高级持续性威胁的检测和防御

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	Detecting and Defending Against Advanced Persistent Threats		
原文作者	Information Week	**原文发布日期**	2012 年 3 月
作者简介	Information Week 是一本数字杂志，提供现实和虚拟事件，总部位于加利福尼亚州的旧金山。http://en.wikipedia.org/wiki/InformationWeek		
原文发布单位	Information Week		
原文出处	http://reports.informationweek.com/abstract/21/8710/security/strategy-detecting-and-defending-against-advanced-persistent-threats.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 3 月

高级持续威胁的检测和防御

对于大小企业来说，APT 的威胁日益严重。要想保护你的企业，远离这些针对性威胁，需要不断提高警惕，培训员工，齐心协力使安全系统可以应对 APT 的每一个阶段。企业还需要设立一个补救和响应的方案，以应对尽管尽了最大的努力，防线还是被突破的情况。

Michael Cobb

Presented in conjunction with

SECURITY dark READING
Protect The Business Enable Access

Report ID: S4390312

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。

Michael Cobb
InformationWeek Reports

Michael Cobb, CISSP-ISSAP, CLAS, 是一位著名的，拥有 15 年 IT 行业经验的，信息安全领域撰稿人。他是 Cobweb Applications 的创始人和常务董事，也是一位提供数据安全服务的顾问。他是 IIS Security 一书的作者之一。他在主流 IT 刊物上发表了大量的技术文章。Michael 还是微软认证数据库专家。

EXECUTIVE SUMMARY

高级持续威胁 正如字面意思，这个威胁是高级的。该威胁的研发和实施者需要拥有较高的专业水平。该威胁是持久的，埋伏着以等待最佳事机。当然是没有预防和战胜 APT 的灵丹妙药。APTs 是一种新的攻击模式。该模式能规避当前的边界和端点防御手段。然而，培训员工，提供健壮的用户凭据，加固服务器和工作站将有助于阻止恶意代码的传播。强大的日志将增加检测到 APT 相关活动的机会，并为应急响应团队提供更优质的信息以辨识和遏制攻击。在这份报告中，我们阐述了一个 APT 的六个阶段，并提出了我们的建议以保护你的企业免受日益严重的 APT 的威胁。

高级持续威胁的检测和防御

最狡猾的网络攻击手段之一是潜伏、等待。这些攻击（俗称高级持续威胁)是一个复杂的、定制化的攻击。他有明确的目标，即进入一个目标系统，并长期潜伏不被发现。一个 APT 的成功需要大量的资源和专业知识—因此，称为“高级”。 “持续”并不意味着希望成功的发动不断的攻击，而是意味着不懈的追求和研发一个成功的攻击方法。这些攻击是由熟练的、有目的性的、有组织的、有充足资源的、有明确路线图的程序员开发的。他们可能花费几个月时间来开发这些攻击，并花费更长的时间来成功部署这些攻击。在本报告中，我们将剖析一个 APT 攻击 (从侦测到数据获取),以识别你的企业的薄弱部位以及如何进行做补救。

近期，你可能已经听到了很多关于 APT 的新闻。Hydraq 和 Stuxnet, 以及近来对 RSA SecurID 和 Lockheed Martin 的攻击都可归类为 APTs。 然而，Conficker 和黑客团队 Anonymous and LulzSec 的攻击不属于 APT。Conficker 没有针对特定的组织，虽然 Anonymous and LulzSec 有特定的目标，但是团队很少或基本没有对攻击行为进行隐藏。

由于 APT 事件的数量不断上升，攻击所造成的损害的严重程度和范围不断的升级，人们对 APTs 的关注正日益增加。Cisco 安全智能运营中心报告：他们发现的，去重的恶意软件样本的数量有显著增加。这是 APT 正被研发或部署的信号。虽然，大型的、有很好防御措施的企业，例如 Google, RSA, Sony 和 Lockheed Martin 已经被攻击，但是有迹象表明，APTs 可能转向攻击那些小型的、没有被很好保护起来的组织，以实现他们最终目标。

图 1

高级持续威胁生命周期

数 据 ： Michael

迄今为止，已被发现的 APT 攻击的性质和被认为的目标显示 ,有政府参与其中。例如，Stuxnet 计算机蠕虫的目标是破坏伊朗的核武器研发。此外，被其它 APT 窃取的信息与情报的需求相关。这些情报涉及到即将进行的企业或政府的谈判和收购，或被作为一种获取攸关国家利益的资源的手段。

为了对抗 APT 威胁，重要是要了解 APT 攻击各阶段的差异性，以及对各阶段应采取的防御措施..

阶段 1：侦查

在 APT 的第一阶段，攻击者搜索企业网络和数据系统，寻找其中的薄弱环节。

在将恶意软件植入受害者网络时，最常用的技术是网络钓鱼。对攻击者来说，将注意力集中在企业员工身上会比试图攻破网络的边界防御更容易。当试图非法驻留于一台机器的时候，使用受感染的电子邮件和邮件附件依旧是种非常有效的手段。通过社交媒体传播也是用来获得在企业中驻留的一种有效手段。

为了使恶意邮件看起来更真实，以诱使收件人打开邮件， 攻击者利用从 Google, Facebook, Twitter, LinkedIn, 以及其他社交网络和公司网站获取到的公开信息来研究潜在的受害者（通常是高级管理人员，或者是能够访问敏感数据或拥有高级别权限的雇员）。地理位置也被越来越多的用于勾勒受害者的个人情况。这些数据不只有助于了解一个人的行踪，还有助了解此人的习惯和生活方式。有了这类信息，攻击者可以更容易的编写出一封与受害者的近期活动相呼应的，个性化的电子邮件。这大大增加了使受害者觉得这封邮件是来自于他/她认识的人的概率。

图 2

高级持续威胁的防御

数 据 ： Michael

所有这些都凸现了警示雇员在互联网上晒生活的危险性的重要性。个人信息的公共来源使得一个攻击者可以精心制作非常逼真的邮件。邮件中常常涉及近期的公司会议或收件人熟识的同事。

攻击者可能还有其他情报来源，例如电话监听和政府档案。重要的是要保证员工能了解最新网络钓鱼技术，并使他们能认识到他们的个人数据和地理位置数据是如何被泄露至公共领域并被滥用的。

阶段二：鱼叉式钓鱼

许多雇员，甚至是那些熟知安全的人，也会被诱骗打开一个邮件或邮件附件，或其中的链接。就侦查阶段而言，很难识别一个 APT 鱼叉式钓鱼邮件。更糟的是，一个攻击者也可以通过发送垃圾邮件来将真正行为隐匿在日常的噪声中，从而转移人们对真正攻击的注意力。

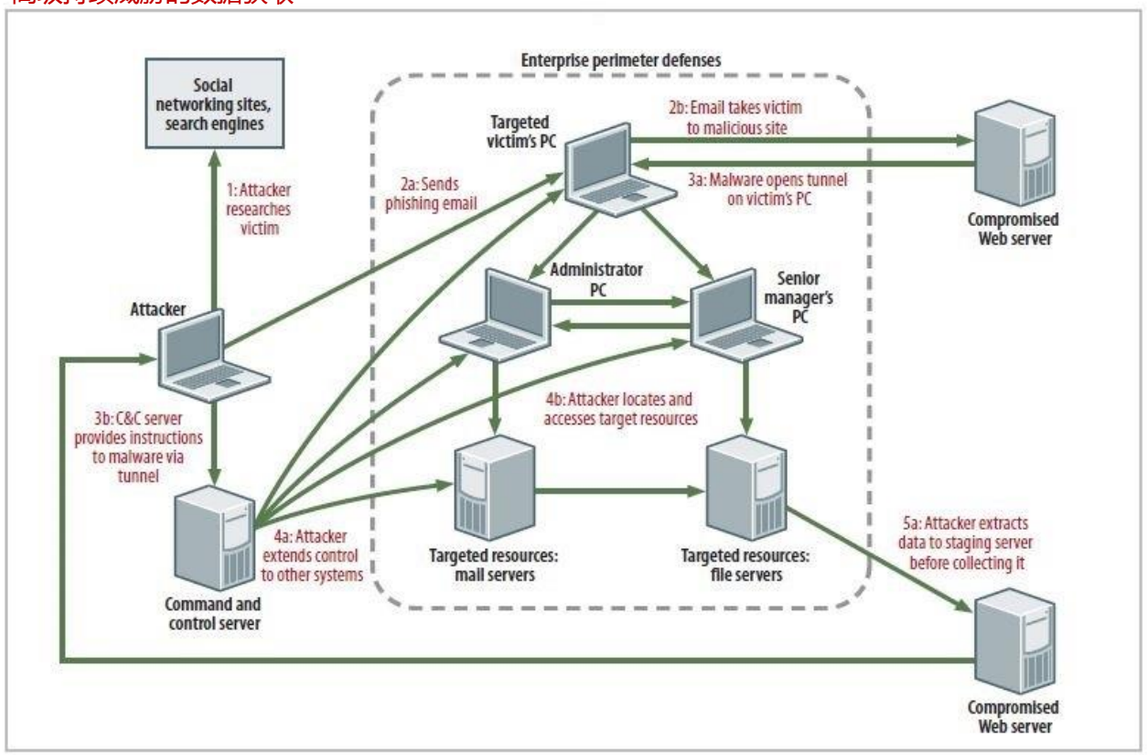
要想阻止攻击的脚步，就需要员工时刻保持警惕。你的主要防御方式是安全意识培训，这包括一个钓鱼攻击是如何工作的，如何和为什么某些员工可能会成为目标。在安保措施方面，员工应该接受培训和再培训，例如，在打开邮件前进行检查以确保它来自于一个受信的地方。是的，这些做法会在邮件交流上造成一些延误，但是它们也使得邮件更安全。随着对社交网络的使用的增加，员工也应该接受培训来谨慎对待他们的个人和企业帐户。重要的是，这些培训应该是持续的，以解决我们在公共社交网络上所看到的个人隐私和安全流程中的混乱（例如，Facebook）。员工也应该接受培训，上报任何可疑邮件，从而加强网络监控。

同样重要的是需安装邮件网关过滤，以及入侵检测和防护系统，并及时更新，从而使他们能够发现带有已知恶意模式的系统和网络行为。例如，对 RSA SecurID 的攻击涉及一个被称作 Poison Ivy 的自定义远程管理工具。它被嵌入在一个微软 office 文档中。Polson Ivy 已经被广泛用于许多其他的攻击中。

其他公认的攻击媒介包括，供应链的攻击（例如，选择 RSA 作为攻击目标是为能成功渗透国防承包商 Lockheed Martin）。检查服务水平合约是

图 3

高级持续威胁的数据获取



Data: Michael Cobb

否覆盖关联第三方对你的信息处理设施的管理（或访问）部分。你应该采取措施来检查附属第三方是否正在实施任何必要的安全措施。与第三方重新评估服务合约是一个很好的做法。这样能确保他们覆盖任何新的风险，并且确保他们的员工了解你的特殊安全需求。

阶段 3：建立据点

一旦攻击者感染了受害者的机器，就开始安装各种攻击工具和探索网络。企业往往不能识别出此类的行为，因为边界防御和流量分析倾向于集中在入站流量上。与此同时，攻击者使用的攻击工具往往是通过有效凭据安装的常用系统管理工具。因此，主机病毒扫描没能发现他们。APTs 倾向于使用常用的网络端口 80 和 443，并且大部分使用加密。进程注入和服务保持也被用来躲避监控。

由于 APT 事件的数量不断上升，攻击所造成的损害的严重程度和范围不断的升级，人们对 APTs 的关注正日益增加。

理想情况下，你应该监控内网和出站流量。因为在某些时候，已经安装的攻击工具需要对外连接。尽管 APTs 是定制开发的，但他们通常包含来自于已知恶意代码的代码段。这些是能够通过分析内网流量和主机信息（例如，注册表）来捕获的。当前已有的安全工具通常能完成这个工作。但是安全专家需要确保它们发现恶意代码后也能继续胜任，甚至对代码进行反汇编并分析。

阶段 4：搜索和跳板

合适的工具就位以后，一个攻击者可以开始分析网络布局和映射网络防御措施，搜索可能有助于攻击的已有的漏洞和程序。在一个装有 windows 系统的机器上，注册表、进程和开放的端口肯定会被检查。为了有助于分析，攻击者最有可能进行截屏、下载密码哈希、抓取流量，甚至可能窃听一个内嵌的麦克风。检查从这些活动中搜集到的数据，以便决定如何更好的行动：是静静的继续抓取数据，寻找更多的接入点和脆弱的系统，还是安装额外的工具以试图控制特定的资源。安全机构（包括 Mandiant 和 SANS）对被入侵的系统的分析显示，攻击者通常同时使用多个工具，这些工具经常发生变种以躲避检测。

但是，即便攻击会改变，目标也从来不会改变：秘密获取信息以便能够访问被更好保护着的数据。利用一个被攻陷的系统绕过防火墙和其他限制措施，以攻击同一网络上的其他系统的过程被称为“pivoting”。一旦完成“pivoting”，一个攻击者可能比系统管理员拥有更多的系统控制权。

IT 安全团队需要确定关键主机和网络资源，因为这些对任何攻击者来说都是主要目标。不同分类的数据应该被保护在不同的安全域中，此外，为了增加攻击者的难度，不同类型的数据应该被存储在不同的服务器中。例如，研发的文件不应该与主要收购计划存储在同一服务器上。

全面的日志纪录对发现和追踪一个入侵是至关重要的。例如，当一个 APT 使用一个零日攻击来攻克最初的主机时，我们可能是无法发现的。但是，通过网络探头记录和分析网络流量来发现异常行为，触发警报，可能会转而发现一个入侵。

为使你的安全团队能够针对一个特定网段调整的特点监控和告警，必须建立一个众所周知的，预期行为的基线。这样，异常的和潜在的恶意流量能被更容易的检测到。例如，由一个内网主机发起的，而不是为响应一个外部请求的端口扫描和流量输出会被标记，作为意外和可疑行为的即时指标。比通常的语句长 10 倍到 20 倍的 SQL 语句是另一明显的，恶意行为的标识。通常，这会是在尝试 SQL 注入攻击。在任何情况下，企业都需要知道什么是正常的，从而确定什么是不正常的。

重要的是记录所有系统的所有事件。企业应该考虑对所有 DHCP 和 DNS 服务器进行日志纪录，

对 VPN 集中器也是如此。此外，需确保 Windows 应用程序，系统和安全事件日志的大小适当，并以恰当的方式进行记录。基于主机的反病毒和入侵防御程序应具有事件记录功能，并记录所有内网流量。关键日志的汇集会使得在将他们整合进安全信息事件管理系统或 SIEM 系统时更容易些。照这样说，任何汇聚的日志的存储应该要完全安全。

安排一个新的安全审计以重新评估公司数据的风险，这对任何公司来说都是一个好主意（尤其是那些易遭受 APT 的公司）。审计将揭示现有保护措施的潜在差距，并强调对额外安全控制的需求。这些可能包括具有 SQL 语法分析功能的数据库防火墙和应用程序白名单。该名单能阻止自定义软件的运行并停止合法工具（例如 netstat）在非管理桌面上的运行。

如果检测到一个攻击，你最不想发生的事就是恐慌和匆忙进行无计划的匆忙响应。

最后，始终接受安全咨询服务，以使得你知道什么是你需要寻找的。

阶段 5：数据获取

攻击者为了能够使用他们细心收集到的数据，需要把数据传出网络。这个阶段的操作（数据提取或渗漏）对一个 APT 来说是最有挑战性的，因为数据需要以这种或那种形式传出网络。攻击者使用各种招数来完成这一任务，其中包括 peer-to-peer 网络，加密，onion 路由应用和信息隐藏。

防数据丢失技术能增加攻击者的数据提取过程的难度。可以通过设置 DLP 规则发送基于对外流量特性的警报，并终止特定类型的文件被全部传出特定网段。然而，因为这些攻击非常复杂，额外的出站流量分析是必要的。同样的，攻击者正在不断的监视和探索你的网络以达成他们的目的。你需要不断地审核正在传出你的网络的流量，以确保它们没有问题。

攻击者可能利用听起来无害的域名作为中转点，或使用 fast-flux 来绕过防御机制，例如基于 IP 的访问控制列表。这样会更难以辨认攻击者的自有网络，但是通过对 DNS 日志中此类流量的存在性的辨识能够显示入侵和可能的泄漏。

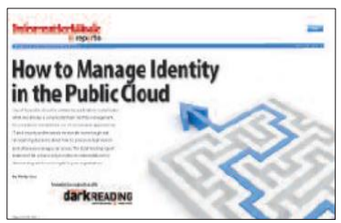
因为这些攻击已经伴随着恶意行为持续了一段较长时间，设备日志的集中可以帮助 SIEM 在不相关的和不连续的事件中找寻相关性。许多 SIEMs 基于预定义规则集，将设备置于一个监视列表中，对某些行为的自动分类，并对可疑主机增加审查。 具有可视化流量捕获功能的解决方案能快速凸现正在探测网络邻居，以寻找攻击者想要入侵的其他系统的、受感染的设备。

阶段 6：保持持续性

一个 APT 攻击需要耗费时间来全面探索和远程操控一个网络。这意味着，在几个月的时间里，攻击者必须对标准防御措施隐瞒他的存在。为攻击的下个阶段编写代码也是需要时间的，因为必须对该代码进行严格测试以确保它能正常工作，并且不会泄露攻击者的存在。对于攻击者这一方来说，这需要耐心。对于你这一方来说，这需要全面和常规的分析以试图在攻击者回传数据时抓住其突发的行为，并安装更新。

补救计划

如果你实现了对 APT 攻击的每个阶段的防御，长期消除薄弱环节，你将减少任何攻击在你的网络中成功立足的机会。如果检测到一个攻击，你最不想发生的事就是恐慌和匆忙进行无计划的响应。在 APTs 攻击时，你不能简单地安装最新的 AV 库并扫描受感染的以停止进一步的入侵。你也不能花费太长时间制定一个补救计划。如果你这样做，感染就会蔓延，危害将更大，修复其所需的时间将更多。这意味着你需要一个预先准备好的应急响应。一个高级经理(最好是在董事会层面)需要主持并为该补救计划负责。这



公有云中的身份管理

在企业应用中使用公有云使得本来就已经是一个复杂的任务的身份管理变得更加复杂。随着企业更多的使用基于云的应用，IT 和安全专家必须就如何采取措施 ,取消措施和在其他方面管理用户访问 ,做出艰难和深远的决定。本 DarkReading 报告探讨了多种方式 ,并就哪一种方式适合你的企业 ,提供了建议。

Download

将确保所有关键利益相关者的协调与合作。它还将确保给应急相应小组或 ERT 分配充足的资源。“做好准备”意味着有实时更新的企业架构文档，包括所有 DNS 和 DHCP 服务器列表、当前所有接入 Internet 的结点、VPN 集中器和 Windows 域，包括在每个 windows 工作站上启用组策略。

一旦了解清楚入侵的全部范围 ,就应该执行补救计划。团队辨识出所有被入侵的 APT 主机。ERT 应该由训练有素的安保人员组成。这些安保人员了解网络的架构 ,熟悉网络正常工作的时候应该是什么样的。这将使得辨识系统被入侵指标和区分 APT 与其他恶意软件变得更快和更容易。如果你没能拥有可用的内部人员，技术和能力来剖析 APT 入侵者使用的工具和技术，你可能很需要专业的外部帮助。如果你认定你的企业是 APT 的潜在目标，你需要开始与你的同行进行讨论 ,以决定如何更好的协同努力来对抗网络威胁。甚至可能有必要与政府机构建立联系，例如，美国网络司令部。该司令部的任务是协调美国军队合作对抗 APTs.

由于 APT 入侵的严重性和以及他蔓延到你的合作伙伴的潜力，不畏艰难、勇敢地面对危险攻击并在发生数据泄露后坦诚公布消息，是非常重要的。要让客户，企业利益相关者及监管部门了解最新情况。我们不得不尴尬的承认，这些攻击正成为 IT 领域的一部分 ,他们正在分享那些能够在其他方面使人更富有活力的经验。

MORE LIKE THIS

参考链接?

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：

数据库防御：对贵公司最敏感数据的最大威胁可能是那些拥有合法访问企业数据库的权限，但是没有合法意图的员工。虽然从内部发生数据泄露的事件有所下降，但是外部攻击经常效仿他们，并造成严重损失。请遵循我们的建议来降低风险。

了解软件漏洞：为了保护您的企业和用户数据，我们需要确定是什么使得它们如此脆弱和如此吸引攻击者。我们也需要了解黑客是如何行事的，以及他们依赖的工具和攻击流程。在该报告中，我们阐述了如何像像黑客一样思考，以及如何确定你自己企业数据料中最薄弱的一环，进而通过这两种方式来保证一个最好的防御方式

虚拟安全的四个步骤: 从访问控制到职责分离，我们展示了在你的虚拟环境中进行风险管理的四个关键步骤。

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。