企业网络犯罪威胁不断上升

非官方中文译本 • 安天实验室 译注

文档信息			
原文名称	The Rising Threat of Corporate Cybercrime		
原文作者	Trusteer	**原文发布日期**	
作者简介	Trusteer 是 IBM 公司(总部位于波士顿)的下属公司，开发了一系列计算机安全软件。Trusteer 于 2006 年成立于以色列，于 2013 年 9 月被 IBM 以 10 亿美元的价格收购。 http://en.wikipedia.org/wiki/Trusteer		
原文发布单位	Trusteer		
原文出处	http://buildingtrust.trusteer.com/Web_WP_-_The_Rising_Threat_of_Corporate_Cybercrime		
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。		

Trusteer

企业网络犯罪威胁不断上升

网络犯罪的动机和方法

新威胁,新思路

目录

完美犯罪

如果“完美犯罪”是指那种完全不会被发现的犯罪，那么企业网络犯罪是一个完美的例子。企业机构每天都在遭受入侵。他们通常完全不会发觉他们宝贵的企业信息资产正在被窃取。网络犯罪通常是安静的并匿名进行的，通过翻找企业帐户来寻找机密数据，随后无迹可循的溜掉，然后利用或售卖窃取到的信息以获取经济利益。

这种广泛的，协同的犯罪行为是通过利用大量的互联网，浏览器，操作系统的漏洞，以及很容易被网络犯罪技术攻陷的应用程序来实施的。网络犯罪分子已经发现，与直接攻击网络相比，攻陷雇员终端是一个进入企业网络的、简单得多的途径。未打补丁的零日漏洞使得网络犯罪分子能够在雇员终端设备上秘密安装恶意软件，并且实质上获得了同样水平的访问企业网络和雇员数据的能力。

“只有两种类型的公司：一种是已经被黑客黑掉的，一种是将要被黑掉的。甚至是被合并为一类：那些已经被黑掉的和将要被再次黑掉的。从长远看，维持代码的沉默并不会满足我们需求。”

联邦调查局局长 Robert Mueller

企业网络犯罪的价值

企业网络盗窃的例子比比皆是。在 2012 年 9 月，FBI 向美国银行发出警告：网络犯罪分子已经将恶意软件和键盘记录器安装在银行雇员的设备上以便获取雇员的登陆凭据。他们利用窃取到的平局来发起$400,000 到$900,0001 国际电汇欺诈。就是在去年 10 月份，FBI 在他的华盛顿办公区创立了一个新的小组，专注于知识产权盗窃案件以打击数量不断增加的网络犯罪。

政府机构报道，广泛的，受国家资助的企业间谍瞄准了各种行业，涉及高科技，医药，通信，金融服务，国防和（据 Bloomberg News，其价值超过 5000 亿美元）。被入侵的企业)。被攻陷的企业代表了名副其实的，高科技的世界。被攻陷的企业涉及 Google， Intel，Adobe，Pfizer 和 Abbott Laboratories。因为犯罪的匿名性本质，很难区分受国家资助的网络犯罪和“私人”网络犯罪。私人网络犯罪网络也积极窃取有价值的知识产权。

早在 2012 年，英国内部反情报和安全机构 MI5 的总干事，Jonathan Evans 透露 “与他们打交道的，主要的伦敦上市公司”已经因遭受国家资助的网络攻击损失了“大约“8 亿英磅”的收益。安全公司 McAfee 发现：“大约 1/4 企业有一个并购或一个新产品/解决方案展示因为一个数据泄露，或一个可信的、数据泄露的威胁而终止或延缓。”[2]

比知识产权被窃所导致的经济影响和敏感客户数据丢失更严重的由于没能充分保护宝贵的企业资产所导致的法律后果。投资者将越来越多的要求对因缺少足够安保措施而产生的漏洞所导致的损失进行赔偿。在给予所有有关企业网络犯罪的关注和告警的情况下，企业高管和高级职员也可能因为没能将正确的、最佳的防护措施部署到位而面临诉讼。高度受监管的行业也将因为没能正确评估与网络犯罪相关的风险并将适当的消除风险的技术部署到位而面临监管机构的愤怒。

“魔鬼最伟大的捉弄是让世界相信他并不存在”。

Charles Baudelaire

防范不可见威胁的困难

十多年来，网络犯罪分子已经瞄准了金融机构，他们通过攻陷金融机构用户的设备来访问网上银行帐户。在此期间，网络犯罪分子也已经悄悄瞄准企业资产。从一个用户的银行账户中窃取出金钱时，经常会被发觉。然而当网络犯罪分析从企业中窃取知识产权和其他敏感信息时，足迹不是那么明显，并且贼可能永远不被发现。

大多数公司完全无视网络犯罪攻击。绝大多数网络犯罪的受害者发现被入侵只是因为第三方通知他们（依据 Mandiant3 报道，有 94%的受害者如此，依据 Verizon4，有 92%的受害者如此）。一旦一个网络犯罪分子获取了访问一个企业网络的能力 检测到该入侵所用的平均时间为 416 天[5]。极有可能的是，有相当数量的入侵完全没有被发现。当入侵切实发生，网络犯罪分子通常花费超过一年的时间来窃取企业信息资产。

McAfee 发现：“只有十分之三的企业报告了所有数据泄露/蒙受的损失，而十分之一的机构只报告漏洞/他们在法律上有义务报告的损失，不会再报告其他。十分之六的企业目前‘挑选和选择’他们上报的漏洞/损失，选择标准取决于他们是如何看待这些漏洞的。“[6] 尽管有 2011 年 SEC 指引用于披露网络犯罪事件，但很少有公司这样做。[7] 这种趋势也反映在一个近期的 PricewaterhouseCoopers （PWC）调查中。 该调查涉及了 78 个国家的企业的 3877 名受访者，调查发现关于网络犯罪的最关心的问题是信誉损害 (40%的受访者这样表示)。[8] 这也就难怪企业人员会犹豫于是否公开披露网络犯罪事件布。不幸的是，这种上报的缺乏极大的阻碍了对企业网络犯罪问题普遍认知。许多企业高管没有意识到他们接触网络犯罪的程度，以直到他们成为受害者。

"我们不会与 Google 共享这个[漏洞]，即便 Google 出一百万美元。我们不想给他们任何信息以帮助他们修复这个漏洞或其他相似漏洞。我们想要为我们的用户保留该漏洞。"

Vupen 安全 CEO，Chaouki Bekrar

(在拒绝 Google 向其支付 6 万美元要求共享 Chrome web 浏览器漏洞后)

企业网络犯罪的方法

网络犯罪分子利用各种技术渗透企业网络。主要的方法是攻陷一个雇员的设备，窃取该员工的访问凭据，然后使用该员工的访问权限来辨识和窃取有价值的信息或直接发起欺诈性金融交易。几个安全厂商发布的年度和定期报告包含了有关网络犯罪方法和趋势的丰富信息，涉及 Trusteer 的所有博客，Symantec 的 Internet Security Threat Report，Verizon 的 Data Breach Investigations Report,，McAfee Threats Report 和 Sophos 的 Security Threat Report.

针对员工终端的网络攻击

有些针对企业的攻击是机会主义的（占大型企业遭受的漏洞攻击的 35%[9]），然而其他攻击是有高度目标性的（占大型企业遭受的漏洞攻击的 50%[10]）。以及各种新的目标攻击技术处于中间态（参见下面"watering hole 攻击"中的讨论). 除了新的感染，Trusteer 的研究发现，在任何时间点，所有 PC 中有将近 1%感染活跃恶意软件。网络犯罪分子并不缺乏企业目标。

网络钓鱼

对于引诱个人访问已经被攻陷的网站，以及诱骗个人下载受感染的文件来说，网络钓鱼仍然是一个有效的方法。尽管就点击陌生连接和打开可以文件的危险，有持续的警告，那些方法仍然是继续有效的。这并不完全归咎于最终用户：网络犯罪分子已经变得更善于掩饰自己的意图。

网络犯罪分子通常使用高度针对性的、鱼叉式钓鱼消息。利用网络上可用的信息(通过 Facebook，LinkedIn，Twitter 等等)或从熟悉的个人那里窃取的信息创建的，可以使受害者相信一个电子邮件是合法的。在 2012 年第一季度和第二季度之间，成功的绕过企业的安全防御的基于邮件的攻击上升到 56%。[11] 恶意邮件包含一个恶意文件，一个指向恶意网站的链接，或两者皆有。尽管进了最大的努力来培训和警告员工，网络钓鱼攻击依旧继续取得成功。

Web 威胁

基于 Web 的传播在入侵员工设备方面也是有效的。网络犯罪分子入侵合法的网站，建立专门的网站来托管恶意软件。通过各种手法，包括嵌入在钓鱼邮件中的链接，搜索引擎优化中毒，社交媒体诈骗（例如，Twitter，YouTube），假调查，免费礼品赠送，以及"must-see"视频，将受害者引诱到恶意网站。

一个称为“watering hole”攻击的新技术感染与目标公司、行业或地域相关的受害者。犯罪分子攻陷被认为是迎合特定受众的合法网站。例如，employees of a defense manufacturing plant 位于一个小镇的国防制造工厂的员工可能会乐于访问当地的新闻网站。因此，攻陷这个新闻网站可以使得网络犯罪分子直接发现国防制造工厂的员工。RSA 和 Symantec 近期都发现了严重以来该技术的大规模网络犯罪活动。[12，13]

托管恶意软件的网站的数量是惊人的。Sophos 的报告称每天有 30,000 个网站被感染，其中的 80%是合法的，被入侵的网站。[14] （WebSense 的数据是 82%[15]）。Symantec 在 2011 年，每天发现 9,314 恶意代码网站[16]，McAfee 的报告称，在 2012 年六月，每天发现 10,000 新恶意代码网站。当一个最终用户简单的浏览网页的时候，他的设备将被感染的可能性比以往任何时候都高。

利用系统中的漏洞

在网络犯罪分子诱骗受害者打开一个恶意邮件的文件附件或访问一个受感染的网站，网络犯罪序列中下一个步骤是用恶意软件感染终端。在发现和利用系统漏洞，以便用恶意软件感染雇员的终端设备并同时躲避安全控制手段方面，网络犯罪分子已经高度熟练。企业每星期平均收到 643 个成功绕过企业安全防线的，基于 web 的感染事件。[18] 毫不奇怪的是，近期的调查表明 74%的 IT 和安全专家相信他们的端点安全（他们的笔记本电脑和台式机）是无效的。[19]

软件漏洞

漏洞是指由于设计上的缺陷或编码错误而导致的软件代码弱点。它使得攻击者可以危及底层系统。 Open Source Vulnerability Database 在 2011 年对基于 web 的系统，应用程序和计算工具的 6,843 个漏洞进行了分类（Symantec 利用 DeepSight 漏洞数据库上报了 4,989 个新漏洞[20]）。虽然，与 2010 年相比，漏洞的数量下降了 19%，高危漏洞的数量一直在上升，现在占据所有上报的漏洞的 24%。高危漏洞是指那些会允许对底层系统的根级别的入侵。

软件漏洞使得网络犯罪分子可以绕过阻止未授权文件安装的安全控制（嵌入在操作系统中或第三方提供安全应用提供的）。微软报告称，在 2011 年上半年披露的漏洞中应用程序漏洞占 70%。剩下的漏洞大致是操作系统和浏览器各占一半。请注意，浏览器和浏览器组件漏洞并不包含在应用软件漏洞的计数中。

漏洞利用

漏洞利用是指一段代码，该代码被设计来利用软件漏洞传输一个会被系统的限制阻挡住的负载（恶意软件）。为了对抗这种威胁，软件供应商疯狂的工作，通过给漏洞打补丁来阻止这些漏洞利用。IBM 报告显示，在 2011 年，所有已知漏洞的 11%有公开可用的漏洞利用代码[22]。将近 91%的漏洞在被公开披露出来的同一天打上了补丁[23]。剩余中的大部分在几周内被打上了补丁。

但是，补丁的可用性不能确保它被安装在最终用户的设备上。最终用户或管理员必须不断的与典型用户设备上使用的各种软件程序的新补丁的信息同步。采用不一致的补丁导致将近 2.7%的微软程序和 6.5%的第三方程序在任何给定的时间里保持没有打补丁的状态。[24] 在乘以数百万用户，这些数字表明，众多的人经常遭遇网络犯罪分子的漏洞利用。

虽然 ,打补丁的统计数据可能看起来并不令人担忧 ,但是他们不反映漏洞和漏洞利用的真正的、潜在的生命周期。特别危险的利用未披露的漏洞的零日漏洞攻击。由于零日漏洞攻击利用目标未知的（并因此未打补丁)漏洞，因此对它们几乎没有防御。

许多人错误的认为，零日漏洞所造成的威胁是有限的，因为被披露出来的漏洞被很快的打上了补丁。然而，近期的研究表明，在漏洞被公开披露之前，攻击者经常会长期利用漏洞，这是由于零日漏洞平均会持续至少 312 天 [25]。也就是说，在任何防护措施就位前，网络犯罪分子能够利用未知系统漏洞来成功的感染终端长达 10 个月。同样的研究也表明，在漏洞被公开披露后，网络犯罪分子立即增加漏洞利用的次数到 2 至 100,000 倍，以便在漏洞被修补好以前尽可能多的感染机器。

对于攻击者来说，发现一个零日漏洞的价值和开发一个漏洞利用程序是有利可图的。一篇最近的 Forbes 文章探讨了零日漏洞的地下市场 。该市场专门提供最新版本的软件的漏洞（参见图 1）。仅仅在微软发布 Windows 8 的一星期后，法国安全公司 Vupen 声称，他们有一个可用的黑客程序（对于 Internet Explorer 10 也是如此)。零日漏洞的价值显示了从网络犯罪中实现的经济收益。

ADOBE READER	$5,000 - $30,000
MAC OSX	$20,000 - $50,000
ANDROID	$30,000 - $60,000
FLASH 或 JAVA 浏览器插件	$40,000 - $100,000
MICROSOFT WORD	$50,000 - $100,000
WINDOWS	$60,000 - $120,000
FIREFOX 或 SAFARI	$60,000 - $150,000
CHROME 或 INTERNET EXPLORER	$80,000 - $200,000
ISO	$100,000 - $250,000

图 1: 黑市上各种零日利用的售价

来源: Forbes, 2012 年 3 月 23 日

令人不安的是，犯罪分子不必只依赖于开发漏洞利用程序以用于新发现的漏洞。因为用户在安装修补严重漏洞的安全更新方面一直做的不好。在发布一个漏洞补丁后，许多漏洞利用程序还会持续有效达几个月或几年。例如，自一个 Microsoft Word 更新发布的一年内，有 39%的计算机没能安装它。自一个 Adobe Flash Player 更新发布的一个月内，70% 的计算机没能安装它 [26]。这种滞后使得网络犯罪分析可以在几个月，有时是几年中持续的使用现存的攻击方法来对抗被修补的漏洞。

感染终端

感染一个端点的过程远比简单的直接下载一个恶意软件二进制文件到终端上复杂得多。这个过程通常涉及下载 dropper 二进制文件来修改设备配置和安全设置，安装一些恶意软件组件，然后访问 最新的犯罪软件套件。该犯罪软件套件安装和更新主要的恶意软件代理。然后，该恶意软件代理定位命令和控制服务器，并与之通信。该服务器管理攻击配置和接收入侵后所获取的信息。这种复杂的方法被设计用来最大限度的躲避安全控制和安装最有力的恶意软件。

网络犯罪分子越来越多的依靠漏洞利用工具包（例如， Blackhole），即主动的扫描一个用户的设备以来寻找各种漏洞，然后安装相应的 dropper 文件来利用该漏洞。如果它没有发现漏洞，该工具包就什么都不做。Dropper 文件是动态创建的，因此大多数反病毒应用程序使用的已知技术（特征和模式匹配）不能发现他们。为了躲避检测，与命令和控制服务器的通信越来越模糊，有时是通过 Twitter，Voice over Internet Protocol (VoIP)，或其他开放的通信信道进行的。

与零日利用有关的是零日漏洞恶意软件。零日利用将那些位置的系统漏洞作为目标。零日恶意软件是指那些尚未被确认的、新的恶意软件种族。零日恶意软件有两种形式：零日恶意软件容器（一个以前从来没见过的文件）和零日恶意软件犯罪逻辑（一个从来没见过的恶意软件攻击算法）。基于特征的反病毒应用程序不能检测零日恶意软件容器，因为他们必须将其与之前发现的恶意软件容器匹配。网络犯罪分子很容易就能利用一种称为多态的技术生产出同一个恶意软件容器的数以百万计的新变种。更为危险的是零日恶意软件犯罪逻辑— 新的，之前未见的恶意软件算法。该算法要求网络犯罪团伙进行实际的设计和编码— 一种完全不同级别的工作。

网络犯罪分子还能够通过其他方法感染用户终端。例如，用户越来越多的使用在网站和文件共享站点上发布的非官方的软件。犯罪分子经常将恶意软件嵌入进那些用户很可能通过这些站点访问的盗版软件，电影和音乐文件中。恶意软件已经被发现预装在零售卖场中售卖的计算机上，以及在媒体存储设备中。总之，并不缺少感染终端的方法。

Trusteer 最近对大型企业的终端设备的分析证实商业恶意软件的广泛存在（参见图 2）。局域网（LAN）安全网络通常显示，每 1000 台设备就有一台被感染高级恶意软件；如包括你自己的设备（BYOD）/家用电脑，该比例在 1:500. 然而，几家大型企业用户在 LAN 安全网络中的感染比例在 1:100。这些数字代表了一个关键的风险水平（假定一个被入侵的设备能够向网络犯罪份子提供破坏性的访问）。

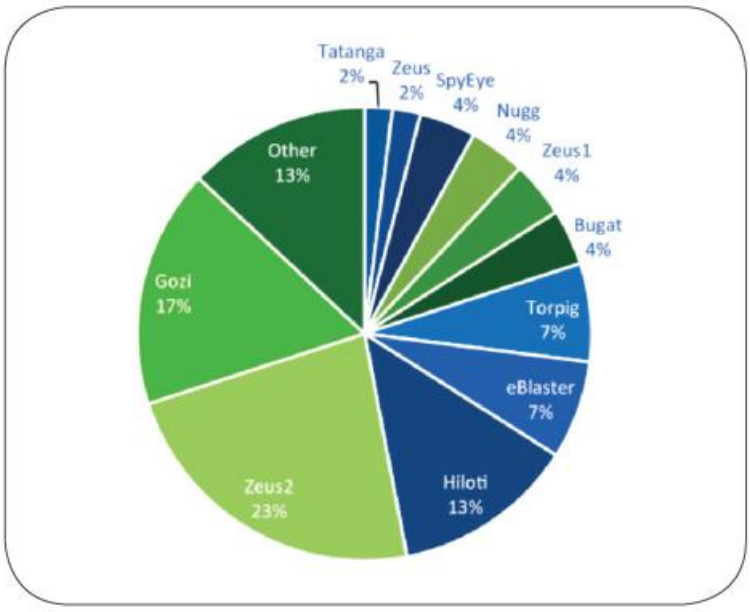

图 2：一个典型恶意软件家族在在一个大型企业的员工终端上的感染分布情况

来源：Trusteer, 2012

终端防护

2012 年 ,企业和消费者将在防病毒软件上花费超过 80 亿美元 [27] ,以提供一定程度的终端防护，抵御网络犯罪份子的攻击。已有的两个主要防护方法可以大致分为设备防护和网络防护。这两种方式都主要是试图辨识以及在恶意软件被安装在终端上之前，删除恶意软件相关的文件（droppers，犯罪软件包，恶意软件容器等等）。

设备防护

设备防护应用程序（通常被称为反病毒或 anti-X）被安装在终端上。在那里，它们扫描所有被安装（或一些）的文件，以及在新文件安装前评估他。设备防护方法主要使用基于特征的方法，将需要评估的所有文件与已知恶意软件文件配置相比照。虽然，设备防护能够有效的对抗已知病毒，广告软件和通常的“nuisance-ware”攻击，但是这个方法已经被证明对更高级恶意软件是无效的。

正如上面提到的，犯罪份子利用多态来不断改变恶意软件文件的表相，专为逃避给予特征的恶意软件检测。网络犯罪份子还是用偷来的的或伪造的证书来使恶意文件呈现为一个合法应用或更新。一旦恶意文件被下载，就已经太迟了，设备防护应用程序不能发现恶意软件。即便应用程序特征数据库被更新为包括一个已经被安装在机器上的恶意软件文件，那也太晚了。

不幸的是，多态只是现代恶意软件用于躲避终端检测的几种技术中的一种。例如，Shylock（在 2011 年，被 Trusteer 首次发现的一个恶意软菌株 [28]） 和 Tilon （Trusteer 在 2012 年 9 月发现的一个新恶意软件菌株 [29])将恶意代码注入进各种原生的 Windows 进程中，然后自我终结。这样，在那以后，内存中就找不到恶意软件进程。为了能够系统关闭后依旧生存，在所有其它应用程序关闭（包括反病毒程序）后，系统完全关闭之前，恶意软件 hooks 到 Windows 关机过程中，以便能够恢复重新安装所需的文件和注册表键。一旦这些恶意软件被安装，它们不大可能被任何防病毒程序发现。

一些设备防护程序开始使用一种被称为沙箱的技术在一个虚拟环境中执行可疑文件，以便察看该文件是否呈现类似恶意软件的行为。沙箱的目标是在机器上创建一个孤立的环境。在允许可疑文件执行前，可以在该环境中对其进行安全的测试。正如所预期的那样，高级恶意软件现在有能力检测一个虚拟机环境（正如在下一节中讨论的那样）并因此采取躲避措施

虽然理论上是合理的，但是沙箱充满问题。因为它是一个软件平台，它有可被利用的漏洞。最近的一个例子是 Java 零日攻击，它突破了 JVM 沙箱的访问控制。此外，一个沙箱通常需要向用户提供一些途径来从沙箱中导出内容到底层设备，恶意软件可以在那里进行攻击。

网络防护

网络防护方法试图在恶意代码或可疑文件被从 Internet 下载到接入企业网络上的终端设备上的时候，辨识出它们。就像防病毒应用程序那样，与已知恶意软件特征匹配的文件被阻止下载到一个终端设备上。如前所述，犯罪份子通常利用多态绕过这个技术。

许多网络防护方法利用虚拟机环境在一个隔离的环境（类似于沙箱，但是没有终端设备）中运行可疑文件来辨识恶意软件。然而，一些恶意软件种族可以检测虚拟机环境的执行，然后逃避检测。例如，恶意软件能检测某些注册表项，进程名字，或鼠标和视频驱动器（通常在虚拟机上没有这些）。然后，恶意软件可以通过不运行或将自己表现成其他东西来躲避虚拟机检测。另一种逃避的策略是，当他被监控的时候，简单的睡眠一段时间来躲避运行。睡眠帮助恶意软件躲避虚拟机检测，但是在一个合法的终端用户设备上，这只能推迟而不能避免。

网络防护只有当终端设备被接入企业网络时才起作用。用户经常在离开企业网络的时候，使用他们用来访问企业网络的设备去访问互联网（例如，当他们在家或在旅途中）。离开企业网络后被感染的设备是一个盲点，因为网络防护应用程序不能扫描设备，寻找恶意软件。

当前终端防护方法的启示

除了拥有并不理想的威胁检测能力，当前终端检测方法是资源密集型的。上述方法通常将文件判定为可疑，然后需要人为干预来做进一步的分析。取决于检测应用程序时如何调教的，它们会产生大量的误报 （文件被错误的判别为恶意的）。此外，一旦上述方法辨认出恶意软件，该恶意软件必须从终端设备上完全删除。这通常需要一个额外的，不便捷的步骤，即一个安全专家必须访问终端设备以确保威胁被完全清除。

新的防护层

显然，当前终端防护方法是落后的。随着网络犯罪份子持续提升他们的能力， 什么是能够被检测到的和什么是完全不可检测到的之间的差距正在扩大。在企业勉励不可挽回的损失之前，迫切需要一个新方法来打击网络犯罪的上升所造成的冲击。

营运假设

要定义一个新的防护层的要求，我们必须先定一个当前的营运环境。下面的营运环境假设（即便没有被普遍接受）为创建一个克服现有方法的弱点的新护范例提供了一个保守的基础：

终端用户不能被教导来避免恶意软件感染。人类犯错和感染的途径也越来越隐秘。

- 尽管做了所有最好的软件设计和测试工作，软件漏洞也将会不断出现。无休止的软件补丁是常态。
- 网络犯罪份子将继续开发新的方法以躲避在整个感染路途中的检测。
- 终端恶意软件感染的数量将持续升高；当前的终端防护方法跟本无法跟上时代的步伐。

最后的防线

如果企业不能防止终端遭受高级的、危险的、具有躲避能力的恶意软件的感染，那接下来给怎么办？ 难道他们会投入更多的钱和更多的防护解决方案在该问题上，期望看到更多的检查导致更多的检测？或者，他们认识到他们需要一个新方法，新途径来看待恶意软件问题？

如果基本的营运假设是：恶意软件将感染终端设备，企业必须找到一种方法来在恶意软件产生危险前检测和移除它。只有当恶意软件在终端设备上执行的时候，才能够导致伤害。一旦恶意软件执行，它就暴露出它是什么。虽然我们不能完全防止恶意软件感染设备，但是我们肯定能决定恶意软件什么时候在设备上运行（如果我们知道寻找什么）。这意味着要进行实时地、持续的设备监控来发现活跃的恶意软件威胁以及重要的、具体确定的、企图攻陷关键企业资源的威胁。

防护手段必须着眼于捍卫特殊的，对敏感企业资源的访问的终端应用程序，例如，应用程序平局或业务数据。企业可以忽略其他应用程序以便减少噪声以及与试图使整个端点抵御各种可能的威胁相关的系统资源。只考虑针对那些已定义的企业资产事项的威胁。

什么样的活动可能会暴露恶意软件的存在？一种是辨识对应用程序内存，进程和应用程序接口（APIs）将提供无限制的，对应用程序功能和通过该应用程序的数据流的访问）的任何篡改。例如，许多高级威胁使、用浏览器篡改。通过篡改内核浏览器功能（内存修改），恶意软件能获得控制权，以在任何时间将一个网页加载到浏览器中，并观察和修改它。

对于监控器，另一种与恶意软件相关的活动是通过键盘记录器捕获凭据和敏感数据，或记录用户的显示活动，该活动能够绘制出应用程序工作流， 商务过程和敏感数据的位置。总之，实时应用程序防护在恶意软件正利用任何手段攻击应用程序时，当场捕获它。

最后，一旦辨识到可疑行为，这个新的防护层也提供补救补救措施。该威胁必须立刻被删除或禁用，这不仅是防止被窃也是防止该威胁采取躲避行动（例如，写文件和注册表键值，以便在被删除后重新安装自己）。该方法更为有效，符合成本效益，并且用户使用起来，比使用一个独立的恶意软件修复程序感觉更友好。

结论

企业终端遭受攻击。网络犯罪份子已经开发出巧妙而有效的方法来安装恶意软件到终端上，从而有效的从终端用户那里窃取所有的控制。而且，没有证据表明，这些攻击即将减缓下来。与所有软件应用程序有关的关键系统漏洞一直是个持续的问题并将一直持续下去。流行的防御技术已经提供了一些防护以抵御最明目张胆的攻击，但是对更高级的威胁的效用不大。迫切需要一个新的终端防御方法。

企业和技术领导者必须认识到，他们处于一个网络战争之中。网络犯罪份子正在从企业的意识缺乏中掠夺，并且积极地从事不大可能被发现（甚至永远不被发现的）秘密企业间谍活动。企业领导者企业将继续忧疑为什么一个新入行的企业开发有竞争力的产品会如此迅速，为什么另一个供应商似乎总是提供一个稍微优惠一些的价格，或企业的敏感信息是如何被泄露给新闻界的。

消除网络犯罪的关键是移除恶意软件。移除恶意软件的关键是与他正面交锋。企业必须在它在终端上立足的那一刻根除它，并且摧毁它。恶意软件已经躲避了所有其他的防御，但是在它运行的那一刻，它就暴露了自己。终端应用程序防护被设计来做其他方法不能做的事：检测活的，运行中的恶意软件并且从终端上移除它。它是最后一道防线。

关于 Trusteer

总部位于波士顿的 Trusteer 是终端网络犯罪防护解决方案的主要的供应商。该方案防止企业遭受金融欺诈和数据泄漏。数百个企业和数以百万计的最终用户依靠 Trusteer 来防护他们的计算机和移动设备，使其免予遭受那些对传统安全解决方案不可见的网络威胁 Trusteer 的 Cybercrime Prevention Architecture 与多层次安全软件和实时威胁情报系统相结合，挫败零日漏洞恶意软件和网络钓鱼攻击，协助企业符合合规性要求。知名企业，例如 HSBC，Santander，The Royal Bank of Scotland，SunTrust 和 Fifth Third 都是 Trusteer 的客户之一。

详情参见：www.trusteer.com

1. www.ic3.gov/media/2012/FraudAlertFinancialInstitutionEmployeeCredentialsTargeted.pdf , accessed September, 17, 2012
2. *Underground Economies*, McAfee, SIAC, March 2011
3. *Mandiant M-Trends*, 2012
4. *Verizon 2012 Data Breach Investigations Report*
5. *Mandiant M-Trends*, 2012
6. *Underground Economies*, McAfee, SIAC, March 2011
7. *CF Disclosure Guidance: Topic No. 2*, Division of Corporation Finance, Securities and Exchange Commission, October 13, 2011
8. *The 2011 Global Economic Crime Survey*, PWC, November 2011
9. *Verizon 2012 Data Breach Investigations Report*
10. *Verizon2012 Data Breach Investigations Report*
11. *FireEye Advanced Threat Report*, 1H 2012
12. *The VOHO Campaign: An In Depth Analysis*, RSA FirstWatch Intelligence Report, September 2012
13. *The Elderwood Project*, McDonald, O' Gorman, Symantec, September 2012
14. *Sophos Security Threat Report 2012*
15. *Websense Threat Report 2012*
16. *Symantec Internet Security Threat Report, 2011 Trends*, Volume 17
17. *McAfee Threats Report: Second Quarter 2012*
18. *FireEye Advanced Threat Report*—1H 2012
19. *2012 Bit9 Cyber Security Research Report*
20. *Symantec Internet Security Threat Report, 2011 Trends*, Volume 17
21. *Microsoft Security Intelligence Report*, Volume 13, June 2012
22. *IBM X-Force 2011 Trend and Risk Report*
23. *IBM X-Force 2011 Trend and Risk Report*
24. *Secunia Yearly Report 2011*
25. *Before We Knew It, an Empirical Study of Zero-Day Attacks in the Real World*, Bilge, Dumitras, October 2012
26. *Microsoft Security Intelligence Report*, Volume 13, June 2012
27. Wired.com, *Is Antivirus Software a Waste of Money?*, March 2, 2012
28. Trusteer Blog, *Merchant of Fraud Returns — Shylock Polymorphic Financial Malware Infections on the Rise*,February 15, 2012
29. Trusteer Blog, *Tilon — Son of Silon, August 9*, 2012