

高级持续性威胁和实时威胁管理

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	Advanced Persistent Threats and Real-Time Threat Management		
原文作者	Realtime Publishers	原文发布日期	
作者简介	Realtime Publishers 为 IT 专业人士提供领先、专业的媒体产品（电子书、白皮书、视频教程，播客等）。Realtime 拥有 IT 领域最好的作者和超过 20 万 IT 专家读者，能够实时提供无可比拟的品牌传播机制，增加您的目标受众并带来真正的产品需求。 http://www.linkedin.com/company/realtime-publishers		
原文发布单位	Realtime Publishers		
原文出处	http://www.trendmicro.de/media/misc/ebook-advanced-persistent-threats-and-real-time-threat-management.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</p>		

	<p>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>
--	---

Realtime
publishers

高级持续性威胁和实时 威胁管理

精华系列

sponsored by



Dan Sullivan

Realtime Publishers 简介

Don Jones , 丛书主编

几年来, Realtime 已经出版数十本高品质的书籍。这些书籍以免费电子书的形式推出。在那些同意承担每本书的出版费用, 以飨读者的赞助商的慷慨支持和合作下, Realtime 形成了这种独特的出版模式。

虽然我们总是向您提供免费的出版物, 但千万不要认为我们不重视质量。我的工作就是确保我们的书籍与您花费\$40 买回来的那些印刷书籍一样好, 甚至在大多数情况下会更好。与印刷书籍相比, 我们的电子出版模式拥有几个优势: 作者一写完, 您就能收到(因此, “实时” 是我们的模式的一个方面), 我们能够通过更新章节来反映技术的最新变革。

我想指出的是, 我们的书籍绝对不是付费广告或者白皮书。我们是一个独立的出版公司。我工作的一个重要部分就是确保我们的作者能够毫无保留的或毫不受限的, 自由的表达他们的专业观点。我为我们在过去的几年中出版这么多优质图书而感到自豪。

如果您是从您的朋友或同事那里收到的本出版物, 欢迎您访问我们的网站, <http://nexus.realtimepublishers.com>, 我们还有各种主题的其他书籍。在那里, 您一定能找到您感兴趣的東西, 而且不用花精力。我们希望您基于学习的目的, 在未来能继续访问 Realtime。

在此之前, 请享受阅读吧。

Don Jones

目录

Realtime Publishers 简介	i
1 超越炒作：高级持续性威胁	1
当今的 APT	1
进化中的威胁场景	1
APT 的要素	2
变化中的商业行为使问题变得更复杂	3
控制 APT 的潜力的务实评估	3
总结	4
2 需要实时管理和响应	5
标准端点和边界安全控制的局限性	5
应对入侵的步骤	6
防止入侵的理想和现实评估	7
总结	8
3 规划实时 APT 对抗策略	9
实时威胁管理的商业案例	9
为实时威胁管理评估当前的准备状态	10
规划实时威胁管理系统的部署	10
用于阻断的控制机制	11
用于监测的控制机制	11
遏制机制	12
总结	12

版权声明

© 2011 Realtime 出版商。保留所有权。本网站包含的已创建、发布、或 Realtime 出版商及本网站受委托和获得许可出版的资料（以下简称“资料”）和任何此类资料受国际版权法和商标法保护。

该资料是“按现状”提供的，没有任何形式的（不论明示或默示）的保证，包括但不限于对适销性、适合某一特定用途，所有权和非侵权性的默示保证。该材料如有更改，恕不另行通知，并且不代表 Realtime 网站赞助商的承诺。在任何情况下，Realtime 出版商或其网站赞助商对其所发布的资料中所含的技术或拼写错误或疏漏负责，包括但不限于任何因使用资料中所含任何信息所导致的直接、间接、偶然、特殊、惩戒性或后果性损害。

除了出于个人的、非商业的用途下载该资料（包括但不限于文字，图片，音频，和/或视频）的一个拷贝至一台计算机以外，不得以任何方式复制，转载，再版，上传，张贴，传输，或分发资料的全部或部分。在相关使用中，你不得修改或遮掩任何版权或其他所有权声明。

该资料可能包含从属于第三方的商标，服务商标和徽标。如无该第三方的事先书面许可，不得使用这些商标，服务商标和徽标。

Realtime 出版商和 Realtime 出版商徽标已在美国专利和商标局注册。所有其他产品或服务名称均其各自所有者所有。

如果您对这些条款存疑，或者您想了解 Realtime 出版商的许可资料，请与我们联系：
info@realtimepublishers.com.

1 超越炒作：高级持续性威胁

企业面对着一个不断进化的威胁场景。其中的最大挑战就是高级持续威胁 (APTs)。APT 是种针对某一特定组织的、复杂的、多方位的攻击。要想削弱 APT 带来的风险，需要在传统的分层安全模式之外将实时威胁管理囊括进来。该概要系列描述了 APT 的本质，给企业带来的风险，对 APT 和其他新出现的威胁的阻止，检测和遏制技术。我们以对 APT 本质的一个务实的评估开篇：

- APT 的本质
- 持续进化的威胁场景
- APT 的要素
- 变化中的商业行为使问题更加复杂
- 控制和削弱来自 APT 的风险的潜力的评估

显然，威胁场景正不断地变得更富有挑战性。对信息系统发起攻击的动机和手段正在发生改变。明确的，坚定的攻击者正采用多种手段来突破安全控制系统。企业需要采用多种安全控制手段（包括实时监控和快速遏制措施）来应对。

当今的 APT

APT 是种针对某一特定组织的复杂的，多方位的网络攻击。该攻击采用先进的技术，攻击者对攻击目标有深入的了解。APT 可能使用多个载体（例如，恶意软件，漏洞扫描，针对性黑客攻击和恶意内部人员）来攻破安全措施。APT 是种长期的、多阶段的攻击。一个 APT 攻击的早期阶段可能侧重于搜集网络配置信息和服务器操作系统的细节信息。此后，攻击工作可能侧重于通过安装 rootkits 或其他恶意软件来取得控制权或与命令和控制服务器建立通信。一个攻击的后期可能侧重于通过复制机密或敏感数据来窃取知识产权。

请务必明白，APT 不是一种新的攻击手段，也不是一种能通过阻止或打断一次就可以彻底解决掉的攻击。APT 更像是一个网络攻击活动而不是一个单一类型的威胁，可以将其认为是个正在进行的过程。一个反病毒程序可能会阻止在一个 APT 中使用的恶意软件，但是这并不意味着 APT 攻击被终止。就本质而言，一个 APT 是一个持续的攻击。如果一个战术行不通，它会尝试另一个战术。实际上，我们不应该寻求一个单一的对策或者为一个多层安全策略增加更多的层。相反的，我们应该寻求一种过程，它在一种情况下尽可能的阻止 APT，在其他情况下能够检测和遏制入侵。那么，我们会问，为什么我们还停留在原地？

进化中的威胁场景

企业和政府面对一个正在进化中的威胁场景。攻击者从最初的以更改一个主要报纸的网站或对流行站点实施 Dos 攻击，阻塞其服务的方式来进行炫耀，转向以获取经济利益为目的的攻击。攻击者能通过欺诈

或窃取知识产权来实现直接的经济收益,或者通过破坏对手提供服务的能力或广泛宣传涉及用户私人财务信息的数据泄露事件来获取非直接的经济收益。除了动机的变化,攻击的实施手段也在改变。

应用程序架构的变化和核心业务的下放为攻击者创造了机会。在过去,银行柜员和 ATM 机是你银行帐户实施交易的唯一方式。现在,你可以通过你的电话进行交易。不久前,我们还在谈论零售商使用实体店和 mall 的图片,现在,网站同样可以出售从书籍到应用的一切。支持许多企业服务的 Web 应用提供了工作流的实现,工作流最终通向库存管理、应收账款等后台系统。这些很容易成为漏洞扫描、注入攻击以及其它的,能够揭示应用架构和潜在漏洞信息的探测器的目标。

进化中的威胁场景的另一个要素是技术的组合使用。恶意软件可以被用来执行一个特殊任务(例如,捕获击键),或者可能包括一个通信模块,该通信模块与命令控制服务器协同工作,下载指令,从而允许攻击者探测、发现以及调整他们的搜索策略。

我们在 APTs 中发现的一些技术在过去的复合型威胁攻击中也被使用过。复合型威胁攻击使用单一攻击载体投递多种形式的恶意软件。我们还发现,攻击会发生变化以应对防御策略。当反病毒软件利用模式匹配技术成功的检测到病毒的时候,恶意软件的开发者采用加密和多态技术来打乱他们代码,以躲避检测。同样的,如果一个系统中的一个路由入口被阻断,一个 APT 会寻求另一个入口。APT 的动态特性是安全威胁的共同特点,但是 APTs 还具有区别于其他类型的攻击的特点。

APT 的要素

在基本层面上,一个攻击成为一个 APT 需具有三个特点:

- 受经济利益或竞争优势驱使
- 一个长期的,持续攻击
- 以一个特定的公司,组织或平台为目标

企业和政府成为 APTs 的目标的原因是很显然的。企业拥有金融资产和高估值的知识产权。可能自从有政府开始,政府就要面对外部的侵略。因此,APT 的概念在许多方面并不新颖。它新颖的地方在于执行这种威胁的方式涉及到网络和应用领域。

长期的攻击可能持续几天,几周,几个月或甚至更长时间。APT 攻击可以开始于搜集情报。这一过程可能持续一段时间。它可能包括技术情报搜集和人员情报搜集。情报搜集工作对后期的攻击起指导作用,后期的攻击可能是快速的,也可能是持续的。例如,试图窃取商业秘密的,可能需要花费数月来搜集关于安全协议、应用程序漏洞和文件存储位置的情报,然后一旦确定计划,用几分钟来实施窃取行动。在其他情况下,攻击可能长期持续。例如,在一个服务器上成功的部署了一个 rootkit 之后,一个攻击者可能定期发送具有潜在价值的文件副本到命令和控制服务器以供查阅。

许多广为人知的 APTs 攻击展示了攻击手段的广度和驱使 APTs 发展的动机:

- Zeus botnet, 开始作为一个攻击金融机构的平台,后来转变为其他类型的 APTs 的框架。
- Aurora APT 攻击 Google 和其他技术公司,似乎试图获得访问并修改应用程序代码的机会。

- Stuxnet 是高度专业化的工业系统恶意软件。它包括一个针对工业设备中的可编程逻辑控制器的 rootkit。媒体猜测 Stuxnet 是由一个或多个政府研发的。

这些 APTs 利用了我们提供服务的方式的变化。

变化中的商业行为使问题变得更复杂

攻击技术和动机的变化是 APTs 成为如此重大威胁的一部分原因。我们构建系统方式和允许访问业务系统的模式也是一部分原因。

考虑反边界 (de-perimeterization)。在过去, 防火墙阻断了非法流量。随着应用的发展, 出现了对更灵活的网络流量的需求。外部人员需要访问内网资源。开发者编写应用, 在被允许的协议 (既 http) 上通过隧道封装被阻断的流量。与对所有的网络资源设置单一边界不同的是, 企业开放更多的服务器访问, 依靠基于设备的访问控制和网络流量监控。

能够被 APTs 利用的另一个因素是移动设备和其他非托管设备的增加。IT 部门不能总要求一个设备在使用内部服务之前, 必须将反病毒软件或访问控制安装到位。这些设备会被 APTs 利用, 成为对企业或政府网络的攻击的一部分。

同样的, 公开的、可用的 Web 应用的增加导致了另一个潜在的攻击方式。例如, 就像收集应用程序结构那样, 可以通过对一个 Web 应用的注入攻击来收集数据库内容的情报。

通过扩大雇员对关键信息设施的访问, 企业可以使员工更容易的, 更有效的完成必要的任务。然而, 这样也增加了攻击者的潜在进入入口。

技术和组织因素与执行一个 APTs 攻击的潜在可能性同在。其中的许多因素, 例如员工授权, 来自移动设备的访问应用都是有利的, 很难去掉的。我们需要减小 APTs 的风险, 而不以牺牲这些和其他先进之处为代价。

控制 APT 的潜力的务实评估

从实用的角度看, 可以做个合理的假设: APTs 在可见的、未来的日子里, 将会与我们同在。网络安全的历史充满了在应对新类型控制过程中出现新型攻击模式的例子。APTs 是长期的、面向过程的攻击。他是攻击者的动机以及他们所能使用的攻击手段变化的产物。鉴于 APTs 的存在, 有什么能够减轻 APTs 所带来的风险的策略?

我们应该继续部署拦截措施。反恶意软件、加密、漏洞扫描和补丁都是很好的措施。仅仅这些并不足够, 为了对抗 APTs, 我们应该假设存在一个漏洞。这并不是说, 那些防御措施存在问题; 这个观点只是认定这样一个事实, 那就是一个坚定的、持久的攻击可以找到一个绕过阻断措施的方法。

在这一假设下 (即, 在某点上存在一个漏洞), 我们必须实时的监控网络流量和主机行为。一旦漏洞被利用, 当务之急就是尽快检测到漏洞, 进而遏制其所产生的影响。遏制行为包括隔离被攻陷的设备, 关闭服务, 以及为取证分析收集数据。

总结

APTs 是一类安全威胁。它给 IT 和安全专业人员带来特殊的挑战。在经济或其他长期利益的驱使下，在大量的恶意软件和黑客技术的武装下，攻击者愿意花费时间和精力去攻陷一个组织的防御。许多过去使用的、优秀的防御方法，在今天依旧没有过时。但是，在下一篇文章中我们将看到，我们需要在我们的对抗策略中加入实施监控和遏制技术。

2 需要实时管理和响应

理想情况下,我们可以部署安全控制策略,以防止高级持续威胁(APT)实施的一个成功的攻击。但是,在我们评估的中,我们应该更务实一些。APTs 攻击是多方面的。一种防御手段(例如,防病毒系统)可能会阻止一个 APT 的一部分,但是攻击可以有不依赖于可探测的恶意软件的其他组成部分。比如,有一个恶意的内部人员,他通过社会工程学的方式来发现一个文档管理系统的一个管理员帐户的密码,复制存储库中的内容,并挖掘其中的知识产权。当规划一个对 APTs 威胁的响应的时候,我们应该假设在某一时间上存在一个漏洞。在这种情况下,风险管理的总体目标是在可能的情况下通过阻断来最小化威胁造成的影响、在其他情况下,检测和遏制威胁造成的影响。因此我们需要实时监控和补救机制。

本文认为需要实时威胁管理和响应,尤其是:

- 传统终端和边界安全控制的限制
- 对一个 APT 入侵的响应阶段
- 防止入侵的理想和现实上的评估

正如本系列的第一篇文章所述,一个核心主题是这样一个假定:我们应该重视 APTs 威胁,并为攻击做好准备。这并不是说所有企业将成为 APT 攻击的受害者或者所有的 APT 都会成功。从一个纯务实的角度来说,为可能遭受的攻击做好准备但攻击却没有发生,比攻击发生却没有做好准备要好得多。

标准端点和边界安全控制的局限性

标准的端点和边界控制可以很好的阻断投机的和不周密的攻击。但是 APTs 被设计来规避这些防御措施例如,一个攻击的开端是用员工身份访问关键信息系统,然后是鱼叉式钓鱼和其他社会工程学技术。在这个阶段,攻击的目标是打着某些合法操作的幌子(例如,点击一封 email 里的链接来访问一个窗口或检索内容),引诱受害人安装恶意软件。

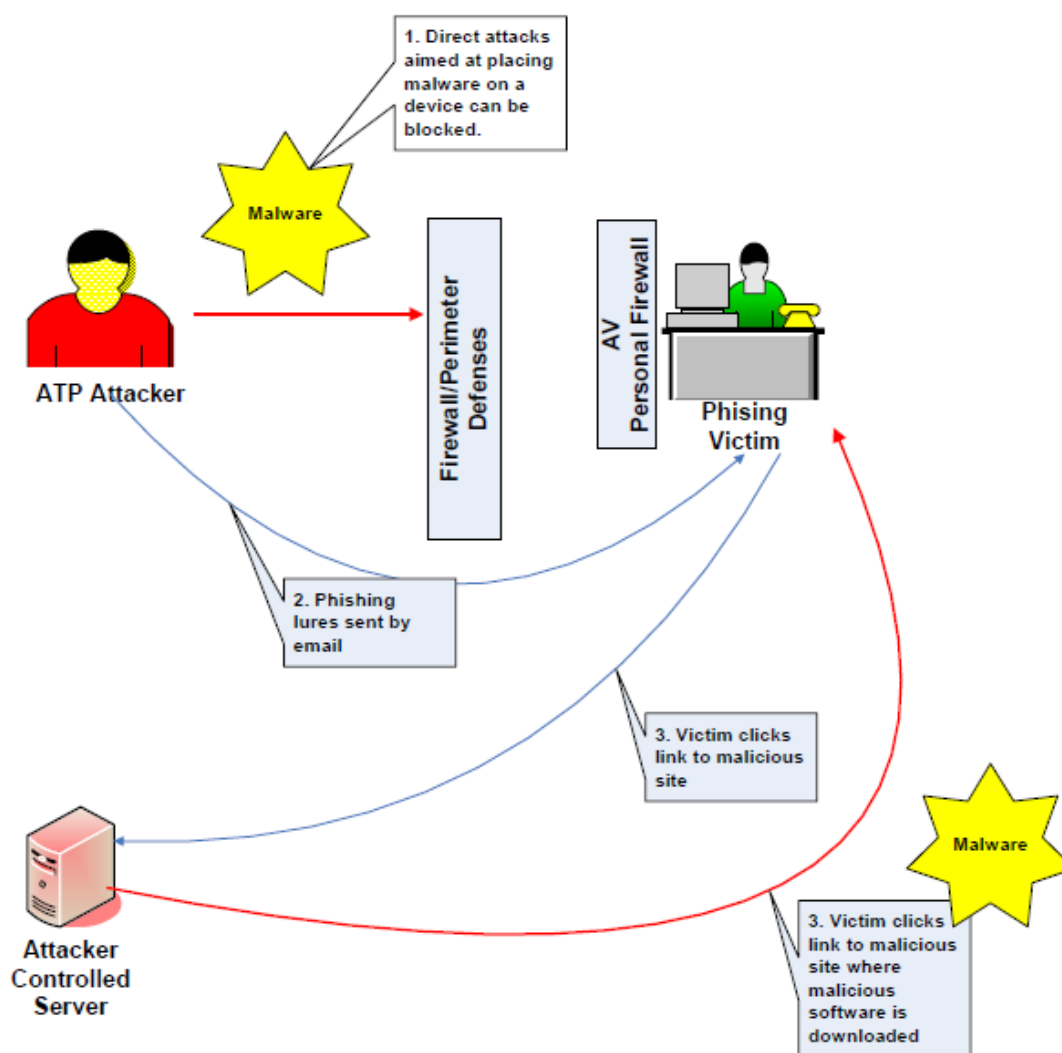


图 1: APT 攻击用网络钓鱼来规避边界和本地设备的安全措施

一旦一个攻击者通过被攻击者控制的服务器找到了一个受害者，他就可以下载恶意软件。攻击可以使用加密和其他技术去躲避使用模式匹配的系统的侦测，使得系统很难判断一个用户正在下载的内容是不是包含恶意软件。

使恶意软件进入受害者的设备只是一个 APT 攻击的第一步。越早探测到这样一个入侵，越有机会遏制该损害。这也就是为什么我们需要实时威胁管理。

应对入侵的步骤

应对一个 APT 的侵入有四步：

- 最初的入口
- 系统和信息的损害
- 发现入侵
- 遏制入侵

从风险管理的角度看，关键的阶段是发现。假定，一个 APT 攻击成功的躲避或绕过了边界、网络和本地防御，那么问题就变成这个攻击在被检测到以前持续了多久。

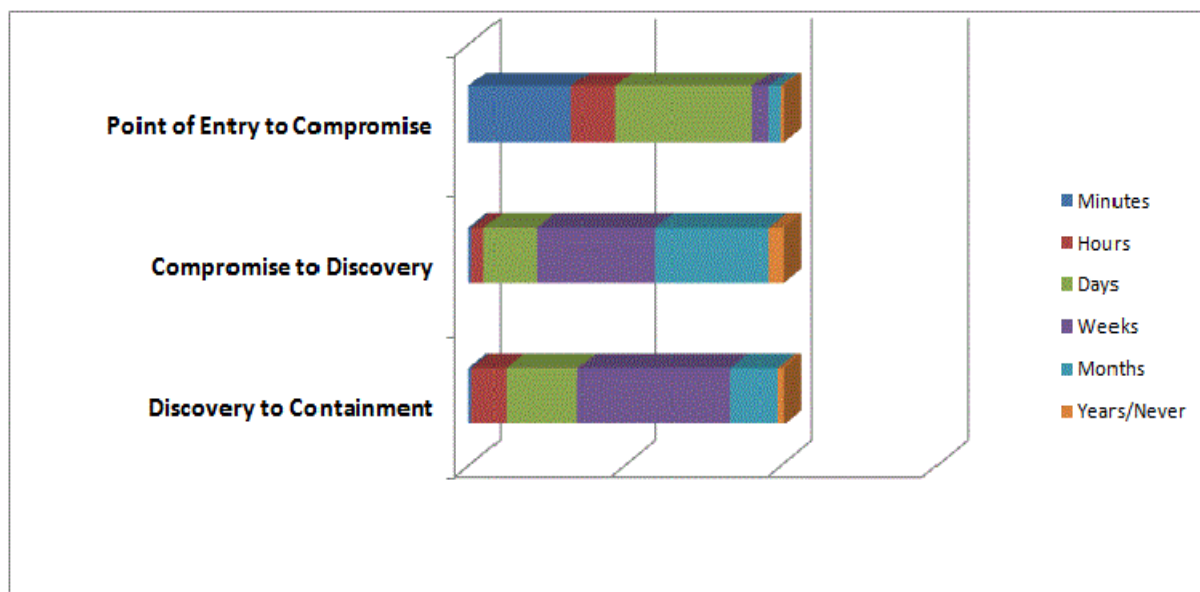


图 2：几分钟之内，攻击的重要部分就从攻入安全控制转移到侵入系统或泄漏信息。许多此类攻击，几星期或几个月都没有被发现。（源：[Verizon 2011 Data Breach Investigations Report](#)）

在 Verizon 数据泄露研究统计报告中，有两点值得注意。首先，在攻击事件中占显著比例的是几分钟内就实现攻陷。APTs 的攻击速度意味着，那种需要手工干预的响应在很多情况下已经为时已晚。这也就是为什么需要实时管理。通常在启动一个响应的时候，一点时间都不能浪费。

我们应该特别注意的另一点是大量的、需要几星期或几个月才能发现的攻击。只有发现攻击，才能够遏制攻击。某些攻击可能是那种时间点攻击。在此类攻击中，攻击者窃取数据或执行某些其他的恶意行为，然后终止攻击。其他类型攻击可以一直持续下去，直到被发现，例如，发送到命令和控制服务器的客户信用卡数据的数据流每天二十四小时都有。这就需要活跃的、持续的监控和分析来尽早发现入侵。

防止入侵的理想和现实评估

正如前面指出的，理想情况下，安全控制（例如，反病毒和边界控制）足以削弱一个安全漏洞的风险。但，事实并不是如此。攻击者知道边界控制和反病毒系统是如何工作的，在许多情况下他们做的很好。事实表明，攻击者选择绕过反病毒核边界控制，以避免直接面对他们。毕竟，当你可以利用社会工程学来欺骗合法用户的时候，何苦费力去设计复杂的，能够绕过检测的恶意软件呢。钓鱼攻击利用了这样一个事实，即有些用户拥有足够权限来访问目标系统和数据。通过一个精心设计的鱼饵，攻击者能够使这些用户无意中充当他们触及目标的渠道。人有时是一个安全策略中的最薄弱的一环。我们要采用一些策略，这些策略能够包容这些弱点，并减弱他们所带来的风险。

一个务实的做法是力图阻止一个入侵，以及一旦入侵发生，减轻其造成的后果。这个方法分三部分。

首先，确保安全控制措施就位并及时更新。这些措施包括反病毒、加密、访问控制和漏洞扫描。因为漏

洞扫描不能探测到零日威胁,所以需要采用先进的网路监控手段监测和阻断入侵。这引发了第二点需求,即需要持续监控网络和服务,以发现入侵的迹象。这包括:

- 网络流量分析
- 服务器日志分析
- 主机入侵防御
- 文件完整性监控

全面的监控有助于检测一个攻击的足迹,例如,午夜,一个服务器与外部 IP 地址之间异常量级的网络流量,或者通过提升权限创建一个服务账户。

第三个需求是遏制入侵导致的影响。虚拟补丁和自动修复等技术能够阻断一个攻击,防止可以导致攻击的漏洞被再次利用。应该在一套风险管理程序集中定义遏制入侵的具体步骤。

这里的总体目标是减少一个攻击的入口点与控制点之间的时间差。需要采用实时威胁管理(包括监控和响应机制)来解决 APTs 带来的威胁。实时威胁管理的价值在于数据的价值不会被丢失和泄漏,因为其遏制的速度比手动发现和遏制攻击的速度快。

总结

常用的终端和边界安全控制都不足以阻断 APT 攻击。钓鱼和其他形式的社会工程学使得攻击者能够提供足够的访问控制引诱用户访问偶然被攻击者利用的设备的方式来绕过这些安全控制。APTs 通常可以在几分钟内,迅速的从入侵点移动到泄漏点。以人工干预的方式来检测和遏制 APT 攻击通常因速度太慢而起不到应有的效果。实时威胁管理可以尽可能快地对 APT 攻击做出回应。

3 规划实时 APT 对抗策略

高级持续威胁 (APTs) 已经成为企业, 政府及其它组织的重要威胁。本系列的前两篇文章已经从 APTs 的技术和减轻 APT 攻击风险需面对的挑战两方面做了分析。APT 不仅仅是恶意软件, 不能仅仅使用反病毒或边界控制的方式来终止它们。APT 采用旨在绕过传统阻断防御措施的社会工程学技术。攻击者并没有试图智取一个反病毒程序, 而是绕过了反病毒程序。当一个员工心甘情愿的访问一个钓鱼诱饵邮件中的链接, 并下载一个貌似是合法程序但实际上是加密的恶意软件的时候, 阻止员工这种行为的机会微乎其微。用户拥有下载和保存应用的访问控制权。基于模式的检测技术不能检测加密软件。综上所述传统的边界和端点防御不能阻止一个 APT。

需要明确的是, 边界防御和端点安全对解决 APTs 导致的风险是必要的, 但并不足够。我们需要实时威胁管理。在部署此类控制手段之前, 评估硬件、软件和安全控制的当前状态, 划分资产优先级, 并进行差别分析是一个明智的选择。这些工作的结果有助于规划如何部署主动控制。

本文是围绕着实时威胁管理部署规划的基本步骤来组织的。实时威胁管理的部署能够减轻 APTs 的风险:

- 为实时威胁管理开发一个商业案例
- 为实时威胁管理评估当前的准备状态
- 制定部署规划

毫不奇怪, 下面的一些建议也同样适合描述其他类型的遏制措施。APT 是一个被精心构建的, 以有条理和全面的方式应用于恶意目的的技术集合。过去使用的那些遏制措施在这里依旧是有用的。APT 的主要显著特征是它的行动速度。这反过来又推动了对实时威胁管理的需求, 以弥补边界和端点防御的不足。

实时威胁管理的商业案例

高管和 IT 经理不担心资源供不应求。为什么当一个企业已经在反病毒, 网络过滤, 身份管理和其他安全控制措施投入这么多的时候, 他们还得在实时威胁管理上投放额外的资源呢? 简而言之, 这是因为这些抵御措施并不足够。

APT 导致的风险是有据可查的。有很多广为人知的案例。例如, Stuxnet, Zeus, and Aurora 都表明 APT 能够通工业控制系统危及金融, 就像其对企业和政府做的那样。这些成功的攻击案例也表明了广泛使用的多层安全机制的局限性。这里再强调一遍, 这些机制是必要的, 但是他们不足以消减 APT 的风险。APT 被设计用来通过人和技术资源来搜集情报、探测漏洞以及针对一个目标规划多步骤的协同行动。APT 中使用的技术是被精心挑选的, 因为这些技术既能攻陷目标又能绕过安全措施。

在实时威胁管理的商业案例中使用的理由是切合实际的: APT 是存在的, 拥有信息、经济资源或足够价值的知识产权的组织是潜在的目标, 以及常用的多层安全防御不足以阻断一个复杂的攻击。在许多攻

击中，一旦攻陷目标，那么破坏性行为会在几分钟内发生。如果需要几个小时或几天来实施一个精心规划和执行的响应，那么我们可以将其视为是无用的。APTs 的速度非常快，以致需要通过一个持续监控来触发自动响应。

为实时威胁管理评估当前的准备状态

一旦完成实时威胁管理部署的商业案例，下一步是评估当前的准备状态。这涉及三个步骤：

- IT 设施清单
- 划分资产优先级
- 差别分析

这个阶段的最终产物是对当前安全控制机制的潜在薄弱的描述。实时威胁管理不是替代边界和终端防御，而是对他们们的一个补充。当终端和边界防御是最新的，并被部署到整个网络时，攻击者不得不花费更大代价来攻克这一体系。

IT 基础设施的清单包括：

- 硬件和网络设施
- 软件，尤其是企业级应用
- 数据库，内容管理系统和其他存储
- 安全控制

形成清单的目的是要了解什么会成为一个攻击的目标，或者什么会被一个攻击利用。网络管理和资产管理工具是可以被利用，它们能够发现一个网络中的资产，并生成这些系统的硬件和软件清单。

当有清单在手时，下一步就是划分资产优先级。并不是所有应用、服务器或其他设施都是平等的。依据这些资产的相对重要性，将它们划分成组，从而可以将资源首先放在最重要的资产上。

我们也要明白，这与当前的多层安全控制机制的配置之间存在着哪些差距。尤其是在阻断，检测和遏制攻击方面，安全控制机制都缺失了什么。现有的控制机制都能够支持实时威胁管理么？例如，日志分析工具能够胜任实时分析模式么？从将一个事件记录进日志到触发警报发之间有多少延迟？

我们还要考虑，当前的规管政策和流程对实时威胁管理是否是足够的。他们还应该包含一些关于如何响应一个可疑事件，以及谁（什么被自动控制）应该参与响应的规范。在这些步骤完成以后，你可以开始规划一个实时威胁管理系统的部署了。

规划实时威胁管理系统的部署

当你规划你的实时威胁管理系统，评估候选系统的时候，需要考虑三方面的关键需求：

- 用于阻断的控制机制

- 用于监测的控制机制
- 遏制机制

用于阻断的控制机制

阻断网络攻击是一个复杂的操作，需要多种类型的控制机制。尽管已经将防病毒软件部署在终端上，还是应该部署网络层恶意软件检测系统。这种冗余的部署是有用的，以防其中一个系统被绕过或者被攻陷。漏洞扫描有助于检测应用程序的薄弱之处。有两种不同类型的漏洞扫描。对于商业或开源应用，漏洞扫描有助于保持恰当的补丁级别，减小被通过已知漏洞攻击的风险。对于自定义应用，漏洞扫描有助于辨识潜在的注入攻击点，尤其是 SQL 注入攻击。尽管漏洞扫描很有用，但是它不能解决零日攻击的问题。这种攻击利用了应用程序中尚未公开的未知漏洞。

合规性验证过程也可以被采用。这一过程能够有助于检测不符合最小安全控制需求的配置。

用于监测的控制机制

实时威胁管理需要多种类的监控机制：

- 网络层分析
- 日志分析
- 主机入侵防御
- 已知的命令和控制服务器黑名单

网络层的分析需要拥有先进的技术，以便能够充分辨识出异常的模式，而又不会产生太多的误报。启发式规则和统计模式识别技术的结合可以使人们通过对这两项技术的取长补短来提高整体性能。

以网络分析为例，在日志分析上，必须要足够准确和精密，以便同时减少假正和假负的情况。它也必须有足够的分析能力以满足站点产生的日志数量。因此在评估这个工具和其他分析工具时，必须考虑性能和吞吐量因素。

除了监控网络流量和日志，还应该监控关键服务器。通过在服务器上建立一个行为基线，主机入侵防护系统能够帮助检测服务器上的异常活动，例如，异常高的 I/O 数量或者应用程序库的变化。这类监控也包括文件完整性检查。

不要忘了监控网络流量的上层，尤其是阻断对已知恶意服务器的访问。一个实时威胁管理应用，在理想情况下，应该能够提供已知对已知命令和控制服务器上的最新黑名单的访问。名单可能指向你网络上的一个高级攻击的一部分。

遏制机制

在一个攻击事件中，一个实时威胁管理系统能够自动的挽救形势。这包括隔离网络上被攻陷的设备，修补已知漏洞。遏制机制还应该支持风险管理流程，例如产生告警并依据事件的严重性不断升级告警。

总结

APTs 从安全的角度提出一系列新的挑战。APTs 被设计用来规避常用的安全控制机制部署。他们在速度上也值得称道。攻击者愿意在搜集情报和探测漏洞上投入更多。传统的边界和终端安全控制机制是必要的，但是并不足以全方位的阻止 APTs 导致的威胁。实施阻断、检测和遏制的实时威胁管理能够有助于减轻快速运动的 APTs 所导致的损害。APTs 能够在几分钟内完成从入侵控制机到攻陷系统和窃取数据的一系列动作。