防御恶意软件和僵尸网络

非官方中文译本 • 安天技术公益翻译组 译注

文档信息			
原文名称	Combating Malware and Botnets --取自 A Roadmap for Cybersecurity Research 第 4 章第 5 节。		
原文作者	美国国土安全部	**原文发布日期**	2009 年 11 月
作者简介	美国国土安全部为美国政府设立的一个联邦行政部门，负责国内安全及防止恐怖活动。 http://en.wikipedia.org/wiki/Homeland_security		
原文发布单位	美国国土安全部		
原文出处	https://www.dhs.gov/sites/default/files/publications/CSD-DHS-Cybersecurity-Roadmap.pdf		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部		

	分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。

防御恶意软件和僵尸网络

背景

本文讨论的问题是什么？

恶意软件是指装载在机器上（通常是合法所有者不知情的情况下）、感染及其并为攻击者带来收益的攻击软件或硬件。目前，恶意软件的种类包括病毒、蠕虫、木马、间谍软件和僵尸可执行文件。间谍软件用于暗中追踪和/或向未经授权的第三方传输数据。僵尸（“robot”的简称）秘密安装于目标系统，允许未经授权的用户远程控制受感染的计算机以实现各种恶意目的[GAO2007]。僵尸网络是指由被僵尸恶意软件感染的及其组成的网络，这些网络受攻击者的控制。

恶意软件通过多种媒介感染系统，包括通过受感染的计算机传播、诱骗用户打开被感染的文件、或诱导用户访问恶意软件传播的网站。当 USB 插入受感染的设备时，恶意软件可以自我加载到 USB，然后感染该 USB 之后插入的其他所有系统。恶意软件可以通过包含嵌入式系统和计算逻辑的设备传播。例如，工厂中受感染的测试设备感染了受测试的设备。总之，恶意软件可以在系统生命周期的任何一点插入系统。万维网已经成为恶意软件传播的主要载体。特别是，恶意软件可以远程注入到其它合法网站，随后感染这些“受信”网站的访问者。

恶意软件并不针对特定的操作系统或设备类别，这样的例子不胜枚举。恶意软件已经被发现在外部设备中（例如数码相框和硬盘驱动器），并可能会编码到系统中（生命周期攻击）。越来越智能的家电是很脆弱的，例如对高端咖啡机[Thu2008]的潜在攻击。很难或者不可能提供这些设备的补丁。表 5.1 总结了恶意软件的传播机制。

潜在的受害系统包括最终用户系统，服务器，网络基础架构设备如路由器和交换机，以及过程控制系统如监控和数据采集系统（SCADA）。

一个相关的政策问题是，理智的人们对什么是合法商业活动与恶意软件存在不同意见。此外，表面上合法的软件实用程序（例如，用于数字版权管理[DRM]的程序）可能导致意想不到的后果，该后果与恶意软件[Sch2005，Hal2006]的影响类似。

攻击者很可能会在将来开发出新的感染机制，可能是通过发现当前系统的新安全漏洞或者新的通信和计算范式的漏洞。

可能的技术挑战是以下几点：

- 避免恶意软件进入平台。
- 检测已安装的恶意软件。
- 一旦恶意软件安装在平台上，尽可能降低损害。
- 面临恶意软件时，安全有效地操作。
- 根据被检测到的恶意软件的信标确定风险级别。
- 一旦恶意软件被安装，则将其移除（修复），监测和确定其来源（追溯）。（在高度监控系统中，有时候追溯完成后才进行修复。在这方面蜜罐也是有用的。）

2009 年 8 月在圣达菲举办的计算网络防御 NSA/ ODNI 研讨会是这个方向的例子（http://www.c3e.info）。

什么是潜在威胁？

恶意软件对信息时代的许多方面产生影响，本文会对一些方面进行介绍。恶意软件可能影响单台主机到网络，可能导致困扰甚至灾难性的后果。负面影响包括降低系统性能和数据破坏或修改。间谍软件允许攻击者记录用户操作（例如窃取用户证书和身份）。僵尸恶意软件能够利用受感染的计算机创建大型网络，从而增加其攻击实力。僵尸网络和恶意软件的负面后果包括垃圾邮件、分布式拒绝服务（DDoS）、窃听流量（嗅探）、点击欺诈、降低系统稳定性、泄密、数据完整性的损失、无法访问网络资源（例如，被识别为僵尸节点，然后被 ISP 或网络管理员阻断，即一位受害者向另一位发起 DoS 攻击）。某些类型网站（如流行的社交网站、web 论坛和 mashup）越来越多，其接受用户生成的内容，如果不仔细检查，攻击者就会注入恶意内容，稍后可能会被用户下载。

除了扰乱使用，恶意软件还可能会产生严重的经济和国家安全后果。恶意软件能够使攻击者控制关键的计算资源，这反过来又可能导致信息泄露、中断和基础设施系统的不稳定（“拒绝控制”）以及金融市场的操纵。

表 5.1：恶意软件传播机制

恶意软件传播机制	示例
生命周期	从开发者开始，无论是故意的还是通过使用被感染的开发套件。
扫描和漏洞利用	大量传播的蠕虫。可能不需要在用户操作就能够传播。
被感染的设备	感染的 USB 令牌、CD / DVD、相框等
被感染的文件	E-mail 附件
Web	恶意网站诱使用户下载被感染的文件。（注：当用户访问这些网站时，较新的恶意软件可能会感染受害者的系统，或通过跨站点脚本将其重定向到被感染的网站）

恶意软件对网络基础设施的组成部分尤其有害。例如，针对域名系统（DNS）的攻击能够将流量定向至恶意网站，并发动中间人和拒绝服务攻击。成功的 DNS 攻击能够使攻击者拦截和重定向流量，例如重定向至恶意或欺骗服务器。除了重定向到恶意服务器，还有选择性或定时 DoS 攻击。从 DNS 中删除一个网址比通过洪泛攻击拒绝服务更容易。这些就是向.gov 执行 DNSSEC 和向 DNS root 服务器执行 DNSSEC 的根本考虑因素。

对手在活跃市场中购买和销售漏洞并租赁僵尸网络[Fra2007]。通过复杂的网络钓鱼攻击，这些僵尸网络可用于大规模分布式攻击、垃圾邮件传播和敏感数据（如安全证书、财务信息和公司专利信息）窃取。使用僵尸网络使得追踪最终肇事者非常困难。僵尸网络向攻击者大量资源，用于监视敏感系统等。

恶意软件传播通常出现于企业和家庭计算机中。然而，它也有可能影响控制系统和其它基础设施系统。例如，2003 年，俄亥俄州 Davis-Besse 核电站的报警系统被 Slammer 蠕虫感染，尽管这些系统被认为不会遭受此类攻击（该工厂当时并未连网）[SF2003]。恶意软件的传播可能加剧了美国东北部 2003 年的大停电并减缓了其恢复。恶意软件作者将针对嵌入式系统和新兴工具，如电力厂的高级计量基础设施（AMI）。

还有与修复受感染及其有关的影响。从 ISP 的角度来看，最大的影响包括处理客户支持电话、采购和发布反病毒（A / V）软件，并且尽量减少客户流失。对于一些后果严重的政府应用程序，感染甚至可以促进更换系统组件/硬件。

谁是潜在受益者？他们的需求是什么？

恶意软件可能会影响任何使用计算机或其它信息系统的用户。在专业管理系统的情况下，恶意软件修复（例如清理受感染的机器）是很难的，超出了很多个人用户和小型办公室/家庭办公室（SOHO）用户的技术能力。快速、可扩展、易用和廉价的修复可能是该方面最重要的问题。如下文所讨论的，改进检测方法和隔离受感染的系统也是必要的。表 5.2 总结了受益者、挑战和需求。

恶意软件对互联网和其他重要信息基础设施的机密性、完整性和可用性的潜在威胁时另一个严重的问题。一个真实例子是： 2007 年春通过分布式僵尸网络对爱沙尼亚的网络基础设施发动攻击[IW2007]。这一事件引发了北约集体自卫任务是否涵盖“网络战”的讨论。在无法追溯的情况下，问题仍然没有实际意义。2008 年 8 月，格鲁吉亚出现了网络攻击，但是仅限于对格鲁吉亚政府网站发起拒绝服务，并没有针对网络基础设施[Ant2008]。最近的恶意软件是 Conficker，最初通过尚未升级安全补丁的系统传播，并随后周期性地出现了更加复杂的版本。

执法部门和国防部对追溯特别感兴趣，但是正如上文所述，目前追溯是很困难的。

当前的实践现状如何？

商业反病毒软件和入侵检测系统/入侵防御系统（IDS / IPS）厂商，以及开源团队，试图通过各种载体发现或防止感染。 清除恶意软件和系统重启是目前主要的清理机制。这种做法的根本挑战是攻击者能够不断释放重新包装和/或修改的恶意软件，但是新的 A / V 签名需要时间来生产、测试和发布。此外，用户团队开发、测试和发布补丁（该恶意软件利用的漏洞的补丁）也是需要时间的。另外，恶意软件开发者可以通过最新的 A / V 版本来测试自己的软件。

表 5.2：受益者、挑战与需求

受益者	挑战	需求
用户	受到多个恶意软件向量的攻击，系统没有进行专业管理。	人性化的预防、检测、遏制和补救。
管理员	保护关键系统，保持持续性；在面对恶意软件变种爆发式增长时进行企业规模的整治。	新的检测范式、强大的整治、预防措施和补丁的稳健分布。
基础设施系统	防止意外感染[SF2003]，针对性感染的挑战。	类似于管理员需求，但往往对遗留系统和能力（而无法在任意时间进行修补和重启）有特殊限制。
ISP	提供连续性的服务，应对比管理员面临的更大规模的恶意软件。	对传播攻击和僵尸网络的防御，在恶意软件领域的进展能够减轻这些后果。
执法部门	越来越多的恶意软件和僵尸网络用于犯罪欺诈以及数据和身份窃取。	强大的追溯，先进的取证。
政府和国防部	防御系统的感染增加，如 Welchia 感染海军陆战队内部网（NMCI）[Messmer 2003]。最近,出现了针对防御系统[LATimes08]的恶意软件。	与管理者、互联网服务供应商和执法部门的需求一致。

对恶意软件检测和防御的研究一直在进行。例如，网络威胁分析项目（http://www.cyber-ta.org）。另外值得注意的是反网络钓鱼工作组（APWG）：http://www.antiphishing.org。

基于 Web 的 A/V 服务已经进入市场，有的提供鉴定服务：即安全人员可以提交可疑的可执行文件，用当前工具确定它是否是恶意的。这种机制最有可能作为恶意软件开发者的测试平台（VirusTotal）。

美国国家标准和技术研究院（NIST）安全内容自动化协议（SCAP）是一种采用特定标准进行自动化漏洞管理、测量和政策合规性评估的方法。

操作系统和应用程序供应商已经开发了在线更新和软件 bug（包括影响安全的 bug）补丁机制。其他防御方法包括反间谍软件、受信网站和机器白名单、声誉机制。

当前的检测和修复方法都节节败退，因为攻击者修改恶意软件来规避大多数现有检测方法是对手相对容易的。鉴于恶意软件金华的趋势，现有的方法（如 A / V 软件和系统补丁）的有效性不断降低。例如，恶意软件编写者开发了若干策略（如多态、压缩和加密）来隐藏签名，规避现有的 A / V 软件的检测。新恶意软件变种的发现和系统补丁及 A / V 更新之间也存在时间差距。此外，一旦恶意软件在目标系统上建立据点，恶意软件作者也力求禁用或颠覆现有的 A / V 软件（例如 Conficker 蠕虫的更高版本）。A / V

软件本身可能容易受到周期性攻击，使其在安装前就会失效。补丁也是一个必要的防御措施，但是也有缺点。例如，攻击者可以对补丁进行逆向工程，从而发现原始漏洞。这可能使得恶意软件编写者完善对未打补丁的系统的攻击。我们可以从 Conficker 近期的多个版本获得经验。

特别是身份窃取，这是恶意软件的一个潜在后果，但也可以通过其他方法进行。身份窃取保险和修复是一个新兴的商业市场。这意味着，一些企业认为自己面临这样的风险。

研究现状如何？

在恶意软件检测、捕获、分析和防御方面有很多活动。主要方法包括虚拟化（在某一特殊宿主的虚拟环境中进行检测/控制/捕获）[Vra2005]和蜜网（网络环境特别是虚拟环境，部署于未使用的地址空间来捕获恶意软件副本以便进一步分析）[SRI2009]。恶意软件越来越多地用来检测虚拟和蜜网环境，并改变其响应行为。行业研究将虚拟机推向了硬件和软件的可信平台模块（TPM）和虚拟机管理程序报术，以及清理/修复（技术上来讲，在某些情况下可以远程实现，但如果系统所有者并没有获得事先许可，则可能会造成法律和政策后果）。美国国土安全部资助了正在进行的跨域攻击的相关性和僵尸网络检测和缓解研究[CAT2009]。分析技术包括传统计算机科学的静态和动态分析方法。

对于特征库的扩展和保护系统方法，有相当多的开源 IDS（Snort 和 BRO）研究。最近的研究认为从可疑数据包有效载荷的共同字节序列自动生成签名[Kim2004]是防御多态恶意软件的一种方法。

对恶意软件在被感染主机上的运行痕迹和相思特征已经进行了大量研究，但我们对恶意软件问题的网络维度的理解不够。某些网络行为使恶意软件感染的重要先导或信标。例如，DNS 区域的变化可以预示着垃圾邮件攻击。DNS 注册的快速变化（如 Conficker）可能表明特定主机是大型僵尸网络的 C2 网络的一部分。在某些网络端口的加密流量可能表明特定主机向僵尸网络发送 C2 流量。

虚拟化和蜜网还是能够提供恶意软件检测、分析和响应方法，至少在近期和中期是这样。为了使蜜网继续有用，必须解决的问题包括：

- 攻击者寻找的能够识别蜜网的特征？
- 蜜网中“进入和撤退”与“进入和攻击”的比例如何？
- 蜜网中观察到的现象与真实世界中的“脚本小子”攻击和针对性恶意软件活动相比如何？

DARPA 的自我再生系统（SRS）程序围绕上述几点开发了一些技术。

对正确的系统使用来说，人工多样性是透明的，但对于漏洞利用则是多样性的。这一直是一个可望而不可及的目标，但商业和研究机构已经取得了一些进展。现在的许多操作系统包括地址空间随机化，并出现了系统模糊处理（功能相当于不同的执行）[Sha2004]，虽然还有一些基本限制。

新兴的方法，比如基于行为的检测和语义的恶意软件描述，表现出了不错的前景并部署于商业反病毒软件中。然而，必须开发新技术，以便与恶意软件的开发保持同步。

未来方向

可以细分为哪些类别？

对于恶意软件和僵尸网络的话题，防止/保护/检测/分析/响应是合理的框架（见表 5.3）。虚拟化和沙箱环境的保护和检测能够防护系统、应用程序和协议。分析包括检查 IT 专家捕获的恶意软件（例如，蜜网捕获的恶意软件），从而制定有效的防御措施。响应是可以由非 IT 专业人员实施并实现成本效益的。

主要的研究差距是什么？

由于恶意软件越来越复杂，且用户（特别是消费系统）不能够及时更新反病毒软件，所以 A/V 和 IDS/IPS 方法的有效性不断降低。恶意软件的多态性速度超过了在 A/V 和 IDS/IPS 特征的生成速度。

目前的研究举措不足以解决日益复杂和隐蔽的恶意软件，包括恶意代码本身的加密和压缩，以及僵尸网络的加密 C2 通道和快速 DNS [Sha2008， Hol2008] 。从广义上讲，研究应更好地了解恶意软件的敏捷性和多态性。恶意软件样本的 C2 结构的自动检测是一个重要的挑战。

对于恶意软件和僵尸网络，我们没有充分地分类。研究发现，恶意软件的很多变种衍生于之前的变种，但这一途径尚未深入探索。该领域的进展可以对一般类的恶意软件进行防御，其中包括作为尚未出现的变种。易于理解的分类也可以支持和改善归因方法。

目前，攻击者-防御者关系是不对称的。对特定系统类型开发漏洞的攻击者会发现大量几乎相同的漏洞。因此，最好是迫使攻击者针对单个主机开发漏洞，从而使开发恶意软件来破坏机器的成本显著提高。人工的多样性可以解决攻击者-防御者关系的日益不对称问题。

表 5.3：潜在方法

种类	定义	潜在方法
防御	防止恶意软件的制作和传播	IDS / IPS、A/V、虚拟化、固有安全系统
保护	当系统中存在恶意软件时，保护系统免受感染	IPS、A/V、固有安全系统
检测	检测在网络中传播的恶意软件，检测特定系统上的恶意软件感染	IDS / IPS、A/V、虚拟化、欺骗性环境
分析	分析恶意软件的感染、传播和破坏机制	静态和动态分析，大型安全环境中的实验
响应	修复恶意软件感染并确定防御未来爆发（与预防类有关）的机制	升级 IDS/IPS 和 A/V、固有安全系统、脆弱的客户端、安全的云计算模式

对于主机来讲，恶意软件防御（例如，A/V 软件、Windows 更新等）通常是操作系统的一部分或扩展。这一事实使恶意软件能够轻松地攻击和禁用这些基于主机的防御方法。研究差距的概要在表 5.4 中列出。

该方面研发的示例性问题？

针对 OS 漏洞的强大的安全机制： 虽然针对操作系统的二进制恶意软件仍然是很重要且值得大量短期投资的，但是恶意软件越来越多地通过社会工程和其他机制攻击浏览器和电子邮件。

保护用户免受欺骗性感染：目前，通过社会工程、安全控制的复杂性和流氓内容注入，攻击者诱骗用户与其系统交流，但是用户却认为正在执行有效的交易，如网上银行业务。这方面的研究应该增加用户培训、提高用户的安全意识、使

安全控制更加实用（尤其是在浏览器中）。搜索引擎控制会使受害者自己感染恶意软件（例如，通过访问受感染的网站），而非攻击者去感染目标用户（例如，通过网络钓鱼和电子邮件）。结构化查询语言注入、跨站点脚本和其他方法已经成为服务器攻击的普遍方法。

表 5.4：差距和研究活动

确定的差距	研究活动	益处	时限
不足以防御电子邮件和 Web 恶意软件	抵御社会工程（工具、界面、培训）的人为因素分析，强大的白名单	更安全的现在和未来电子商务	近期
规避虚拟机	硬件/软件的 TPM 不足	将虚拟化的可用性延伸为防御策略	近期
难以修复	脆弱的客户端，自动修复	迅速和性价比高的恢复	近期
测试环境不足	互联网规模的仿真	恶意软件传播动态的安全观察，更好的控制策略	近期
攻击者/防御者不对称	多样性，固有可监测系统	攻击者必须对大量平台进行攻击	中/长期
无攻击容错	攻击遏制、安全沙箱、多样性	“亚临床”恶意软件感染时的正确操作	中/长期
检测方法不用于大规模	固有可监测系统、强大的软件白名单、正确软件行为的基于模型的监控	攻击者隐藏活动的空间减少；广义可扩展的检测	中/长期
不能充分理解威胁	攻击者市场的分析、攻击者渗透、观察僵尸网络的同时遏制其破坏	使得防御者占据上风的战略眼光	长期

互联网规模的仿真可以提供恶意软件研究的突破。能够在互联网中观察到恶意软件（特别是僵尸网络和蠕虫）而不将真正的互联网置于危险中有助于识别恶意代码的弱点、其传播方式或对外界刺激的响应。此外，宏观层面上观察到的字符可能给我们检测和响应微观层面恶意软件的线索。高保真的大型仿真是许多下面讨论的举措的一个重要实现能力。

虚拟化和蜜网将在近期和中期提供有价值的保护和检测方法。从多态性和规避技术方面来看，恶意软件越来越具备适应性。后者可以提供防御优势。如果恶意软件检测到在虚拟机或在蜜网环境中，就能够进入休眠状态，则防御者的主动欺骗（使生产系统看起来像虚拟系统和使生产网络看起来像蜜网，反之亦然；十分迅速地改变虚拟和真实系统；甚至在用户未使用计算机时，用模拟的“屏幕保护程序”将计算机从真实状态切换为蜜网状态）

可能是有用的。一般的研究问题是防御者如何能够最好地利用“欺骗”。

这些方法的局限性也引发了担忧。例如，如果用户操作系统中存在缺陷，那么即使正常运行的管理程序也是不够的。此外，高度复杂的恶意软件很可能能够规避现阶段的虚拟环境。改进的硬件架构访问机制将在一定程度上保持这些方法的有效性。然而，需要其他的技术研究来弥补我们计算系统中的战略低地，并将安全功能与其他功能分开。关键点是，我们的检测方法和仪器必须比恶意软件驻留于更低的硬件/软件堆栈。否则，恶意软件就会控制防御者的态势感知，而防御者就没有什么机会了。最近在硬件中植入漏洞的的研究显示了未来的破坏可能性。

协同检测可能涉及独立领域（可能没有建立信任关系）的隐私保护的安全信息共享。我们可以共享恶意软件样本、样本的元数据和经验。活跃恶意软件的数据库可以加快研究进展，但也会引发安全问题，因此必须根据相应的政策严格控制数据库的访问，但是该政策又难以界定。此外，共享恶意软件可能是非法的，这取决于机构的业务。

协同检测支持态势感知。特别是，检测、隔离和修复僵尸网络是恶意软件研究需求和态势感知之间的重要重叠。网络级的防御必须连网，以补充主机级防御。例如，我们需要在运营商层面更好地识别恶意流量。这就是规模和速度的挑战。

脆弱的客户端技术早已被提出。在这个模型中，用户的机器是无状态的，并且所有的文件和应用程序在一些网络上分布(术语“在云中”偶尔使用，虽然也与传统的主框架计算有相似之处)。如果我们可以保证分布式资源的安全，这本身就是一个很大的问题。攻击者对用户资产的攻击选择大大减少，而修复仅仅是重新启动的问题。朝着这个安全云计算模式的长期研究挑战是确保分布式资源库的安全，并允许任何地点的通过身份验证和授权的用户访问资源库。

受感染系统的修复是非常困难的，我们无法断言先前受感染的系统已被彻底修复。特别是，系统可能被 rootkit 感染。这种感染有许多形式，包括用户级到内核级 rootkit。最近，硬件虚拟机（HVM）rootkit 已被提出，它们能够自我加载到现有的操作系统，将系统转化为 rootkit 控制的操作系统[Dai2006]。我们需要完善修复、内置的诊断仪器和 VM 自省（提供嵌入式数字取证以应对威胁）。

遏制技术（包括前面提到的 TPM 方法）是有希望的，但需要进一步的工作。一个有趣的目标是对恶意软件的容错（例如，在可能不受信的系统上安全地执行受信交易）。另一个目标是对关键交易设置“安全沙箱”（相对于目前的沙箱环境，旨在将恶意软件遏制在沙箱中）。最后一个问题是大型系统是否容忍其组件和子系统内正在进行的破坏行为。一般情况下，研究议程应该发现恶意软件是环境的一部分，在存在恶意软件的环境中安全运行是至关重要的。

固有的安全、可监测和可审计系统的开发面临着显著挑战。一般情况下，这是一个中长期研究领域。所有设备的受信路径的短期工作可能会降低风险，例如，降低击键记录软件的风险。在短期内，我们需要完善验证的更新，最终开发免疫恶意软件的系统。

较长期的研究挑战是开发系统、应用程序和协议，它们对而已软件个人的免疫力更强，也更容易以可核查的方式监测（实际上是减少恶意软件在系统中隐藏的空间）。特别是，提供 COTS 计算设备的客观自省和无阻碍控制的基于硬件的仪器不会被恶意软件发现，可以帮助实现嵌入式取证和可审计系统。

人工多样性有多种形式：代码在每个站点是不同的，代码的位置是不同的，系统调用是随机的，或其他数据也被改变。如何将指令集、操作系统以及在不同系统重启时加载的库随机化可能是值得研究的（无论是实用性还是经济学方面）。一个棘手的最终目标是开发功能等同的系统，从攻击的角度来看该系统是唯一的，所以攻击者必须针对各个机器制定攻击策略。人工多样性仅仅是改变攻击者-防御者不对称性的一个方法，我们需要新颖的想法。

我们的威胁分析是不够的。在任何情况下，威胁的性质随时间而改变。一个有趣的研究途径是攻击者市场的经济分析。攻击者出售恶意软件漏洞（被感染机器的网络，或僵尸网络）。价格波动使得我们可以分析攻击者趋势，还可以制定防御有效性的指标。相关的经济方法是使得恶意软件缺乏经济吸引力（例如，通过更好的破坏遏制、提高分布的有效性、限制特定漏洞针对的系统的数量、改变现有法律/政策使刑罚反映网络犯罪的真实社会成本）。

何种研发是更高级的？何种是更基本、更高风险和颠覆性的？

在短期内，我们处在防御性斗争中。研发应在虚拟化和蜜网领域继续。我们需要近期修复上的进步，来解决日益困难的恶意软件清理问题，特别是在最终用户系统中。近期和中期攻击属性研究可以帮助维持必要的互联网治安。共享各类恶意软件攻击数据的机制目前也是缺乏的。研究人员在该领域面临隐私问题、数据共享的法律问题以及数据本身的绝对数量问题。我们需要进行足够的元数据生成和出处研究来克服这些障碍。

捕获和分析恶意软件以及更快的防御技术对于遏制感染来说是必不可少的。长期的研究应集中在固有的安全、可监测和可审计系统。威胁分析和攻击者市场的经济分析应在短期内以试点的形式进行，如果有用则更大力度的进行。

衡量成功的标准

在任何时候，我们都需要受感染机器的基线测量。随着时间的推移和取得成功，这部分的测量将会减少。

一些研究人员目前正在追踪恶意软件的出现。以这种方式，它们能够识别趋势（例如，每月的新恶意软件样本的数量）。恶意软件数量上升趋势的逆转就代表成功。

恶意软件捕获和防御（或者更恰当的是，对存在漏洞的系统实施防御）之间的时间差代表人工和自动化响应时间的进步。

参考资源库，我们可以定义一组必须检测的对象，从而在一定程度上评估有效性。

通过回答下列问题并随着时间的推移跟踪答案，我们可以在一个较高的水平上定义成功的标准：

- 有多少机器被恶意软件感染？
- 新恶意软件出现的速度如何？
- 垃圾邮件是主要的僵尸网络输出，哪一部分的电子邮件是垃圾邮件？

- 业界对恶意软件感染的主机的评估如何？
- 恶意软件严重性的趋势如何（包括骚扰、广告软件间谍软件、僵尸网络）？
- 已知攻击的哪些部分是成功的，哪些部分是挫败的？

我们还可以考虑基于成本的标准 （从防御者的角度来说），例如：

- 搜索恶意软件传播者的成本是多少？
- 识别僵尸网络和它们的 C2 基础设施的成本是多少？
- 增加恶意软件主机列表共享的成本是多少？

攻击者市场的经济分析允许特定防御方法有效性的指标的定义。

拥有可靠的评估特定系统漏洞的指标是很有益的，这些指标还能够评估系统对其他类型的恶意软件攻击（如 DDoS 攻击）的防御能力。同样，建议采用特定恶意软件防御方法或修复策略的指标也是有益的。

测试和评估需要什么？

除了恶意软件的逆向工程，队恶意代码的最有效的研究发生在网络测试平台中。这些测试平台包括简单的“连网”虚拟机，测试平台由数十或数百真实的（非虚拟）节点，如 DETER [DET]，以及在网络模拟工具内创建的模拟网络。研究界已经对互联网规模的模拟环境中的恶意软件进行了研究。目前不存能够打造 10,000,000 或更多节点的仿真环境的基础设施和工具。

随着恶意软件的复杂性的增加，对虚拟环境检测能力的提高，虚拟化环境（例如，虚拟机或蜜网）测试平台面临着挑战。

随着恶意软件的演变，研究恶意软件的工具和环境也要不断完善。特别是，目前安全界并没有基于硬件/固件的恶意软件的测试平台。

充分提升测试环境所需的工具和基础设施都属于研究问题。研究恶意软件的测试平台是针对此应用程序的。即使面临复杂的恶意软件，该试验台也不应该作为测试环境。

安全界需要最新的可靠的恶意软件库来进行研究。目前的恶意软件库是有限的，而且不向研究人员提供。另一种可取的资源是共享蜜网，研究人员可以利用蜜网学习恶意软件的行为。当前蜜网大多由各个独立小组临时运行。然而，法律法规问题抑制了有意义的交流。

互联网规模的仿真允许测试真实的防御和与恶意软件的动态交互。该层面的观察将提供前所未见的蠕虫和僵尸网络传播和运行信息。

我们可以何种程度地测试实际系统？

在真实系统中测试防御效果是可能的。实验可以设想为：真实和仿真网络暴露在具有和不具有特定防御措施的公共网络中。然而，防御措施的快速自动配置和传播必须首先在仿真系统中彻底验证。

参考文献

[Ant2008] A.M. Antonopoulos. Georgia cyberwar overblown. Network World, August 19, 2008 (http://www.pcworld.com/businesscenter/article/150021/georgia_cyberwar_overblown.html).

[CAT2009] Conference for Homeland Security 2009 (CATCH '09), Cybersecurity Applications and Technology, March 3–4, 2009. The IEEE proceedings of this conference include relevant papers on detection and mitigation of botnets, as well as correlation and collaboration in cross-domain attacks, from the University of Michigan and Georgia Tech, as well as Endeavor, HBGary, Milcord, and Sonalyst (among others).

[Dai2006]Dino Dai Zovi, Vitriol: Hardware virtualization rootkits. In Proceedings of the Black Hat USA Conference, 2006.

[DET] Cyber-DEfense Technology Experimental Research laboratory Testbed (DETERlab) (http://www.isi.edu/deter/).

[Fra2007]J. Franklin, V. Paxson, A. Perrig, and S. Savage. An inquiry into the nature and causes of the wealth of Internet miscreants. Proceedings of ACM Computer and Communications Security Conference, pp. 375-388, October 2007.

[GAO2007] CYBERCRIME: Public and Private Entities Face Challenges in Addressing Cyber Threats. Report GAO-07705, U.S. Government Accountability Office, Washington, D.C., July 2007.

[Hal2006]J.A. Halderman and E.W. Felten. Lessons from the Sony CD DRM episode. In

Proceedings of the 15th USENIX Security Symposium, August 2006.

[Hol2008] T. Holz, C. Gorecki, K. Rieck, and F. Freiling. In Proceedings of the 15th Annual Network & Distributed System Security (NDSS) Symposium, February 2008.

[Kim2004] Hyang-Ah Kim and Brad Karp, Autograph: Toward automated, distributed worm signature detection, In Proceedings of the 13th USENIX Security Symposium, August 2004.

[IW2007] L. Greenemeier. Estonian attacks raise concern over cyber 'nuclear winter.' Information Week, May 24, 2007 (http://www.informationweek.com/news/internet/showArticle.jhtml?articleID=199701774).

[LAT2008] J.E. Barnes. Cyber-attack on Defense Department computers raises concerns. Los Angeles Times, November 28, 2008 (http://www.latimes.com/news/nationworld/ iraq/complete/la-na-cyberattack28-2008nov28,0,230046.story).

[Mes2003] Ellen Messmer. Welchia Worm Nails Navy Marine Corps, Network World Fusion, August 19, 2003. (http://pcworld.com/article/112090/welchia_worm_nails_navy_marine_corps.html).

[Pou2003] Kevin Poulsen. Slammer worm crashed Ohio nuke plant network. SecurityFocus, August 19, 2003 (http://www.securityfocus.com/news/6767).

[Sha2004] H. Shacham, M. Page, B. Pfaff, E.-J. Goh, N. Modadugu, and D. Boneh. On the effectiveness of address-space randomization. In Proceedings of the 11th ACM Computer and Communications Security Conference, Washington, D.C., pp. 298-307, 2004.

[Sha2008] M. Sharif, V. Yegneswaran, H. Saidi, P. Porras, and W. Lee. Eureka: A framework for enabling static malware analysis. In Proceedings of the 13th European Symposium on Research in Computer Security (ESORICS), Malaga, Spain, pp. 481-500, October 2008.

[Sch2005] Bruce Schneier. Real story of the rogue rootkit. Wired, November 17, 2005 (http:// www.wired.com/politics/security/commentary/securitymatters/2005/11/69601).

[SRI2009] SRI Cyber-Threat Analytics (http://www.cyber-ta.org/) and Malware Threat Center (http://mtc.sri.com). For example, see analyses of Conficker.

[Thu2008] R. Thurston. Coffee drinkers in peril after espresso overspill attack. SC Magazine, June 20, 2008 (http://www.scmagazineuk.com/coffee-drinkers-in-peril-after-espresso-overspill-attack/article/111458).

[Vir] Virus Total (http://www.virus-total.com).

[Vra+2005] M. Vrable, J. Ma, J. Chen, D. Moore, E. Vandekieft, A. Snoeren, G. Voelker, and S. Savage. Scalability, fidelity and containment in the Potemkin virtual honeyfarm. ACM SIGOPS Operating Systems Review, 39(5):148-162, December 2005 (SOSP '05).