

不断进化的端点恶意软件检测：对抗高级的、有针对性的攻击

非官方中文译本 · 安天实验室 译注

文档信息			
原文名称	Evolving Endpoint Malware Detection: Dealing with Advanced and Targeted Attacks		
原文作者	Securosis	原文发布日期	2012 年 7 月 12 日
作者简介	Securosis 是一家独立的研究和分析公司，致力于思维的领导性、客观性和透明性。我们的分析师都拥有经理职位，并致力于为客户提供高价值的，务实的咨询服务。 -- 参见本文的“关于 Securosis”部分。		
原文发布单位	Securosis		
原文出处	https://securosis.com/assets/library/reports/Securosis_Evolving-Endpoint-Malware-Detection_FINAL.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	<p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p>		



不断进化的端点恶意软件检测： 对抗高级的、有针对性的攻击

版本 1.3

发布：2012 年 7 月 12 日

Securosis, L.L.C. 515 E. Carefree Highway Suite #766 Phoenix, AZ 85085 T 602-412-3051

info@securosis.com

www.securosis.com

作者注：

本报告的内容与任何厂商无关。报告内容基于 [Securosis 博客](#)发布的资料，并对其进行了增补，审核以及专业的编辑。

特别感谢 Chris Pepper 在编辑和内容方面的支持。

Trusteer 许可



总部位于波士顿的 Trusteer 是端点网络犯罪防御解决方案的主流供应商。此类解决方案协助企业对抗金融欺诈和数据泄漏。数百个企业和数以万计的终端用户依仗 Trusteer 来防护他们的计算机和移动设备，以远离那些对传统安全解决方案

不可见的网络威胁。Trusteer 的 Cybercrime Prevention Architecture 将多层安全软件与实时威胁智能感知系统（real-time threat intelligence）相结合，实现对恶意软件和钓鱼攻击的持续防护，并满足法律法规遵从性需求。全球性企业，例如 HSBC、Santander、The Royal Bank of Scotland、SunTrust 和 Fifth Third，都采用了 Trusteer 的解决方案。网络银行的主流供应商，例如 First Data、Harland Financial Solutions、Intuit 和 S1，通过整合 Trusteer 来为各种规模的金融机构提供世界级防护。www.trusteer.com

版权

本报告采用共享创意署名—非商业性—禁止衍生 3.0（Creative Commons Attribution–Noncommercial–No Derivative Works 3.0）许可协议进行许可。



<http://creativecommons.org/licenses/by-nc-nd/3.0/us/>

目录

失控	3
行为信标	5
提供上下文背景	9
控制	12
衡量和折中	15
总结	18
关于分析师	19
关于 Securosis	20

失控

随着所有安全专家意识到恶意软件的重要性，我们已经开始注重对恶意软件的发展以及新兴的，对抗恶意软件的控制手段的研究。我们在几年前就已经开始编写[端点安全基础](#)，近期开始关注[基于网络的，于边界检测恶意软件的方法](#)。最后，我们承担了艰巨的任务来剖析在确认病毒感染时涉及到的过程，分析恶意软件，并通过[恶意软件定量分析](#)追踪它的扩散。

因为你不过是一个小小的安全分析师，你的头脑中已经被灌输了分层防御的重要性。没有什么控制措施是足够的。尽可能多的堆积免费的控制软件（不完全影响用户体验），会迫使攻击者转战其他地方去寻求易实现的目标。无论号称有多好的防御措施，现实是，随着当下端点的移动性，我们需要持续的对端点进行防护，因为我们通常不能控制那些端点的位置或它们使用的网络。显然，没人会完全相信当前的端点防护手段的防御效果很好。因此，是到了评估它如何能更好地工作的时候了。本文将此类评估。但是，在我们换掉现存的端点安全控制手段之前，先让我们看看我们不断变化的需求。

失控

敏感的企业数据变得前所未有的易于访问。PC、智能手机和云服务（Salesforce.com、Jive、Dropbox 等等）之间被设计成有助于协作的模式，你不能假定任何设备（甚至是那些你自己拥有和控制的）没有在访问关键信息。试想一下，你的个人工作环境在过去的几年里是如何改变的。你将数据存储在云中的某处。你通过各类设备访问企业数据。你通过各种网络（有些是来自朋友或当地咖啡馆）来上网。

我们曾经一度控制了我们的计算机环境，但是现今不再如此。今天，你不能假设任何事情

我们曾经一度控制了我们的计算机环境，但是现今不再如此。今天，你不能假设任何事情。设备可能是属于雇员。你的 CFO 的孩子可以用他父亲的公司笔记本访问互联网的任何地方。人们通过酒店和其他公共网络来上网，你并不知道在那些网络中都潜伏着什么。显然，你不能就这么放弃，并忘记控制你的内部网络。但是，你知道你的边界防御措施（以及他们设想的出口过滤和内容分析）有时会被简单的绕过。

单单缺乏对基础设施的控制并不足以令人不安。你还需要考虑用户因素。存在一种很不好的倾向，那就是员工喜欢点击任何看起来有趣的东西。胡乱的点击开启了员工与各种有害东西之间的通道，将感染源带回你企业环境，并使你的数据处于危险之中。因此，我们需要尽可能的加固端点并做最坏的假设。

不断进化的对手

攻击者使事情变得更困难。今天，专业的恶意软件编写者已经走在这些趋势的前面。他们利用先进的恶意软件（远程访问木马[RATs]和其他商业恶意软件技术）击败了传统的端点防御措施。由于多态机制、恶意软件释放器（droppers），以及模糊代码等技术，传统的文件匹配方式（在端点，邮件和 web 网关）不再能有效检测这些攻击。这已经是公认的事实。

厂商用通用术语“零日”来定义以前没见过的恶意软件，但是可悲的是，我们还没有看到已经正式发布的，任何重要的东西。它对我们来说是全新的。

更严重的是，你不能期望在一个攻击对你发起进攻以前看到它。无论它是一个迅速变形恶意软件攻击还是一个有针对性的尝试，以前通用的样本采集过程（蜜网，WildList 等等）都对此无效，因为这些恶意软件文件是独一无二的，针对一个目标定制的。厂商用通用术语“零日”来定义你以前没见过的恶意软件。但可悲的是，你还没有见到已经正式发布的，任何重要的东西。

当我们称他们为专业的恶意软件编写者时，我们并不是在开玩笑。这些人现在正采取一个敏捷开发方法来构建他们的攻击。他们拥有工具，能够开发和测试他们的恶意软件的效果，并能确定现有的恶意软件防护工具是否能够检测到他们的攻击。

即便有信誉系统和其他机制来检测这些高级攻击，当下的“解决方案”也是远远不够的。这意味着安全从业人员需要采取新的策略来检测和阻断针对他们的用户的恶意软件。

不断进化的端点恶意软件检测

好消息是，端点安全厂商认识到他们的传统防御方法可能会像以前的渡渡鸟一样灭绝。他们已经在改进方法——推出的产品已经大大减少了对设备计算资源的占用，并且其产品通常擅长检测简单的攻击。但是，正如我们之前描述的那样，简单的攻击并不是需要担心的那一个。因此我们将探讨端点防护手段是如何演化发展的，以便能更好检测并希望阻止当前的这一波攻击。

我们将以辨别一个恶意软件攻击的行为信标作为论述的开始。就像一个扑克选手，每一次攻击包括了他自身的“通知”，这会使你意识到正在发生的，不好的事情。然后，我们将描述一些其他的数据资源。在确定一些可疑行为是否有害时，这些数据资源能够提供其所需的背景情况。我们将评估一系列不同的控制手段。这些手段能够在攻击链条的不同环节上阻止攻击。最终，我们将以一个坦诚的讨论来收尾。它是一个关于在对抗高级恶意软件过程中的权衡和妥协的讨论。你可以停止这些攻击，但是治疗可能比疾病本身更糟糕。我们将为你提供如何在检测、响应和用户影响之间寻找平衡点的建议。

行为信标

攻击者持续推进他们的攻击策略。高级攻击者很少使用同样的文件或恶意软件传播媒介两次，并且攻击者不断地对恶意软件文件进行变形。这使它很难被那些采用基本的、基于文件的检测手段的传统反恶意软件工具检测到。所以，对检测恶意软件的检测工作不再完全专著于恶意软件看起来像什么（一个文件哈希或一些其它的识别因素），必须纳入一些新的数据资源以供判定所需。

业界已经进行了巨大的研究投入以分析预示着攻击的行为的类型，构建检测工具以实时寻找那些类型的行为信标。

这些新资源包括，它做什么，它是如何到那里的，谁发送的它；结合传统的文件分析，这一更广泛的数据基础提高了你的精度并减少了误报。不，我们认为传统反病毒（特征匹配）不再拥有一席之地。首先，合规性强制执行 AV，所以，除非你是不受管制监督的少数的幸运者之一，你别无选择。但是，更务实的说，并不是所有的攻击者都是“高级”的。寻找薄弱防御路径的攻击者使用已知恶意软件工具包，利用已知恶意文件。没有理由让一个可识别的恶意文件在你的设备上运行（当然并不只是为了确认它是恶意的）。在这种情况下，AV 是有用的。但需要明确的是，如果恶意软件工具包生成多态文件，那么现有的恶意软件引擎存在一个盲点。

但是，很明显，旧的、检测恶意软件的策略不善于应对高级和针对性攻击。这些额外的数据资源提供了额外的信息，以帮助更精确的分辨好的和恶意的代码。最有前途的是行为分析。好消息是，业内已经进行了巨大的研究投入以分析预示着攻击的行为的类型，构建检测工具以便在设备执行代码的时候，实时寻找那些类型的行为信标。

行为分析

当我们说“恶意软件特征”时，我们正在谈论是什么呢？那取决于你正在试图完成什么。特征的一个用例是在深度[恶意软件定量分析](#)中的恶意软件分析描述。在这种情况下，我们的目标是去了解恶意软件是什么，详细了解恶意软件会做什么。你能使用这些特征来发现已经被攻陷的其他设备。

另一个用例是利用典型恶意软件行为的特征，在设备受感染前，检测设备上的攻击。这一切都是为了搞清楚恶意软件做了什么，以及什么时候会做，从而利用那些信息，在恶意软件造成损害以前阻止它。有几个东西是对检测有用的：

- 注册表设置
- 进程/服务
- 注入代码
- 新的可执行文件
- 域/协议
- 网络通信目标 (C&C)

Mandiant 的词条，[入侵信标](#)，总结的非常好。如果恶意软件在一个标准操作系统文件（例如，Windows 的 winlogon.exe 或 services.exe）中注入恶意代码，在 Windows 设备中添加某些注册表项以确保持续性，连接已知会散布恶意代码的外部服务器，甚至是使用一个不透明的加密协议（大概是指令和控制流量），你就拥有了有力的证据来确定该可执行文件是恶意的，你需要阻止他。

有限的死亡方式

如果你能捕获一个恶意软件的样本，通过运行它来对其进行静态分析和动态分析，以弄清楚该样本是做什么的，由此得到的恶意软件特征是非常有用的。但是如果你不能获得恶意软件，那么会发生什么呢？你是不是只能等待，直到设备拥有一个特征？这听起来更像是一个被动的办法。这个被业界依赖多年的方法会产生灾难性的影响。

你需要一个具有共性的，能够标识恶意活动的行为清单。你可以将这个清单用于一个早期预警系统，以应对可能的攻击。当然，纯粹的依赖此类特殊行为可能会导致误报。因为代码注入和更改注册表设置可能是合法活动（例如，在打补丁的时候）。你在多年前使用主机入侵防护技术（host intrusion prevention technologies, HIPS）时，可能已经受到了沉重的教训。所以你需要将行为信标用于初级预警，然后对其进行额外的分析以辨别你是否真的正在遭受攻击。

但是如果你不能获得恶意软件，那么会发生什么呢？你是不是只能等待，直到设备拥有一个特征？这听起来更像是一个被动的办法。这个被业界依赖多年的方法会产生灾难性的影响。

该过程近似于从你的 SIEM 接收告警。你不能假设一个 SIEM 告警就意味着一个攻击。但是，这意味一个调查的开始。一个熟练的分析人员像在 [Network Security Operations Quant](#) 中所述的那样，检查该告警，然后或确认或排除攻击。那么，分析人员是如何确认这是否是一个攻击呢？他们通过他们的经验来了解产生该告警的背景。

但是，你不可能在一个典型端点或服务器设备上安排一个熟练的手工分析师来费力的处理所有的潜在告警。所以，你需要一个工具。该工具能够联系足够的上下文，以确定这是否是一个攻击，确定是应该阻止还是应该放行。

典型行为信标

当我们探讨典型的，能够代表恶意代码的行为信标的时候，这些信标一般可以分为两个集合：一个集合是那些代表着攻击中，攻陷的行为，另一个集合是那些代表着窃取数据时，建立恶意软件的行为。

第一集合中的信标被传统的端点防护广泛的应用于“行为启发”以及预防攻击。

- **内存崩溃/注入/缓冲区溢出:** 旧的，衡量设备被入侵的标准是“通过向程序提交特制的输入来改变该程序的执行流程”。这不是我们自己下的定义。它来自于 [Haroon Meer 2010 的论文\(PDF\)](#)。该论文论述了内存攻击的历史。如果你不熟悉这个攻击要素，该论文给你提供了大量的资料。它足以说明内存崩溃这种方式是存在而有效的，任何行为检测方法都必须留意这些攻击。
- **系统文件/配置/注册表改变:** 正常的可执行文件很少更新注册表、配置或系统文件设置。所以，任何此类的行为都需要调查。
- **释放器 (Droppers) 和安装代码:** 恶意软件的编写者需要比以往更快速的更新他们的攻击。因此，对于他们说，更有效的方式是植入一个被称为 dropper 的存根程序 (stub program)。该 dropper 访问网络，下载最新的恶意软件文件到被攻陷的设备上。因此一个行为像 dropper 的可执行文件需要被阻止。你也应该对那些通过注入代码 (或理所当然的做其它动态变换) 来加入或改变可执行文件的程序秉持怀疑态度。
- **关闭现存的保护:** 一个会关闭标准安全控制措施的程序(例如 ,反病毒 agent ,使用者账户控制(User Account Control)) 很可能是恶意的。因此，这些是很有效的恶意软件信标。
- **身份和权限操做:** 创建本地帐户、权限提升等行为通常都预示着恶意软件正在获取设备更进一步的控制权或攻击网络上的其他设备。

另一个集合中的信标倾向于，已立足的恶意软件利用此类行为来试图窃取数据或进一步在环境中扩散。

- **父/子进程不一致:** 一些进程和可执行文件总是由特定的进程和可执行文件来启动的。违反这些关系的东西可能意味着恶意软件。
- **伪装成补丁:** 近期的 Flame 恶意软件表现得很明显，攻击者正扮演成更新以掩盖他们的行为。这很难被探测。因为补丁被认为会更改文件，注入代码，更新配置文件和注册表的设置。
- **键盘记录器:** 少数情况下，键盘记录器实际上是一个合法的程序。但是，我们将其认作万分之一的特例，并单纯的认为一个键盘记录行为或任何其他拦截设备驱动命令的技术通常预示着恶意。
- **屏幕截图:** 为了应对用户使用软键盘来代替键盘输入，攻击者也在用户点击的时候截屏，以探测被用户选定的字符。这很繁琐，但是许多攻击者的人力成本低（例如 hacker boiler rooms），因此它是有经济效益的。在不恰当的时候进行的屏幕抓取（例如，在登陆银行站点的时候）是绝对需要被注意的。

当然，这些行为中的一些行为在特定的场景下是合法的。因此，我们再次强调，在决定是阻止还是放行的时候，上下文背景的重要性。

提供背景

对当前的高级恶意软件的检测，不仅仅是需要将文件看作典型的 AV，我们还需要利用行为信标。为使事情更有趣，可疑的行为在特定场景下可以是合法的。因此，为了精确和有效的检测，你需要更好联系上下文背景，例如代码是做什么的，它从哪里来，它来自于谁，以便就是否允许或阻止其执行，达成一个合理的判断。

当你没有这方面的背景的时候，会发生什么？让我们进入时空机器，回溯到主机入侵防护的(HIPS)的早期。HIPS 类产品在设备上运行，扫描预示着恶意软件的攻击特征和行为。在没有足够的上下文背景的情况下，这些控制手段阻止了各类事件（包括很多的误报）并通常对业务造成了很大的破坏。对于那些真正需要设备能够启动和运行的企业来说，即使付出了一定的安全成本，这些手段也没能取得很好的效果。

但是，监控攻击的概念是个立方体。它是一个实现的问题。如今，额外的上下文背景减少了误报，增加了准确性，减少了对运营的干扰—所有有价值的目标，一个控制手段管理新攻击向量时所追求的所有有价值的目标。因此，我们深入剖析一些超越行为信标的数据资源，以帮助辨别恶意的东西。

HIPS 类产品在设备上运行，扫描预示着恶意软件的攻击特征和行为。在没有足够的上下文背景的情况下，这些控制手段阻止了各类事件（包括很多的误报）并对业务造成了很大的破坏。

从何处：Dropper

我们已经提到，恶意软件编写者利用 droppers 来实现在一个设备上的立足，然后下载当前的和/或附加的攻击，而不是试图将整个恶意软件放到设备上以作为初始攻击阶段的一部分。当然，droppers 是恶意软件，而不是其他任何东西。但是他们更频繁的变身，这使得初始检测变得很困难。正如我们在[恶意软件量化分析 \(Malware Analysis Quant \)](#)中所描述的那样，唯一比被感染糟糕的事情是被已知恶意软件重复感染。

因此，对恶意软件 droppers 的剖析使你在你的场景中搜索这些文件。通过跟踪 droppers 的踪迹，你能识别那些已经被攻陷的，但是还没有被激活的设备。其中的关键是对“哪个文件在哪台设备”的数据的分析。当一个文件被发现是恶意的，如果你有数据并及时进行分析，很容易就能确定哪个设备被安装了恶意文件。

当然，这依旧是被动的。但是 dropper（或类似已知恶意文件）的存在，结合任何其他不良行为，是确认一个机器被攻陷的相当确凿的证据。对 droppers 的追溯足以将你指向恶意软件的起始点，消除任何痕迹，并且你能防止重复感染。

你正在做什么（以及为什么这样做）？

一些明显的活动使“sniff test”没能区分什么是正确和错误的。恶意软件的编写者已经将他们的恶意意图掩盖在那些似乎是可接受的功能之中。例如：

- **浏览器插件**：允许插件（例如，Skype）在标准网页中高亮显示电话号码，以使用户很容易的点击并自动拨号。这很酷。但是，如果同样的技术被用于高亮显示有趣的文本，以使毫无怀疑的最终用户来点击链接，并被偷渡式下载感染的时候，会发什么？
- **更改应用程序功能**：攻击者在高级恶意软件中使用的一个常见技术是将功能添加到一个应用中。所以，分析每个应用的常见活动，然后寻找该分析的行为边界，是很重要的。这类似于白名单的方式，其区别是，相对于白名单跟踪可执行文件来说，你跟踪的是应用的行为。

当然，很难去收集对每一个用户使用的应用所作的分析的上下文背景，然后跟踪他正在那个应用中做着什么，进而判断它是否是合法的。但是这种分析是必须的，以便检测我们每天面对的高级攻击。

何时：攻击时间

只评估设备上运行的代码是不足够的。关于“何时”的上下文背景也很重要。例如，让我们以抓屏来比喻说明时间对于建立上下文背景的重要性。每一个操作系统都有捕捉屏幕的能力，因此抓屏并不会引发告警。但是，如果抓屏是发生在用户正敲击一个虚拟软件盘，登陆他们的银行账户的时候呢？或者，如果发生在他们正在登陆进他们的 VDI（虚拟桌面）的界面的时候呢？是的，这可能是不妙的。但是，如果它发生在用户正在浏览一个新闻站点的时候，这可能是没什么问题的。话说回来，你不可能总是对的（因为新闻站点也可能被攻陷），但通过额外的数据来提供上下文背景，可以最小化你可能错过什么东西的可能性。

信誉最初被用于增加反垃圾邮件装置的效率。现在信誉已经成为每一个厂商威胁情报提供工作的一个基本方面。

是谁：信誉

其他可用于检测高级恶意软件的有用资源是文件的信誉，发送者，或 IP 地址。信誉最初被用于增加反垃圾邮件装置的效率。现在信誉已经成为每一个厂商威胁情报提供工作的一个基本方面。大的安全厂商能够从安装他们产品的亿万端点和设备中获得大量的数据。他们对这些数据进行挖掘以确定哪些文件、设备和网络地址有可能会作坏事。

这些都是不精确的科学——尤其是考虑到变形一个文件，欺骗 IP 地址，或伪造设备指纹的简单性。我们必须假设高级的对手伪装成无辜的事物，以使他们的意图让人迷惑。你不能让你的恶意软件/清除判定严格依赖于信誉。但是，你可以在分析可能的攻击的时候，将它作为额外上下文背景的支撑数据源。

当然，恶意软件编写者不会轻易让你弄懂他们正在做什么。你的最好办法是收集尽可能多的数据，分析在设备中正在发生什么（行为分析），并结合来自外部资源的数据来判断正在你设备上运行的、代码的本质和意图。这至少会给你一个抗击攻击的机会。到目前为止，我们一直专注于分析和检测。但是，如果没有一个机制来真正阻止被检测到的攻击，检测是没有用处的。

控制

让我们将关于检测高级恶意代码的讨论转入下一个层面：利用我们已经搜集到的信息作一些事情。我们需要制定一个评判某个东西是否是恶意软件的标准。如果是，那么就阻止他。此处，你需要权衡不同的控制手段，并为你的环境选择最好的一种。

恶意软件检测 Cocktail

让我们乘坐时空机穿梭到垃圾邮件检测的黄金时期。垃圾邮件发送者得到了不错的发展，他们发展他们的技术以绕过每一种邮件安全人员使用的新防御手段。在 3 到 4 年里，大约 2004 至 2005 左右，安全厂商使用了 15 到 20 种不同的策略来确定一封特殊邮件是否是不清白的。听起来很熟悉？恶意软件检测已达到了一个相似点。大多数技术都不是万无一失，没有严重的误报后果的。

从反垃圾邮件厂商的发展中，我们能学到什么？你能达到并保持一段时间的效果是有限的。除了这一事实，你还学到了什么？处置一系列不同检测技术的最好方式是使用一种 Cocktail 方法。这涉及到给每种技术打分（可能不是很精确），然后将其输入一个为每一种技术分配恰当权重的算法，并确定一个标明是恶意事件的阈值。显然，这个秘密武器在算法里，是由安全厂商负责的。

是的，这种很多都是发生（并应保持）在后台，你不会有能力去配置这个算法或者 Cocktail。但是我们正在试图阐述这一过程是如何工作的，以便使你可以聪明的评估那些新的，宣称能够检测高级恶意软件的设备和产品。

但是，我们知道你不可能每次都做对。所以，是时候将我们的研究应用于事件响应和取证上面了，包括[事件响应基础 \(Incident Response Fundamentals\)](#)，[更好、更快的应对 \(React Faster and Better\)](#)，和[网络安全分析 \(Network Security Analysis\)](#)，以确保你为必然的失败（即便使用最好的恶意软件检测手段）做好了准备。

让我们看看组件和控制手段。你将依赖这些手段来阻断检测到的攻击。

处置一系列不同检测技术的最好方式是使用一种 *Cocktail* 方法。这涉及到给每种技术打分（可能不是很精确），然后将其输入一个为每一种技术分配恰当权重的算法，并确定一个标明是恶意事件的阈值。

传统端点防护

由于合规性要求和复核中心审计，你依旧需要端点防护（通常称做防病毒）。但是大多数端点安全套件不只包含传统的防病毒库，还包括一些我们已经讨论过的策略。显然，在这有着 15, 20 成员的市场中，检测质量是五花八门的，并且是动态的。每一个安全厂商都有着跌宕起伏的检测效果。

那么，在选择一个端点保护套件的时候，我们该怎么给出建议呢。这涉及到整个系列的文章，但是我只想说检测效果可能不应该是最重要的选择标准。这很难验证。他们都在从事着一个体面的工作，即发现已知病毒，而不是从事着一个不体面的工作，即发现本文关注的高级攻击。为了合规，你需要端点防护。因此，你应该最小化价格，确保代理商能够有效的管理（尤其是如果你有数千个端点），并且确保他们尽可能的瘦。使用一个非但不能像需要的那样很好工作，反而使设备性能崩溃、加重损失的控制手段是一件很糟糕的事。得利用所有手段检查最新的，具有可比性的效果排名。但是对他们的了解很快就会过时。

越早检测到恶意软件并阻止恶意软件，不得不去清除的混乱就越少。

基于网络的恶意软件检测

你越早检测到恶意软件并阻止恶意软件，你不得不去清除的混乱就越少。那意味着，在一个攻击到达你的桌面附近以前，在边界或甚至在云端就消除它。你该如何做呢？一种新型网络安全设备详细检测入口流量，以便在恶意软件文件进入你的企业网络以前检测到他们。我们期望，一段时间以后，此种能力成为每一个边界设备的功能。而不是

像现在，你将需要处置特定的公司和独立的设备。我们在今年的早些时候发布了一些研究成果。关于其中的方式方法、限制条件，以及这些设备在你的网络安全策略中所扮演的角色的详情，请参见[基于网络的恶意软件检测 \(Network-based Malware Detection for \)](#)。

高级端点控制

我们都知道，传统的端点安全套件遗留了太多的，暴露于高级攻击者面前的攻击面，这取决于你的疼痛阈值（你怎样更容易被一个高级攻击者选为攻击目标）。额外的端点防护可能也是必要的。因此，让我们讨论一下这些替代的手段。这些手段基于行为信标、追踪文件轨迹和传播、以及/或允许被授权的可执行文件来进行检测和阻断。

第一类的高级端点控制是针对应用层的，它为在操作系统底层的、运行着的应用提供保护。一些新产品上已经出现了对上述恶意软件检测 Cocktail 的利用。这种“端点上正在发生什么”的分析方法结合来自应用活动和行为的上下文背景（正如上面“提供上下文”一章中描述的那样），能够减少误报并提高效率。这些工具的阻断影响了用户体验（通常这是好事），但是在广泛部署以前，对其进行适当的调查。但是，你利用所有新技术这样做了，对吧？

对于追踪恶意软件在你的环境中的传播，保护原点安全，减少再次感染的可能性来说，我们已经探讨了对恶意软件的扩散分析是如何非常有用的。我们提倡将这类分析作为另一个层面的防御。在收集用于分析的信息的时候，你有两个主要的选择：要么从端点收集，要么在网络中收集。端点解决方案提供了一个瘦 agent，该 agent 将信息上传到提供分析和虚拟化的云端存储库中。利用了来自许多其他的组织的疫情数据。显然，这涉及到另一个桌面 agent 以及另一个管理界面，但是共性分析能提供有趣的信息。

你也可以通过监控出口流量来寻找你网络中的 C&C 连接。

服务器保存有 C&C 网络的列表和 botnet 使用的通信模式，以识别被攻陷的设备成员。请记住，走到这一步，已经迟了。在这一点上，设备已经被攻陷。但是你可以进行一个准确的评估，以便确定哪个设备需要被立刻清理，因为他们的行为方式被认为是恶意的。不幸的是，着眼于网络并不能明确识别恶意软件源点，这限制了它在减少再感染方面的效用。

最后，你有一个苛刻的选择：应用程序白名单。这涉及端点上的一个“默认拒绝（default deny）”方法。这种方法只允许一组被授权的可执行文件在受保护的端点上运行，而阻止任何其他的运行。这种方式是苛刻的，因为他极大的影响了用户体验。通常不是一个好方法。多数白名单产品提供了宽限期（grace period），以允许程序的运行，直到一个管理员批准或拒绝该请求。但是这种妥协违反安全模型。某些厂商进行内存分析并引入其他行为方法，以减少宽限期的风险，但是一个宽限期本身引入了重大风险。我们认为 AWL 更适合固定功能设备（例如信息亭，呼叫中心，控制系统等等），通用的软件不会在这些设备中运行。

当然，或通过外部购并或通过内部开发，这些先进策略中的大多数最终会被归入到现有的控制手段中。这也正是安全市场的运作方式

这种“端点上正在发生什么”的分析方法结合来自应用活动和特定行为的上下文背景，能够减少误报并提高效率。

当然，或通过外部购并或通过内部开发，这些先进策略中的大多数最终会被归入到现有的控制手段中。这也正是安全市场（以及大多数其他技术市场）的运作方式。今日的先进将会是明日的标准。但是这一过程会耗费 2 到 3 年，多数企业都等不了，因此，你可以衡量这些技术以填补空白。

当然，不是所有的这些控制手段都在端点运行的，尽管这一系列文章的标题是这么写的。你需要将不同的控制手段应用在你的处置中，有一些手段在你的 IT 架构的其他部分会工作的更好。对这些进行权衡，并设计一个有效的，层次化的控制集合是一门艺术，而不是信息安全科学。

层次化的控制集合是一门艺术，而不是信息安全科学。

衡量和折中

时间

为检测高级恶意软件，你需要在你的规划中涵盖时间要素。不同的手段是更有效率，还是不那么有效率，这取决于你什么时候使用他们。例如，发件人或文件的信誉在攻击发生的早期是很有价值的。如果你获得了一个基于信誉的，情报的提示，你可以跳过其他更高要求的分析。同样的，对恶意软件特征的检查是快速的，并需要及早进行的。

但是，在恶意软件执行之前察觉攻击正变得越来越困难。我们提及的很多行为信标只有当恶意软件运行时才可用。一旦它激活，其他的就出现。下面这个图表阐述了我们的意思。

攻击前/中/后期的检测		
攻击前期	攻击中期	攻击后期
信誉（设备，发送者）	内存崩溃/缓冲区溢出	出口网络流量
文件签名	系统文件/配置/注册表更改	命令和控制网络流量
基于网络的恶意软件检测	父子进程不一致	恶意软件文件传播分析
邮件/钓鱼防御	Droppers 和安装代码	键盘记录器活动
网页过滤	关闭安全控制（例如 AV 和/或 HIPS）	屏幕抓取
		权限提升（和其他有趣的身份攻击）
		DLP（和其他内容过滤技术）

当然，你越早检测到攻击越好。因此，在任何潜在的感染发生以前，检测到恶意代码的控制手段是更可取的。但是，正如我们反复提到的那样，在恶意软件运行以前察觉高级攻击的难度正在增加，这使得中期和后期都需要为检测而努力。与大多数的安全策略一样，正确答案是上述所有手段，混合控制手段并使他们契合攻击链条上的所有环节，以最大限度的提高检测到攻击和随后被攻陷的机会。

设备/位置差异

当设计控制手段的时候，需要考虑的另一方面是你施加于设备上的控制手段的数量，以及它是什么类型的设备。保护移动设备和保护 PCs 是有本质上的不同的，尤其是如果你的企业不拥有设备（例如 BYOD）。显然，你对公司的电脑有最大的控制权，你可以在那上面进行证书扫描，安装一个设备 agent 来检查文件签名和信誉，以及检察行为信标。

保护移动设备和保护 PCs 是有本质上的不同的，尤其是如果你的企业不拥有设备（例如 BYOD）。

对于那些你不能实施控制的设备（例如，那些隶属于承包商、客户和也许属于员工的设备），你也许可以通过扫描网络连接或安装浏览器插件来保护一个特定的 web 应用或一组域。但是你需要小心从事。隐私通常是设备不受你控制的一个主要原因。如果安装一个 agent 或插件是不可行的，你需要依靠上面描述的，对攻击前期的控制手段，以便（希望）在该设备被接入你的网络时阻止攻击。攻击后期的网络监控应该被作为一个备用手段，以在攻击者获取你的数据之前抓住他们的不当行为。

当该设备被接入你的网络（无论是物理的还是通过 VPN），它从你的边界安全控制中获得了入口和出口的防护。如果它没有被接入网络，这些基于网络的控制手段是不可用的。

智能手机有点不同。你也许能够安装一个 agent，但不同的手机操作系统之间，功能变化很大。不要指望会有很大能力来检查智能手机上的行为信标，因为 agents 很少实时访问移动设备的内核。与 IOS 相比，安卓系统提供了更大的访问范围。因此反恶意软件 agents 在安卓系统上是可用的。但是，与基于 PC 的 agent 相比，任何移动设备 agent 的能力都是有限的，除非移动设备越狱或被 rooted。那就是另一个完全不同的讨论了。

请记住，一个设备的当前位置影响你保护它的能力。当该设备被接入你的网络（无论是物理的还是通过 VPN），它从你的边界安全控制中获得了入口和出口的防护。你能够通过基于网络的恶意软件检测或邮件安全设备在边界阻断攻击。你也可以通过执行出口过滤来寻找预示着一个攻击

的 C&C 流量或数据泄露。

折中

你在处置过程中使用的控制手段涉及从监控到锁定设备。检测高级恶意软件需要所有的手段，但是你需要认识到发生在终端用户身上的破坏性影响。在其中找到一个平衡点，即具有足够安全又不很具有破坏性，可以操纵对设备所有权和控制权的限制约束，以及可以切实可行的、跨设备的地点和网络连接场景。不存在简单的，正确的答案。只有一个把握需求的机会，并确保决策者明白他们所选择的这折方案。

总结

今日的对手有大量的资金，专业的知识和耐心来持续的攻击他们的目标，一直到他们在其中站稳脚跟。第一个立足点被用于在你的环境中建立一个“大本营”，以便在未来可以攻击设备、窃取数据，以及继续留在你的业务系统中。

但是，对此类攻击者的一个错误认识是：攻击者总是使用高级恶意软件和针对性攻击。攻击者只使用在先进性方面刚好达到他们要求的攻击手段。所以，如果一个企业的防御措施有限，攻击者就使用简单的方法。相反的，如果建设了强壮网络和应用控制的企业实施了一个精确的安全程序，并监控了环境中的大量活动，攻击者则需要使用非常复杂的攻击手段来实现他们的目标。

大多数端点防护产品所采用的检测技术不足以抓住或阻断这些高级攻击，因此安全行业需要超越传统的检测手段，增加抗击这些攻击者的手段的复杂性。安全策略（例如行为分析，信誉，和恶意软件的传播分析）提供了一个更坚实的基础，以便在数据失窃之前发现攻击。

当然，如果没有将上下文背景因素纳入对“用户正在做什么”的探寻中，你注定会重复技术（类似于，主机入侵防御，HIPS）上的失败。它摒弃了许多误报和产生不利影响的技术。其他控制手段（包括应用程序白名单）提供了针对这些高级攻击者的防护。但是这是以用户体验产生不利影响为代价的。最终，企业认定不对用户产生不利影响比使他们免受恶意软件侵害更重要。因此，安全专业人员需要回过头来，重新开始，以便在不干扰用户体验的情况下提高检测能力。

传统的检测技术在发现已知攻击方面仍占有一席之地。但是在检测高级攻击和对抗执着的攻击者方面，你需要结合一些高级端点分析技术，以提供足够的上下文背景，以便确定一个特定行为在那个时刻是清白的，还是恶意的。

如果你对这个主题有任何疑问，或是想专门讨论你的情况，请发信至 info@securosis.com 或通过 Securosis Nexus (<http://nexus.securosis.com/>)提问。

关于分析师

Mike Rothman, 分析师/总裁

在企业确定有效的战略以应对动态安全威胁场景时，Mike 的大胆观点和不羁的风格是非常宝贵的。Mike 专注于从事安全领域中那吸引人的部分，例如，网络和端点防护，安全管理和合规性。Mike 是安全业中最受欢迎的演讲者和评论员，在信息安全方面具有深厚的背景。在安全领域闯荡了 20 年后，他就是那样一个“知道尸体埋在哪里”的探员。

Mike 作为程序员和网络顾问开始了职业生涯。他在 1993 年加入 META 集团，称为 META 进军信息安全研究的先头部队成员。Mike 在 1998 年离开 META，建立 SHYM Technology (PKI 软件市场的先驱)，然后在 CipherTrust 和 TruSecure 担任主管。在厌倦了安全厂商的生活之后，Mike 在 2006 年创立了 Security Incite，以图在被过度炒作的，平庸的安全行业内向外界提供一个理性的声音。在短暂的担任 eIQnetworks 的战略高级 VP 以追寻在安全和合规性管理领域的灵感之后，Mike 加入 Securosis，在安全状态和作为一个安全专家幸存下来都需要什么的领域重新焕发青春。

2007 年，Mike 发表了 The Pragmatic CSO <<http://www.pragmaticcso.com/>>，使面向技术的安全专业人员意识到自身与高级安全专业人员之间存在的细微差别。他在康奈尔大学的运筹学和工业工程学院获得了工程学位。他的家人高兴地看到，他将他所受的教育的一部分用于每天的工作。你可以通过 mrothman@securosis.com 联络他。

关于 Securosis

Securosis, LLC 是一家独立的研究和分析公司，致力于思维的领导性、客观性和透明性。我们的分析师都拥有经理职位，并致力于为客户提供高价值的，务实的咨询服务。

我们的服务包括：

- **Securosis Nexus** : Securosis Nexus 是一个在线环境，能够使你的工作做得更快、更好。它提供了对安全议题的务实研究，该研究向你讲述的内容恰恰是你所需要知道的。它在业界领先的专家的支撑下，回答你的问题。Nexus 被设计得更快，更易于使用，并且使你能尽可能快的得到你所需的信息。访问链接：<<https://nexus.securosis.com/>>.
- **主要的研究出版物** :我们当前通过我们的博客发布了绝大多数的研究成果，这些研究成果是免费的，并存档于在我们的研究库里。大多数的研究文档能够每年发布。所有发布的资料和演示文稿符合我们严格的客观要求，并遵循我们的完全透明研究政策（Totally Transparent Research policy）。
- **针对终端用户的研究产品和战略咨询服务** :Securosis 将引入一个研究产品线和基于调查的订阅服务，以便在促进项目和计划的成功方面协助终端用户企业。Securosis 也有其他的咨询项目，包括产品选择的协助，技术和架构策略，教育，安全管理评估和风险评估选择产品。
- **针对厂商的预付费服务** :虽然我们将接收来自任何人的简报，但是一些厂商会选择更严格，更持续的服务。我们提供了灵活的预付费包。作为包中的一部分的服务包括，市场和产品的分析和策略，技术指导，产品评估，以及并购评估。即使对已付费的客户，我们也保持着我们严格的客观性和机密性的要求。更多的关于我们的预付费服务的信息（PDF）已经发布。
- **对外的演讲和社论** :Securosis 的分析师经常在行业活动中发表演讲，进行在线演示，在各种刊物和媒体上撰写文章和/或发表讲话。
- **其他专业服务** :Securosis 的分析师也提供其他服务，包括战略咨询日，战略咨询服务，和投资者服务。这些往往是定制的，以满足客户的特殊需求。

我们的用户从潜在创业者到一些最知名的技术厂商和终端用户。客户包括大型金融机构，机构投资者，中大型企业和主要安全厂商。

此外，Securosis 与安全性测试实验室结成伙伴，以提供独有的产品评估。该产品评估将深度技术分析 with 顶层产品、架构和市场的分析相结合。更多的关于 Securosis 的信息参见我们的网站 <<http://securosis.com/>>.