根除复杂的恶意软件

非官方中文译本 · 安天实验室 译注

文 档 信 息			
原 文 名 称	Rooting Out Sophisticated Malware		
原 文 作 者	Information Week	**原 文 发 布 日 期**	2012 年 5 月
作 者 简 介	Information Week（《信息周刊》）是一本在线数字杂志，探讨现实和虚拟事件，总部位于加利佛尼亚的旧金山。 http://en.wikipedia.org/wiki/InformationWeek		
原 文 发 布 单 位	Information Week		
原 文 出 处	http://reports.informationweek.com/abstract/21/8813/Security/strategy-rooting-out-sophisticated-malware.html		
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。

InformationWeek
reports
Reports.InformationWeek.com
2012 年 5 月

根除复杂的恶意软件

由于恶意软件变得越来越复杂,我们用来检测和根除恶意软件(或者,最好是在恶意软件入侵网络系统之前阻断恶意软件)的技术和策略也必须随之越来越复杂。没有一种产品或产品类别可以独立的完成此项工作。相反的，安全专家必须熟悉并善于利用一个技术组合。安全专家也必须善于联接某些表面上看似平淡无奇的事件中的各点来根除麻烦。在本报告中，我们讨论了可减轻上述工作难度的工具，技术和策略。

John H.Sawyer

Presented in conjunction with

SECURITY dark READING
Protect The Business Enable Access

Report ID: S4880512

TABLE OF CONTENTS

关于我们

InformationWeek Reports 的分析师借助定性和定量的研究、业务 技术的评估和规划工具，和源自经验的最佳实践，以真实世界的视角来武装商业技术的抉择者。联络方式：常务总监 **Art Wittmann**awittmann@techweb.com，内容总监 **Lorna Garey** lgarey@techweb.com，特约编辑 **Andrew Conry-Murray** acmurray@techweb.com，研究总编 **Heather Vallis** :hvallis@techweb.com。报告下载地址：reports.informationweek.com。

John H. Sawyer
InformationWeek Reports

John H.Sawyer，John H. Sawyer 是 InGuardians 的高级安全分析师，专门从事 Web，移动业务和网络的渗透测试。他在 IT 企业安全领域的经验包括渗透测试 ,系统和网络强化，入侵分析和数字取证。他曾是佛罗里达大学盖恩斯维尔城的一名高级安全工程师，他是 Dark Reading, Network Computing and InformationWeek 的撰稿人和博主。

John 是 1@stplace 团队的成员。1@stplace 是一小队公益黑客，他们赢得了 2006 年和 2007 年在拉斯维加斯举办的 DEFCON 大会的电子夺旗，计算机黑客竞技赛。他在恶意软件分析 ,黑客攻击和数字取证方面为联邦 ,州和地方执法机构做咨询。他的证书包括 GCIH，GCFA，GCFW，GWAPT 和 CISSP。

EXECUTIVE SUMMARY

每周都有新的恶意软件或僵尸网络威胁企业和家庭用户的新闻。事实上，似乎我们没有一天不会听到有关恶意软件影响同事或家庭成员的计算机，或有关一些僵尸网络造成了世界范围内的破坏得消息。此外，恶意软件越来越复杂。它往往结合了蠕虫，木马和僵尸程序，并且能够自动变形以躲避检测。恶意软件是无处不在的，因为网路犯罪分析购买 point-and-click 型恶意软件攻击包的入门门槛低，更不用说其潜在的丰厚回报。在形势扭转之前，这种情况可能会变得更糟。

在过去的五年里，这成为一种显而易见的痛苦，即传统反病毒产品自身不能跟上新恶意软件的肆虐。杀毒软件厂商将聚类分析和云端强大处理能力做为自己产品的补充，但是他们依旧面临挑战，需要足够快的适应形势以应对当下的威胁。

已出现一个新的产品类别来帮助人们应对未知恶意软件。基于网络的恶意软件检测系统和恶意软件沙箱超越了反病毒供应商提供的传统的基于特征和有限启发的功能。这些系统能通过虚拟机运行可疑文件 ,监控网络、文件系统和进程层的恶意行为。他们的目标是检测和阻止恶意文件进入目标网络。毕竟，如果文件没有到达计算机或服务器，那就不能入侵这些设备。

然而 ,没有任何一个产品(无论多复杂)能检测所有恶意软件 ,它也不能代替一个分层安全系统。一个技术和最佳实践的结合能在检测并在严重漏洞发生之前阻断高级恶意软件攻击的斗争中向企业提供帮助。

找出复杂的恶意软件

恶意软件编写者正在以极快的速度研发新的恶意软件变种。不久前,恶意软件的防御还只意味着辨识一个病毒或一个木马并消除它.但,当今的高级恶意软件被设计为对抗监测和清除。恶意软件编写者还研发出许多新的技术以用于隐藏恶意软件或者使用加密的 HTTPS 流量或通过隧道技术将他的 command-and-control 流量作为标准 HTTP 的一部分以使该软件看起来是良性的。在本报告中，我们讨论了一些方法来辨识高级恶意软件和消除那些攻破你的企业防线的恶意软件的影响。

企业恶意软件防御工作的目标应该是阻止恶意软件不断到达计算机桌面。要做到这一点，需要在网络层进行分析、检测和防御。起始边界、内容过滤网关、下一代防火墙和新的基于网络的恶意软件检测应用程序提供了第一层防御。他们能够分析流量，检测恶意文件和阻止恶意软件不断到达预定目标。当然，值得关注的是这些系统是否能够跟上越来越多的，每天释放的恶意软件样本的数量，以及是否能够有效地应对日益增加的网络吞吐量需求。

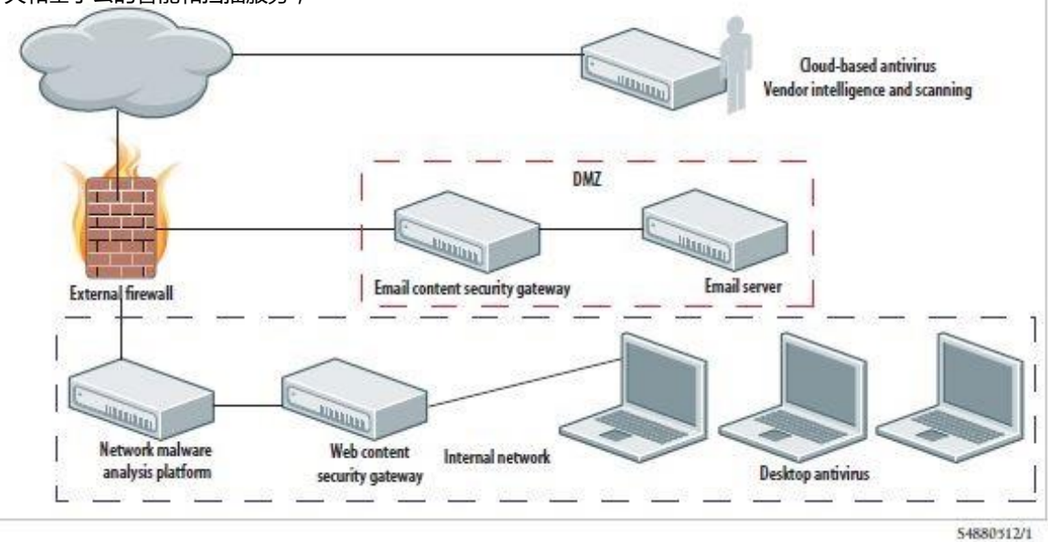
为了扩充基于网络的恶意软件检测产品，许多厂商正在转向基于云的服务来分流分析和计算能力。基于云计算的服务提供更多的算能力，因而能分析更多的恶意软件样本。他们做为一个集中的分析资源提供服务。

虽然我们想要在网络层阻止所有的恶意软件，以使它们永远不会到达桌面系统，但我们知道这是一个不切实际的目标。桌面防病毒依旧是个战场，许多桌面防病毒厂商正在使用与网络检测系统相同的云服务来进行文件比较和信誉查找。

图 1

层次化安全方案

下图是一个层次化的安全方法的例子。它充分利用了桌面防毒软件，网络恶意软件分析设备，内容安全网关和基于云的智能和扫描服务，



无论你正在使用什么技术，传统的最佳做法应该是实施并随后为检测和防御提供最佳机会。这些方法包括应用最小权限原则,积极的面向网络主机的补丁管理和允许浏览互联网的工作站，权限分离，检测操作系统变化的变化管理，监控日志以检测异常事件。

内容检查的困境

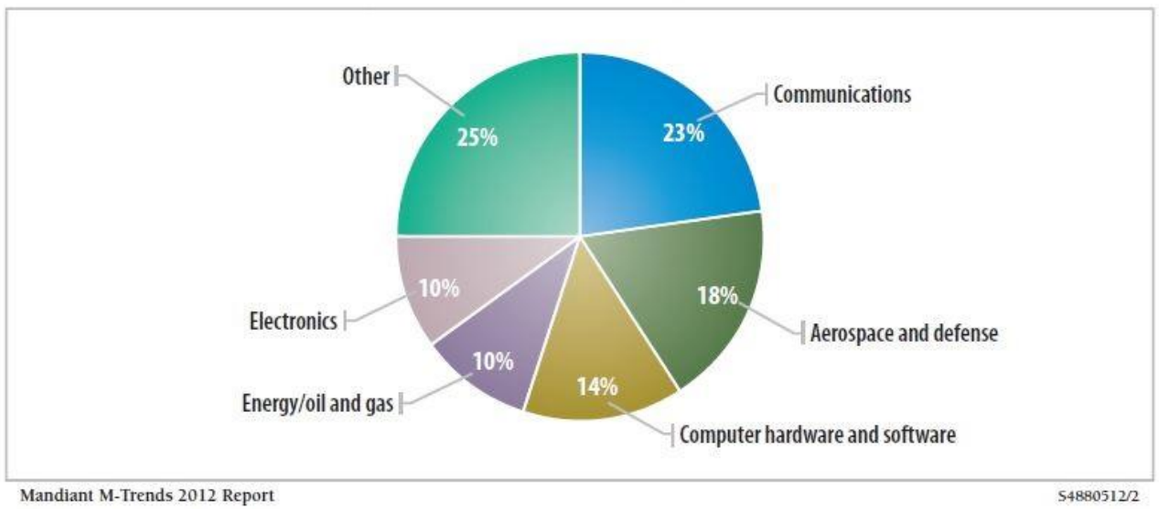
最大的网络安全挑战之一是线速的网络流量内容检查，在网络边界、内容安全网关和下一代防火墙检查传输的网络流量，阻断恶意内容。这些系统传统上依赖基于特征的反病毒方法来检测和阻断已知的恶意文件或网站。

这些产品中使用的杀毒引擎往往是 OEM 系统，并且阻断已知病毒的能力只取决于所包含的病毒特征。新的或有针对性的恶意软件可以轻易的绕过这些设备。为了应对这一形势，厂商正在利用基于云的服务来扩充他们在文件比较和信息查找方面的检测能力。

这样做是有意义的:假设有大量的文件需要被分析,大量的企业网络流量需要被检查。利用通过基于云的情报系统和分析系统获取到的知识来弥补反病毒扫描引擎的弱点。内容安全网关能考察文件来源的信誉，文件的内容和从文件中获取的任何其他信息。这些数据然后可以与在分析其他用户文件的文件过程中搜集到的数据进行比较。

图 2

被高级攻击所针对的行业



下一代防火墙被用来弥补防火墙和内容检测间的空白。他们提供一些与安全网关类似的能力。因为他们是应用感知型的，并了解诸如 HTTP、SMTP 和 FTP 的协议以及诸如即时通信和文件共享的特殊应用流量。

下一代防火墙真正的大好处是可以写入规则来防御特定应用的流量 ,而不是只检测那些基于 IP 地址和端口数的流量。在下一代防火墙上进行如此多的内容检查的缺点是该过程能会响防火墙的核心功能。在流量通过时，对流量进行的分析越多，就越有可能产生影响性能的延迟。然而，即便有这些担忧 ,这些防火墙也正在提供超出传统防火墙的，

策略：威胁情报：什么是真正需要知道的

如果有那么一个时刻，威胁情报能够被自动处理，那就会是一个终结。随着先进的，多维度的威胁的增加，企业不能再孤立的依靠现存的网关工具来清楚邪恶活动。越来越多的企业正在考虑开发一个内部威胁情报系统，花费人力和其他资源来深入检查网络和应用的数据和行为，并将其关连起来。在本报告中，我们将探讨实现一个内部威胁情报系统的驱动力，本问题围绕着人员，成本以及有效实施该工作所需的必要工具展开。

Download

更好的追踪和拦截能力。除此之外， 他们可以利用基于信誉的信息和对已知恶意域名和IP地址的阻断来防止恶意软件进入。很明显，下一代防火墙是有前途的。

内容安全网关和下一代防火墙在边界提供一个初始层面的防护。但是，在对抗复杂恶意软件和针对性攻击方面，他们的能力有限。例如，他们在运行可疑文件过程中，无法提供动态分析以检测恶意行为。这正是新一代基于网络的恶意软件检测设备试图填补的空白之处。

实时动态分析

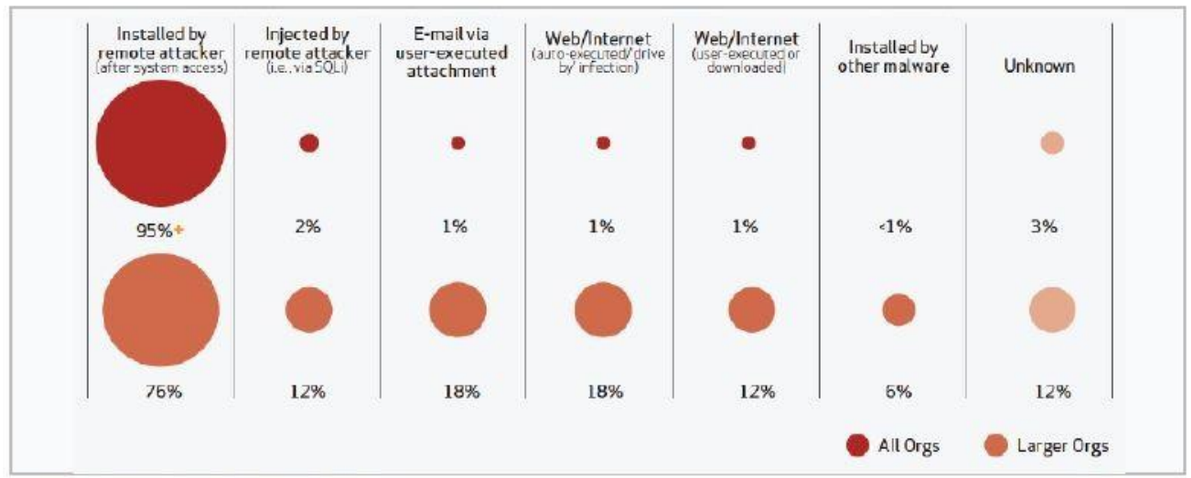
网络恶意软件检测设备（例如，FireEye 和 ValidEdge 的设备）能够通过动态分析可疑文件来判断他们是否是恶意的。所有这些都是在网络层，利用板载虚拟机和仿真技术完成的。设备在虚拟机或仿真器中打开或执行文件，分析文件的行为以判断他们是否是恶意的。然后，该设备决定是否允许该文件通过或产生某种告警。

分析的时候,产品寻找对已知的，恶意的命令和控制服务器的出站连接,对注册表的修改,新服务的创建,对正在运行的进程的代码注入,以及其他行为。一个恶意代码分析师或安全事件应急响应人员在调查一个可能的恶意代码感染事件的时候也会寻找上述同样类型的事物。如果手工完成这个过程，那将是紧张和耗费力的。设备试图使该过程自动化、实时化，从而可以在网络流量通过时迅速做出决策。

网络恶意软件分析设备是从独立的恶意软件沙箱进化来的。在有具体需求的基础上，采用这种独立沙箱来进行分析。这些需求几乎不涉及本地系统或网络。沙箱通常会独立于他们的网络，因为他们是基于 Web 的服务。比较知名的沙箱有 Anubis，GFI SandBox，Joebox，Norman 和 Cuckoo。这些类型的沙箱模拟或完全虚拟一个Windows系统来监测一个可疑文件都对一个系统施加了那些影响。配置的改变（例如修改注册表或额外的新服务），以及试图启动新进程和进行网络连接会被上报。

图 3

恶意软件传播媒介占恶意软件漏洞利用的百分比划分



Verizon Data Breach Investigation Report 2012

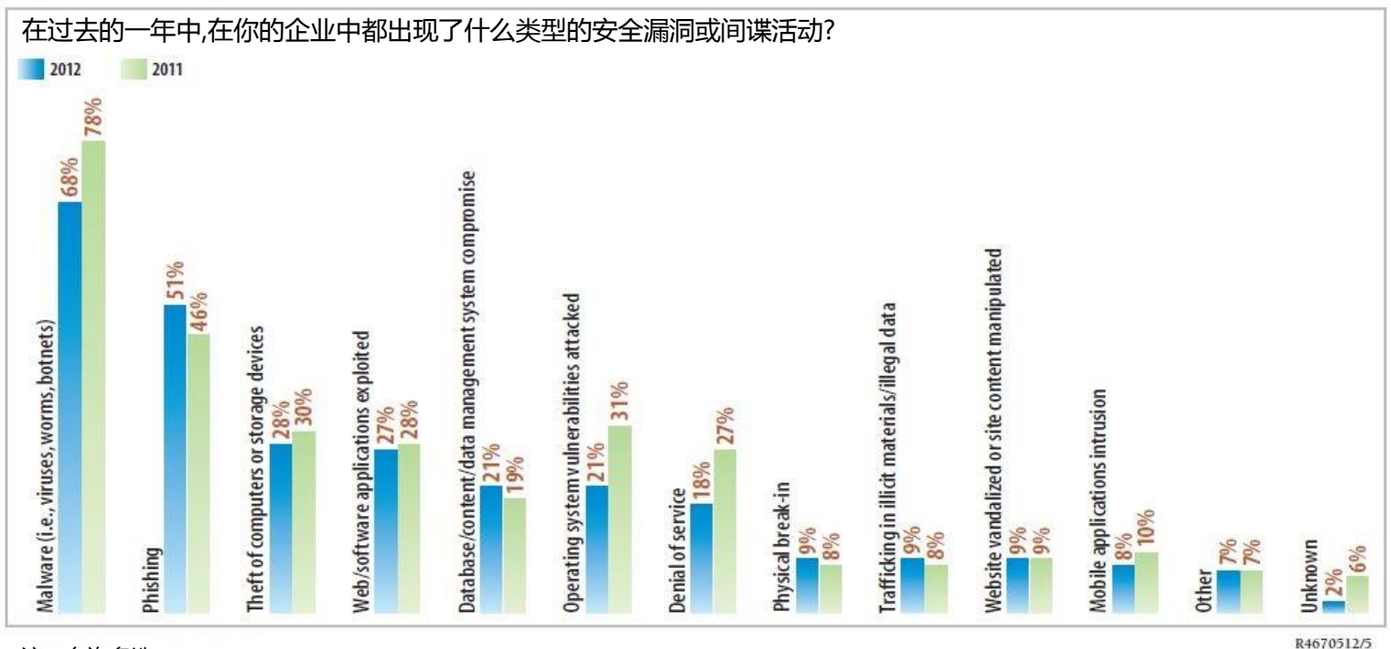
S4880512/3

沙箱的一个最大好处是他们通常都、速度快,能快速提供情报。该情报可被用于构建新的入侵检测系统和防火墙的规则。缺点是他们导致了一个风险，如果沙箱的防护机制被绕过，就会导致一个活性恶意软件在你的企业网络内传播。攻击者意识到了沙箱技术，一直在努力击败该技术，并努力模糊他们的恶意软件的行为以躲避检测。

单独使用自动恶意软件分析系统来监测高级恶意软件攻击既不是一个简单的方法也并不廉价。要进行网络流量实时分析，一个结实的沙箱是必须的，但该沙箱也同样有着一个牢固的价格。有几个性能非常不错的免费或开源沙箱可用(包括 Cuckoo 和

图 4

过去一年中的安全漏洞



注：允许多选
库：2012 年 3 月的 183 位受访者，以及 2011 年 3 月，在过去的一年里经历一个安全漏洞的 219 位受访者
数据：InformationWeek Strategic Security Survey，针对拥有 100 名以上雇员的企业中的业务技术专家和安全专家的进行调查

Zero Wine），但是他们的易用性和配置的复杂性差别很大。此外，某些企业可能害怕提交他们环境中的文件，因为这可能会泄露他们是一个针对性恶意软件攻击的受害者。

手工分析的痛苦

基于网络的恶意软件检测和沙箱可以很好的自动动态分析疑似恶意软件，但是他们并不否定对人工分析的需求。将会有这样的案例，即自动分析技术跟本无法充分的分析特定类型的恶意软件片断。更糟糕的是，恶意软件分析是一个漫长的、烦琐的过程。该过程涉及到的专业技能有对可疑文件的逆向工程，确定其特性和功能，通过在一个真实系统中运行可疑文件来进行动态分析，并监控对系统所作的改变。

企业恶意软件防御的目标是阻止恶意软件到达桌面。

逆向工程可能包括使用 Ida Pro 反汇编程序反汇编恶意代码二进制文件,通过 debugger 来进行运行分析，以及使用一些新的，针对恶意恶意代码的逆向工程工具。这些工具包括 HBGary Responder 和 AccessData 的新 Cerberus 恶意软件分类工具。该工具帮助实现逆向工程和未知文件分类的部分自动化。他们了解恶意软件的常见属性是什么，能够基于恶意软件的内部功能来帮助辨识恶意软件。所有这些信息被用于开发一个针对恶意软件的描述，以便在一旦恶意软件进入系统时阻断或监测到它。

当处置一个针对性攻击时，关键是要了解攻击者使用的恶意软件的能力，包括它的传播方法；一旦感染系统，是如何继续留存在系统中的；它的目的和它可能使用的，与攻击者交互的任何通讯通道。对恶意软件进行一个准确的特征描述是很关键的，从而能够确定整个企业中已经被入侵的系统。特征描述中的属性（通常被称为攻陷指示器）包括进程、文件名、注册表条目、事件日志、网络流量和可以唯一标识出一个恶意软件片断的任何其他信息比特。该特征描述可以通过多种方法获得，包括 sandbox 分析、动态分析和对已知受感染系统的取证分析。

当然，这其中的关键是尽可能的精确的描述特征。了解恶意软件是如何传播的能有助于辨别有可能被感染的系统。可以通过补丁管理系统和漏洞扫描器来对该信息进行相互对照。任何关于数据泄漏或恶意软件用于与攻击者通信的网络流量的信息也都是有用的。可以设置新的 IDS 和防火墙规则来检测和阻断该通信。监控 DNS 查询和已知恶意域名的假 DNS 入口的插入能够有助于检测和防御。

找出被入侵的系统

在过去的几年中，我们已经看到新的企业级应急响应工具的出现，包括 AccessData Enterprise，Carbon Black，F-Response Enterprise，Encase Enterprise 和 Mandiant Intelligent Response。这些产品的功能各不相同，但是每一个产品的目标都是使应急响应和企业安全专家能够通过桌面上的 agent 或集中收集的数据来大规模的执行应急响应程序。

这是创建一个恶意软件特征描述变得非常重要的原因所在。因为这些来自恶意软件的属性能够被用来在很多系统或日志中进行搜索以确定哪些机器已经被入侵。他们是很强大的，他们的功能包括内存分析，远程磁盘镜像和远程取证分析。如果恶意软件分析显示某些文件或服务是在一个被攻陷的系统上创建的，这些攻击能够使安全专家快速的搜索企业中的所有计算机，以确定其他系统上是否存在被破坏的文件或服务。

在街头进行斗争

即便恶意软件的编写者使用新的和更巧妙的技术来掩盖他们入侵系统的痕迹，依旧有这样一个简单的事实，即大多数恶意软件想要具有持久性。一些恶意软件被设计为一个下载器，唯一目的是使其到达目标系统并下载其他恶意组件。然而下载器是临时的，并服务于一个单一目的的。他们下载下来的组件将寻求在目标系统中持久的留存，以便进行其邪恶活动。当恶意软件居留于系统中，并将自身设定为重起其所生存的系统的时候，它会因改变受害者的计算机系统而暴露自己。

即便恶意软件的编写者使用新的更巧妙的技术来掩盖入侵系统的痕迹，依旧有这样一个简单的事实，即大多数恶意软件想要具有持续性。

我们怎么知道要寻找什么。我们已经探讨了入侵指示器，企业级事件响应工具使用其描绘和检测恶意软件。但是传统的实践方法，包括变化管理，日志监控和最小权限原则也能在恶意软件防御战中起到效果。

Verizon 的 2012 Data Breach Investigation Report 指出，Verizon 调查的漏洞中有 84%可以在受害者企业监控日志的过程中被识别到。那些握有证据（帮助 Verizon 确定在漏洞攻击过程中都发生了什么）的日志文件与受害者利用监控捕获入侵时所使用的日志是同一个。依据报告，有用的入侵指示器包括日志文件的行数，日志文件的行长度，流量类型中的峰值，IP 连接的起源和电子邮件信息的发送/接受。

不幸的是，对于很多企业来说，日志记录似乎是一个艰巨的任务，他们考虑到在那里的每一个操作系统，网络设备和服务都在产生日志。集中日志和进行基本分析以寻找之前所提到的那些异常并不会花费太多的时间、精力和金钱。Verizon 的报告说到："有关此类监控的真正有趣的事情是，不需要花费大量的现金来实施一个有效的解决方案。可以利用几个 Linux 或 Windows 系统的命令来完成它。"

普通观点认为，集中式日志需要昂贵的企业日志记录平台，该平台带有专门的 Web 界面以及底层的机密数据相关性。然而，与此相反的，存在很多低成本的和免费的选择。他们可以使企业开始收集当下的日志数据，并集中处理和分析它们以寻找恶意软件活动。例如，所有反病毒产品都创建日志，通常这些日志就在 Windows 事件日志中。可以使用免费的日志工具来集中这些日志，并使用命令行工具或自动化方法很方便的对其进行搜索。

配置管理数据和变更管理监控工具可以被用来检测新的，被创建来允许恶意软件持久驻留的服务。一些变更管理工具有能力执行文件完整性检查。正常补丁修补时间之外的 Windows 系统目录中的新文件或文件的更改可能预示恶意软件正试图在系统上建立一个永久的驻足点。

异常网络行为与之前不可见的网络通信是另一个应用现有监控工具的领域，当然这是假设有 netflow 功能的路由器，防火墙和入侵检测系统已经就位。这些设备进行记录日志，并经常登陆到中央服务器，但是他们的日志经常无人察看。那些工具（Tenable Security Center）可以使安全专家能够将这些信息第一时间与可辨识的，提供网络服务的主机关联起来，并与已知恶意代码服务器和恶意域名通信的主机，网络流量的峰值，新网络协议等预示一个攻击的所有潜在信号关联起来。

MORE LIKE THIS

更多资料

InformationWeek 今年发表了至少 150 份报告，他们对注册用户是免费的。我们将通过提供来自于 IT 专业人士的分析和建议，来帮助你筛选供应商的宣传，评估 IT 项目和建设新的系统。在我们的网站上，你会发现：

策略：如何通过 FFIEC 的合规性来提高安全性：只需一个智能手机，用户就可以在任何时间进行几乎所有的银行业务。然而，这所有的灵活性和便利性开辟了欺诈和网路犯罪的新途径。FFIEC 几年前布局的指南先于当下出现的很多能力和漏洞。在本报告中，我们研究了最新的指南，就应该如何扩展工作以使其符合 FFIEC 指南从而加强企业的整体安全态势，保证用户和用户数据安全给出了建议。

研究：2012 战略安全调查：当提及到安全和风险管理，试图去解决一切是很诱人的。一个更有效的方法：专注于最有可能的威胁。我们的调查结果显示安全和 IT 专家正全神贯注于他们拥有一定控制力的风险上，例如，实施更好的访问控制，审核云服务供应商，培训移动设备安全防护，用户和构建更安全的软件。看看还有什么应该是在你的名单上。

策略：监控和衡量云服务厂商表现：没有忽略云，这意味着 IT 专家必须寻找一个监控和衡量云服务供应商表现的方法。正如安全团队以一个管理的角色经常与公司内的安全管理作斗争那样，我们与不再位于我们自己的数据中心中的资产的安全管理做斗争。当前的挑战是为云产品开发和实施一个强壮的管理模型，该模型确保安全是对话的一部分。

其他: 署名报告，例如信息周刊薪酬调查、信息周刊 500 和年度国家安全报告，国家全面安全问题等。