会因家庭和学校自动化的新形式而变得更加复杂。

2.6 总结

您构建或操作的系统可能会受到范围广泛的对手的攻击。弄清楚谁可能会攻击您以及如何攻击您很重要，能够弄清楚您是如何受到攻击的以及被谁攻击也很重要。您的系统也可用于攻击他人，如果您不事先考虑到这一点，您可能会发现自己陷入严重的法律或政治麻烦之中。

在本章中，我将对手分为四个主题：间谍、骗子、黑客和沼泽。并非所有威胁行为者都是坏人：许多黑客负责任地报告漏洞，许多举报人热心公益。 （“我们的”间谍当然被认为是好的，而“他们的”是坏的；道德价值取决于游戏中的公共和私人利益。）情报和执法机构在狩猎时可能会混合使用 trac 数据分析和内容采样，并有针对性地收集收集；收集方法包括通过恶意软件进行的法律强制和欺骗。间谍和骗子都使用恶意软件来建立僵尸网络作为基础设施。骗子通常使用机会主义收集进行大规模攻击，而对于有针对性的工作，鱼叉式网络钓鱼是首选武器；情报机构可能拥有更高级的工具，但使用相同的基本方法。还存在与特定业务部门相关的网络犯罪生态系统；基本上，犯罪将在它可以扩展的地方发展。至于沼泽，选择的武器是愤怒的暴民，现在由国家和激进组织使用

甚至个人演说家。滥用可以通过多种方式扩展,在设计系统时,您需要弄清楚针对它的犯罪或滥用它可能会如何扩展。仅仅考虑可用性是不够的;您还需要考虑可滥用性。

人身虐待也很重要。每个警察都知道袭击或谋杀你的人通常不是陌生人,而是你认识的人 也许是你班上的另一个男孩,或者是你的继父。安全研究界忽略了这一点,也许是因为我们大多是来自好社区稳定家庭的聪明白人或亚裔男孩。

如果您要保护任何规模的公司,您会看到网络上有足够多的机器被感染,您需要知道它们是僵尸网络中的僵尸还是目标攻击的一部分。所以仅仅依靠打补丁和杀毒是不够的。您需要观察您的网络并保留足够好的日志,以便在发现受感染的机器时,您可以判断是孩子在构建僵尸网络,还是目标攻击者在失去一个观点后争先恐后地开发另一个观点。您需要制定应对事件的计划,这样您就知道该向谁求助,这样您的 CEO 就不会像搁浅的鱼一样在电视摄像机前喘不过气来。您需要系统地考虑您的基本控制措施:从勒索软件中恢复的备份、阻止企业电子邮件泄露的支付程序,等等。如果您是在为一家大公司提供建议,他们应该已经掌握了很多,如果是一家小公司,您需要帮助他们弄清楚如何做足够多的事情。

本书的其余部分将填写详细信息。

2.7 研究问题

直到最近,对网络犯罪的研究还不是真正的科学。有人会得到一些数据 通常是来自反病毒公司的保密协议 计算出一些统计数据,写出他们的论文,然后去找工作。任何其他想要检查结果或尝试新型分析的人都无法获得这些数据。自 2015 年以来,我们一直在尝试通过建立剑桥网络犯罪中心来解决这个问题,我们在该中心收集有关垃圾邮件、网络钓鱼、僵尸网络和恶意软件的大量数据,作为研究人员的共享资源。我们很高兴其他学者使用它。如果您想研究网络犯罪,请致电我们。

我们还需要类似的东西用于间谍活动和网络战。试图将恶意软件植入控制系统和其他操作技术的人很可能是国家行为者,或者是向国家出售网络武器的供应商。艾森豪威尔总统对“军工联合体”的批评在这里毫无疑问地适用。然而,似乎没有一家传统智库有兴趣追踪正在发生的事情。因此,各国更有可能做出战略误判,这不仅会导致网络冲突,还会导致真正的动能变化。

至于对网络滥用的研究,现在有一些研究,但技术专家、心理学家、犯罪学家和政治学家之间的交流还不够。有很多问题,从儿童和年轻人的福利和权利到我们举行公平和自由选举的能力。我们

需要让更多的技术人员参与公共政策问题,并让更多的政策人员了解技术的现实。我们还需要让更多的女性以及来自发达国家和欠发达国家的贫困社区的人们参与进来,这样我们就不会那么狭隘地看待真正的问题是。

2.8 延伸阅读

关于本章所讨论主题的文献很多,但相当零散。斯诺登揭露的起点可能是格伦·格林沃尔德 (Glen Greenwald) 的书《无处可藏》[816];有关俄罗斯战略和策略的说明,请参阅 2018 年提交给美国参议院外交关系委员会的报告 [385];有关宣传史的精彩介绍,请参阅 Tim Wu 的“The Attention Merchants”[2050]。有关网络犯罪的调查,请参阅我们 2012 年的论文“衡量网络犯罪的成本”[90] 和我们 2019 年的后续文章“衡量网络犯罪不断变化的成本”[91]。比尔·钱布利斯 (Bill Chambliss) 等犯罪学家研究了国家组织的犯罪,从上个世纪的海盗和奴隶制,到最近情报机构走私毒品和武器,再到酷刑和暗杀;这为评估非法监视提供了更广泛的背景。 Zoè Quinn 的“Crash Override”[1567] 讲述了 Gamergate 的故事。最后,阻止 Wannacry 的恶意软件专家 Marcus Hutchings 的故事在 [811]。