弥补攻击检测领域的空白

非官方中文译本·安天实验室 译注

文档信息			
原文名称	Closing the Breach Detection Gap		
原文作者	Triumfant	**原文发布日期**	
作者简介	Triumfant 使用粒度变化检测和专利分析方法，以发现、分析和修复端点计算机上的恶意攻击，不需要事先了解攻击。Triumfant 不需要任何先验知识，如特征，能够检测高级持续性威胁、零日攻击、规避传统保护措施的其他恶意软件。 http://cn.linkedin.com/company/triumfant-inc?trk=tabs_biz_home		
原文发布单位	Triumfant		
原文出处	http://www.triumfant.com/pdfs/White_Paper_Closing_the_Breach_Detection_Gap_v11.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	• 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。		

弥补攻击检测领域的空白

概述

经验丰富、目的性明确的攻击者正在穿透最好的防御措施。我们清醒的认识到，各个机构并没有在攻击检测方面作好准备或武装。防御工具和取证工具之间存在着一个相当大的空白。这使得企业无法快速的检测攻击，并提供具有可操作性的信息，以满足快速响应行的需求。Triumfant 能够检测那些规避防御软件的工具，这种能力填补了这一检测领域的空白。它向企业提供了快速检测和响应工具，使企业能够有效地应对漏洞攻击行为，并尽量减小企业和企业声誉所面临的风险。

本白皮书中采用的数据来自于几个被 IT 安全行业广泛认可的研究报告。每一个都在脚注中进行了标注。本白皮书基于“presumption of breach”学说，并不试图建立或论证既定企业具有一个漏洞的概率。在被引用的报告以及其他可信数据源中的，有关于上报的漏洞的丰富的数据表明，企业正在遭受侵害。因此，本文着重关注企业在被攻陷时所面对的挑战重点或一个能够快速检测漏洞并创建一个恰当的以及同样快速的响应的解决方案。

攻击检测领域的空白

您将被攻陷

上报的漏洞数量正在升高，而且这种趋势并无减缓的迹象。业界发布了几个非常可信、详实的漏洞研究报告。这些研究报告中的综合数据显示漏洞不因企业规模的大小和行业的不同而不同。此外，最具吸引力的攻击目标是那些拥有貌似高水平的技术能力和安全敏锐性的企业。这是关键的一点，因为企业承受不了因采取“这不会发生在我身上”的态度和忽略证据所导致的后果。

图 1 中的图表展示了许多 IBM 安全系统研究的漏洞。漏洞范围之广使 IBM 宣称 2011 年是“漏洞年”。[i]

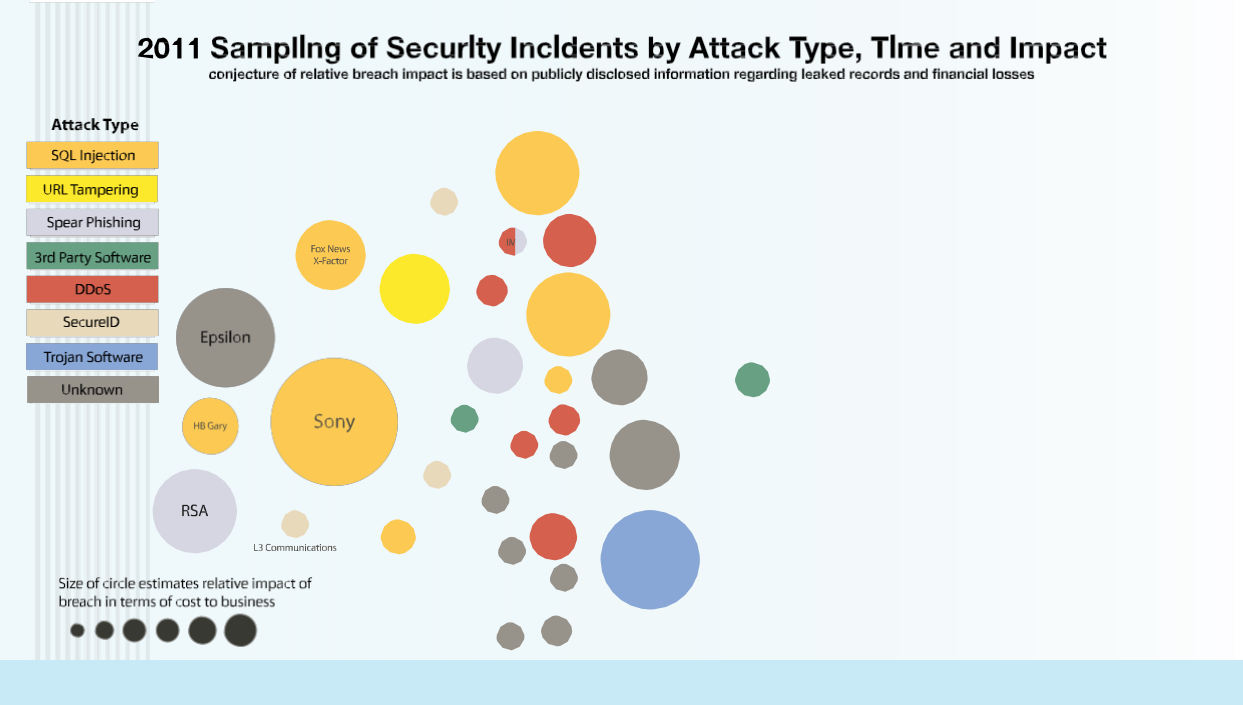


图 1: 2011 年漏洞样本

制造漏洞攻击从未如此简单。开放的市场中有大量的远程访问木马（RAT）和提权工具。他们易于使用，能够攻破防御壁垒。在 M-Trends Annual Study 中，取证技术厂商 Mandiant 指出，在他们研究的案例中，有 77%的攻击者使用公开可用（现成的）的恶意软件。[ii] 这表明，攻击者能容易的规避防御软件，即便是在攻击中使用了已知的恶意软件。其次，有目标性的攻击并不要求攻击者动用大量的资源以及使用一个零日漏洞攻击。第三，恶意软件经常利用在几个月或者几年前就已经被发现的已知漏洞，这表明漏洞被迅速发掘，但是慢慢消亡。Shmoocon 2012 的一个演讲中，展示了躲避白名单工具（最新的一劳永逸的解决方案之一）的六种方法。越来越多的和明确的证据表明，企业只能采取漏洞假设原则：假设企业将会被攻陷，然后为快速检测漏洞和发起一个及时的和做之有物的响应做好准备。

定义攻击检测领域的空白

经验丰富、目的明确的攻击者正在穿透最好的防御措施。这使绝大多数企业都面临一个直接的和严峻的问题：我能够检测一个漏洞么？ 证据表明并不能。

- Trustwave 的 2012 年全球安全报告指出，他们报告中研究的漏洞存在于被攻击的企业网络中而未被发现的时间为平均 173.5 天。[iii] Verizon Business 的 2012 年数据泄露调查报告（DBIR）指出，在他们研究的漏洞中，有 85% 藏匿了一个星期或更多时间而未被发现。55%藏匿的时间超过 30 天。[iv] 这些是被*检测*到的漏洞的平均数。
- Verizon Business DBIR 调查了超过 850 个漏洞。其中的 92%是被第三方发现的，而不是被受影响的企业发现的。[v] 在那些被认为拥有最好的漏洞检测能力的大型企业中，只有 16%的漏洞是被通过主动发现模式检测到的。[vi] 数据表明，人们对漏洞检测存在侥幸心理—客户或合作伙伴这一异常行为吸引取证研究。

企业无力检测漏洞的原因很容易解释。如图 2 所示，在多层防御解决方案和取证工具之间缺少了一个关键的部分。这使得企业不能在被入侵的那一点上检测漏洞。

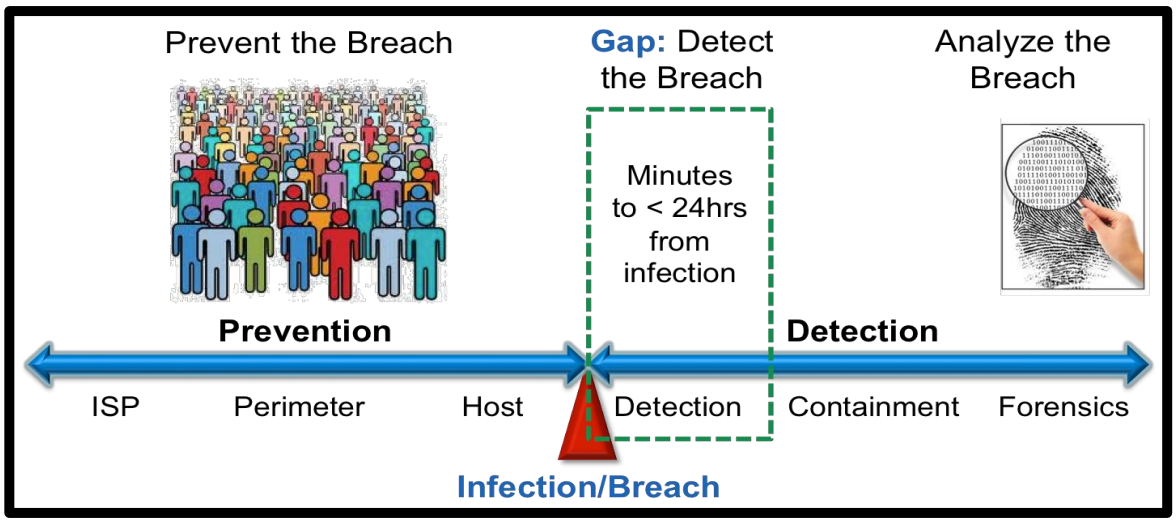


图 2.漏洞检测领域的空白

防御（在攻击攻陷目标前阻止它）是 IT 安全行业的焦点，尽管人们很清楚的认识到，以防御为中心的策略是注定要失败的。对防御的偏好甚至依旧驱使企业投入预算来研究下一代万无一失的防御技术。谍报技术残酷、快速的发展以躲避防御软件的任何捕获。有针对性的攻击被设计来躲避那些对防护他们的攻击目标来说特效的防御措施（以隐喻的方式形容该恶意软件就是“子弹上面有你的名字”）。

企业投入了很少的预算。资源都被用于处置入侵（攻陷）发生后的事情，历史上建设的重点是放在取证工具上。这些工具为漏洞攻击调查过程提供了深刻的见解和有价值的分析。但是，这些也只能在检测到漏洞攻击后才派上用场。如果没有很好的检测能力，那就意味着企业正在将他们的“后”攻陷（post-infiltration）预算使用在那些被用于分析漏洞的工具上。而这些漏洞在企业的网络被入侵后存在了 173.5 天（平均）。

该漏洞检测手段的缺失处于防御工具和取证工具之间的临界点。这使得企业没拥有必要的，实时检测漏洞的手段。显然，没有检测就不能及时响应。企业需要一种工具，该工具可以在被入侵的时间点上检测到漏洞，并且在检测的时候产生尽可能多的取证信息，并使企业能够立即采取行动以阻断攻击和修复机器。

这种空白所导致的后果

企业的这种无力于快速的和准确的检测漏洞的现状直接方便了当今的那些正在寻求对关键信息系统进行长期、不间断入侵的攻击者。过去的那种强行攻占的策略已经被替换为耐心和持久的方式，攻击者通过一个高质量的隐身和长期的访问来实现攻击的目的。当一台机器被入侵，攻击者将采取措施来模糊攻击的证据和他们在该机器上的存在感。攻击者通常遵循一个深思熟虑的，耐心的原则（称为“low and slow”），以之做为指导思想来实现目的并使暴露的风险最小化。攻击者可能已经投入很多时间和资源来创建攻击，因此他们更乐于等待时机以避免被发现。

一些精心设计的攻击有多个步骤，每一个步骤都必须被执行以实现最终目标。这些步骤被称为一个杀伤链（kill chain）。尽管最近的防御技术已经迫使攻击者减少命令和控制的频率，但在整个攻击过程中，攻击者通常能够持续监控和控制攻击的进展。Verizon Business 的 DBIR 指出，他们研究的 71%的漏洞攻击有两个或更多的步骤， 漏洞攻击的步骤平均有近三个（2.9）阶段或步骤。[vii]

在某些情况下，被入侵的机器并不是攻击的最终目标，而是他们进入网络的最初的立足点。例如，终端机器被用来做为进入存储着目标数据或知识产权的服务器的中转站。在这些情况下，攻击者通常将键盘记录器安装在入口点的机器上以获取访问凭据，继而移动到其他机器上。具有有效凭据的横向移动可以使躲避检测的攻击者受益。

精心设计的威胁被用于持久性（攻击者创建机制在攻击被发现时重起攻击，在命令和通信被中断时恢复他们）。攻击者通过很多不同技术获得持久性，但是他们的目标是相同的：确保攻击持久地留存于机器中，一直到实现目标。2011 年 10 月，对美国的无人机指挥和控制中心的攻击就是个很好的例子。一旦攻击被发现，被植入到受影响网络中的持久机制就会持续重复感染系统 ，尽管人们在努力修复受感染的环境。[viii]

这种空白所导致的企业风险

拥有恶意软件的第三方长期的，秘密的潜伏于企业网络中是无任何好处的。其中的原因是显而易见的：持久性和秘密性为攻击者提供了必要的时间，以使其完成对目标的攻击。由此带来的风险是多方面的，其后果是毁灭性的，而长期的影响力能对企业产生重大冲击。每晚发现漏洞一天，都会增加企业的风险。

企业风险维度	
财务	**信誉**
来自 Online Trust Alliance 的研究报告表明，558 个漏洞平均造给受影响的企业造成了 720 万美元的损失。[ix] 2011 年，8 月 5 日，10Q 领域，RSA 的母公司 EMC 宣布为在 2011 年 3 月爆发的 RSA 漏洞一次性付出 6630 万美元。该漏洞最终影响了超过 700 家企业，据报道，银行业的损失超过 1 亿。[xi] 据报告，索尼已经为他们多次出现的漏洞付出了 10 亿美元。	没有一家公司希望由于漏洞而登上华尔街日报的头版。漏洞对声誉的影响可以削弱公司客户的信任，在商务环节中增加客户的流失（商务环节中的客户流失是一个正常的因素）。难以用简单的钱数来衡量信誉的价值。但，结论就是企业更希望避免负面的，与高影响力漏洞相关的宣传。
估值	**生存**
经济损失和信誉影响能最终影响公司的股值。一项评估指出，索尼的安全问题负面冲击了索尼 6%的估值。[xii] 公平的说，没有具体的证据表明漏洞能对估值产生长期影响。例如，在被公开一个漏洞之后，Heartland Systems 的估值已经反弹。有研究已经将其中的短期的因果关联起来。可以肯定的是，公司更希望避免对估值的冲击，即便只是暂时的。	2011 年，几家公司付出了最后的代价。漏洞攻击成为了公司停业的催化剂。 最明显是证书颁发机构 DigiNotar。2011 年九月，在被爆出被漏洞攻击攻陷后，该公司关闭了运营。

表 1：企业风险维度

设计一个攻击，渗透进网络，藏匿在网络中不被发现，其中所需要付出的精力是非同小可的。因此，这些行为必然有一个最终的目标。企业的风险和最终结果直接与攻击的目标相关联，他们可分为几类：

- 数据泄露。这些攻击寻求窃取那些含有机密或敏感信息的数据记录。在许多情况下，该数据是直接或间接访问银行账户、信用卡的个人验证信息（PII），或被用于经济获益的其它模式的数据。数据泄露会导致高额的直接损失，因为企业必须花费资源来处理漏洞所导致的影响，以弥补受影响的客户。披露制度也迫使企业披露涉及 PII 的漏洞，因此这些漏洞也是最众所周知的。
- 知识产权。美国众议院常设情报委员会近日报道，丢失 IP 使公司在丧失发展资本和潜在收入方面付出了上亿元的代价。鉴于有关数据泄露的法律都集中在个人身份数据上，此类攻击的频率很可能远远大于公开报道中的数据。
- 数据收集。建立一个针对性攻击或 APT 需要拥有有关目标的情报。在最高界别，民族/国家之间进行的攻击可能会利用人力收集的情报。鉴于大多数恶意软件编写者不能使用人力情报资源，攻击者创建了能够搜集情报的攻击，以增强他们最终的攻击力量。最近发现的 Duqu 攻击（所谓的“Stuxnet 的儿子”）是此类攻击的一个高度精心设计的案例。这些攻击利用诸如键盘记录器之类的技术来搜集访问高度受保护的系统和机器所需的信息。
- 工业间谍。Stuxnet 攻击最吸引人的一面是他的终极目标：一个对工业控制设备的攻击。Stuxnet 利用控制设备使机器转数超出正常操作设定值，有效的关闭伊朗核计划中的试验室离心机，最终损害设备，从而导致其无法使被用。Stuxnet 是一个极端的例子，因为他们无疑是一个由一个民族/国家发起的，极其精心设计的 APT。既然那么多工业过程与工业控制系统相关联或者由工业控制系统运行，那么未来可能受害者更多。

证据表明，选择忽视漏洞检测领域的空白的企业将无疑会面对一个可估算的，能导致重大后果的风险。最起码，企业应该考虑投资防御工具的做法会导致回报递减。将他们的一部分预算和资源重定向到漏洞检测和响应是在优先级方面的一个谨慎转移。

快速检测和响应

快速检测

企业正在出现漏洞，他们没能力检测这些漏洞并对其进行响应，使响应对受影响企业有切实的效果。更好的检测只是答案的一部分，因为真正的价值来自于能够进行一个同样快速的和熟知情况的响应以应对识别到的漏洞。我们所需的是快速的检测和响应以弥补漏洞检测领域的空白。

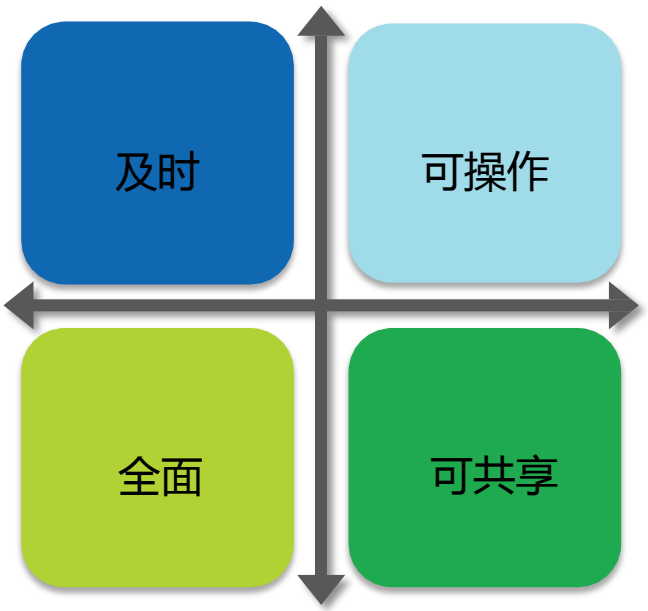
快速的检测使得被攻击的企业能够在攻击的早期阶段检测到多阶段攻击。希望这种早期的检测使企业尽早中断“kill chain”，以便在数据被窃取或造成其他损害前终止攻击链条。正如前面提到的那样，许多攻击有一个早期阶段。该阶段使用了一个在终端机器上的键盘记录器，以便向攻击者提供有关承载目标数据或知识产权的服务器所需的访问凭据。在终端机器上检测攻击早期阶段的能力以及中断“kill chain”的能力使得企业可以在敌人从终端进入点跳转之前中断入侵。

时钟节拍

Verizon Business 的 DBIR 显示 60%的漏洞花费一周或更多时间来实现控制，不到 10%的漏洞在不到 24 小时内完成控制。与此相反的是，60%的漏洞显示数据的泄漏开始于入侵后的第一个 24 小时。[1]

快速响应

对漏洞攻击的快速响应是有利的，但是要想拥有快速响应能力需要有具有几个基本特性的信息：



在快速响应中，速度不是唯一的维度

- 及时性。很明显的一点是，企业越快获得关于漏洞的信息，便可越早的做出响应。对各种漏洞研究数据的统计表明，就入侵和被发现入侵之间的时间跨度而言，攻击者没有感觉到强烈的紧迫感。及时性是有价值的，因为漏洞攻击最初时刻（在攻击者开始横向移动并且模糊他们的存在感之前）是最好的响应时间点。
- 可操作性。单纯的识别漏洞是不够的，必须对其进行分析，提供实施一个谨慎和明智的行动所需的信息。该信息必须是实用的，并能够提供尽可能多地信息以减少（或潜在的移除）额外的分析时间。
- 全面性。在植入恶意可执行文件和支撑文件之外，攻击通常会改变机器设置。配置改变，端口开放，持久性机制与主攻击计划相分离。如果不知道所有这些改变（主要的和附带的损害），就不可能使机器的脆弱点免于遭受后续的攻击或禁止持久性机制重起攻击。
- 可共享性。分析必须是一种能容易的与其他信息和工具相整合的格式，以便易于进行更广泛的分析和权能归属。例如，有关漏洞检测的信息可能会与数据元素（像防火墙日志）被整合进一个 SIEM/SIM/SEM 工具，以提供更好的防御类似攻击所需的分析。对于进行分布式管理的大型企业，如果在一个安全事件中，一个攻击已经被用于攻击该企业中的其它机器和网络，那么信息必须与其他团队和业务线共享。

自动快速响应

对一个漏洞的响应取决于攻击的复杂性，持久性方法的强度，以及网络漏洞和相关目标的灵敏度。显然，补救一个简单的漏洞要比补救一个复杂的，产生广泛、重大的附带伤害的漏洞容易得多。有效的漏洞修复需要辨识所有这些损害，并进而进行修复。手工修复的速度慢，因为企业经常缺乏正确和全面辨识一个攻击所造成的损害所需的工具和人力资源。为此，修复脚本最终是失败的，因为他们依赖于现有的先验知识，而恶意代码分分钟都在进行着变种。

对于一个能够消除重装需求的快速检测和响应解决方案来说，它必须能够识别该机器遭受的所有损害。这包括附带损害，例如修改配置参数，损坏操作系统调用，开放端口，在现有进程中嵌入进程。一旦辨识出所有变化，同一个工具将需要去修复这些变化： 恢复配置， 退出进程，关闭端口，修复被损坏的系统调用。不幸的是，这种修复更复杂，因为一些攻击破坏或删除了参数，例如注册表键值或文件。修复损害或删除属性需要一个方法来提供对这些参数的替换而不是重装软件或人工干预。

Triumfant 填补了攻击检测领域的空白

如果要为快速漏洞检测和响应描绘一个最佳场景，该解决方案需对恶意攻击进行检测而无须恶意行为特征或其他任何形式的实时先验知识，需以分钟为单位进行取证分析，并建立一个修复过程，阻断每一个攻击，修复受影响的机器而无需重起或重装。该工具将在几分钟内检测、分析并修复问题，而不需要中断终端用户或他们的工作。事实上，检测、分析和修复的整个过程可以在终端用户不知情的情况下进行。信息将会被以电子的方式共享给其他系统和 IT 安全团队，以便将攻击事件中搜集到的信息用于定性和未来更一步的分析，从而加强企业的防护能力。这个解决方案就是 Triumfant。

Triumfant 的方法

Triumfant 对漏洞的检测是通过检测主机的变化，使用已申报专利的分析方法来关联和分析这些变化，进而辨识异常和恶意活动。这一方法使 Triumfant 能够辨识恶意行为，而无需拥有恶意行为特征或其他任何形式的先验知识。Triumfant 可以辨识不断进化中的，可躲避传统防御方式的攻击，有效的填补了防火墙，IPS 和反病毒解决方案之间的空白。这包括零日漏洞攻击，rootkits，有针对性的攻击，高级持续威胁（APT），以及恶意内部人士的行为。

我们面临的挑战在于要精确的辨识和评估异常行为和恶意代码所导致的改变，而无误报。误报在过去一直困扰着对变化检测的尝试。与其他变化检测软件仅分析被攻击的机器的变化不同，Triumfant 独创了在获取的主机集群上下文背景中分析机器的变化。Triumfant 的分析方法自动构建和维持该上下文，然后利用该上下文背景来确保精确性和有效的消除误报。迄今为止，Triumfant 的分析技术已经获得四项专利，其中的三项专利被赋予给精确识别能力，关联能力和表征变化能力。

这种辨识和关联所有与攻击有关的变化的能力使 Triumfant 能够在入侵发生的几分钟内，对攻击进行综合。Triumfant 返回一个风险因素的详细分析报告，并给出一个响应建议，涉及机器上的每一个属性改变的细节证据。一个经验丰富的分析师往往需要耗费几小时或几天才能提供 Triumfant 几分钟内提供的内容，。

以变化检测为基础，Triumfant 能够通过分析，生成一个针对该问题的补救建议，从而将快速检测和响应带到一个新的高度。一旦检测到一个攻击，Triumfant 利用深度分析来构建一个场景化的，上下文关联化的补救建议，以彻底解决攻击和所有相关的附带损害。该机器几分钟内就从受感染变为被修复，而不需要对该机器进行重装或重起。

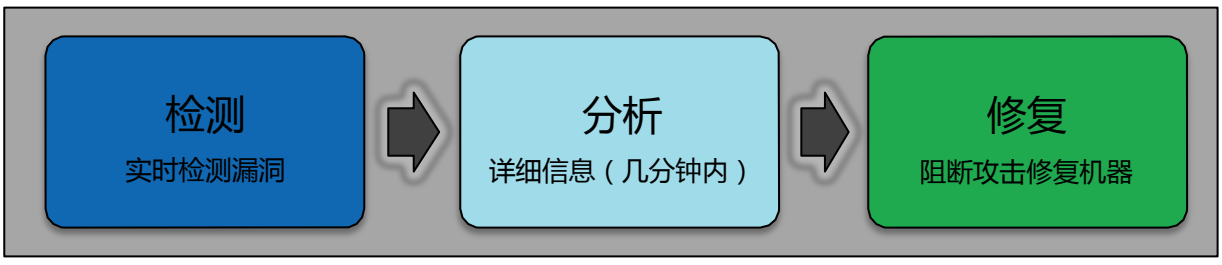


图 3：快速检测和响应的组件

检测

Triumfant 的恶意软件检测方法有效的填补了漏洞检测领域的空白，尽可能的靠近入侵点来提供快速漏洞检测。Triumfant 是建立在这样一个前提下的，即，要想攻击一个机器，必须先改变该机器。因此一个可以检测和分析机器改变的解决方案能够识别那些躲避防护措施并侵入机器的攻击。当然，在攻击侵入机器的那一刻，它就成为了一个漏洞。因此，Triumfant 的核心是漏洞检测解决方案，并切合了快速检测的需求。

与其它检测技术相比，变化检测拥有巨大的优势。因为，对于攻击向量、间谍，漏洞利用或传输机制来讲，该技术从本质上是中立的。由于消除了对先验知识的依赖性，Triumfant 能够检测零日攻击，已知攻击的变种，针对性攻击和高级持续攻击（APT）（无论漏洞的来源是什么）。在 IT 市场经受着永无止境的攻击浪潮，貌似万无一失的防御技术被快速的躲避过去的情形下，这一优点使得 Triumfant 有很强的适应性。

对于那些采具有多攻击阶段的复杂攻击，Triumfant 将使企业能够检测早期攻击阶段，并且能够尽早的中断攻击链条以减少攻击的影响。Triumfant 可以检测到受影响机器上的异常文件，尽管这些文件还没有真正执行。通过这种方式，Triumfant 通常可以发现“low and slow”攻击，即便这些攻击还处于休眠中。

分析

创建有关漏洞检测的，综合的且有操作性的信息也是 Triumfant 的固有特点。那是因为 Triumfant 的分析的目的是辨识，关联和分析所有有关攻击的机器变化，以便为评估风险和辨识恶意代码行为提供必要的数据。信息不是一个副产品，它对于 Triumfant 检测分析过程是必不可少的。

在入侵发生的几分钟内，如果攻击处置人员手中有具有可操作性的信息，这将会增强他们评估形势和实施一个及时的响应的能力。Triumfant 有一个摘要综述，该总综述饱含一个描述和建议，以及辨识出的风险参数。该摘要还包括相关的进程和可执行文件，高频串，以及相关互联网连接。该分析随后提供了每一个受影响的参数的细节，包括注册表项，文件，端口，过程和服务。很有必要深挖每一个参数的细节，以便明确的勘查是什么发生了变化以及它是如何变化的。对于每一个漏洞，没有其他工具能像 Triumfant 这样，达到如此的广度和详细度。

该分析可以以多种形式呈现，并且能够被直接集成到其他工具中。有关漏洞的详细信息可以很容易的被应急响应团队或取证团队用于进一步的分析。Triumfant 将生成一个 ArcSight Common Event Format (CEF)格式的系统日志。该格式的系统日志能够与 SIEM 工具整合，以便与防火墙日志和其他数据中的漏洞相关信息关联起来。该信息能够被导入到一个构建的向导。Triumfan 过滤器可以被用于在其他机器和网络上搜索攻击。

响应（修复）

Triumfant 的综合分析使能力 Triumfant 利用通过分析得到的详细信息来构建一个针对被检测到的漏洞的补救方案，建立了一个针对该攻击的明确且及时的响应方案。该补救方案是精确的且具有可操作性，能够阻断攻击并移除攻击所导致的不良伤害。关闭端口，恢复被修改的配置, 替换被损坏或删除的文件，恢复注册表项。

该补救方法能够修复正在运行中的机器，而无需重起机器或对任何对服务的中断。防御领域将此称作“fighting through“—但检测到对机器的攻击，即以对业务造成最小（接近于 0）冲击的方式修复机器。该补修方案不是一个回滚或重装一个镜像。他是对攻击影响的参数进行修复。因此，在该过程中，主机用户不会失去任何他们想要保留的更改。我们完全可能看到用户的机器受到攻击，随后被修复，而用户对此没有察觉。Triumfant 能检测一个攻击，对其进行分析，并在几分钟内修复机器。我们有理由宣称，Triumfant 完成全部的检测，分析和修复过程所用的时间少于一个收到告警的分析师开启手工过程并开始收集有关恶意代码行为的数据的第一步所用的时间。

修复恶意软件所造成的损害比简单的删除相关文件和注册表项更困难。对丢失的或被破坏的参数的处置需要恢复这些参数。Triumfant 独创的“Donor Technology” 利用从主机集群那里获得的上下文背景，将主机集群转化为一个捐赠库来修复丢失的或被破害的参数，包括文件和注册表项。对于每一个丢失或被破坏的参数，Triumfant 查询已获取到的上下文背景以找到一个列表，列表中包含着候选的捐赠机器，捐赠机器中有修复受影响机器所需的参数。Triumfant 的分析验证了捐赠的参数的完整性，随后，将他们用于修复被损坏的参数。Donor Technology 是 Triumfant 的创新，Triumfant 将该技术申请了专利。

有关 Triumfant 如何检测恶意软件和修复其所造成的损伤的详情,请参见 Triumfant 白皮书: Detecting and Remediating Malicious Attacks

优势

Triumfant 的独特的，创新的快速检测和响应解决方案具有很多优点：

- Triumfant 有力的弥补了漏洞检测领域的空白，为企业提供了其所需的快速检测和响应工具，以降低企业由于未检测到漏洞而面对的财务、信誉和管理的风险。
- 没有工具能够全面地保护企业使其免于丢失敏感数据和知识产权。Triumfant 对漏洞攻击的实时检测增加了 IT 安全团队在丢失敏感数据或 IP 之前即对漏洞进行处置的概率，进而减少企业的风险和后续的损失，并防止潜在的重大事件。
- Triumfant 提供了一个综合的取证分析，并在几分钟创建了一个场景化的，有上下文关联的补救建议。进行相应的分析，构建一个修复方案，每项工作都需要耗费分析师几小时或几天才能完成。通过在攻击发生的几分钟替向企业完成上述两项工作，Triumfant 使企业能够制定一个具有丰富信息支撑的攻击响应，并且提供阻断攻击和修复机器的方法。自动化分析和补救过程使得以前消耗在调查攻击和撰写补救建议的人力资源转为积极主动的阻止攻击而不是应对攻击。这种关键安全人员用途的改变可以有效的降低企业风险。
- Triumfant 创建了一个补救方案，该方案能够移除恶意代码，消除所有与攻击相关的机器的改变。该补救方案是全面的修复机器的损害，而不丢失正常工作所产生的改变。它不会中断对用户服务，无需重起机器。因为该修复是完全的，所以无需重装机器。
- 对于攻击向量、间谍，漏洞利用或传输机制而言，Triumfant 从本质上是中立的。例如，近来的攻击利用便携式存储设备（U 盘）或无线连接来躲避检测工具（例如，深度包检测解决方案）。随着恶意软件持续不懈的进化，基于 Triumfant 方法的本质，Triumfant 将会持续检测漏洞攻击。Triumfant 不是一个防护盾，但是它为企业提供持续不断的，覆盖零日漏洞攻击和不断进化的攻击的检测，一直到防御技术能够迎头赶上。
- 与其它检测技术相比，变化检测拥有巨大的优势。因为，对于攻击向量、间谍，漏洞利用或传输机制来讲，它从本质上是中立的。由于消除了对先验知识的依赖性，Triumfant 能够检测零日攻击，已知攻击的变种，针对性攻击和高级持续攻击（APT）（无论漏洞的来源是什么）。
- Triumfant 是对其他 IT 安全工具的一个补充，完善和扩展，例如，与 AV suites，SIEM 工具，和 Trouble Ticketing 工具整合。对于 CIRT 和取证团队来说，有关攻击和数据捕获以及随后的补救方案是无价的信息，他们可用这些信息增强企业的防御，缩减其受攻击的范围。

结论

企业正在被迫接受一个新的现实：企业将会遭受漏洞攻击。企业没有做好检测和应对所遭受的漏洞攻击的准备。攻击者正在利用此种情形。防御工具和取证工具之间存在着一个很大空白，这使得企业不能快速的检测一个漏洞，为实施快速、有丰富信息支撑的响应提供具有可操作性的信息。

Triumfant 实时检测漏洞，伴随着攻击的每一个分钟生成一个全面的，具有可操作性的分析，构建一个场景化的补救方案，该方案阻止漏洞攻击并修复机器遭受的所有主要的和附带的损害。Triumfant 采用一个创新的解决方案有效且高效的填补了漏洞检测领域的空白，消除了企业所面临的相关风险。

要了解 Triumfant 解决方案的详情，请参见 Triumfant 网站 www.Triumfant.com 更多信息发信至 Info@Triumfant.com.

备注

[i] Casey, Bryan; et al (March 2012). IBM X-Force 2011 Trend and Risk Report. IBM Corporation. Retrieved from https://www14.software.ibm.com/webapp/iwm/web/signup.do?source=swg-Tivoli_Organic&S_PKG=xforce-trend-risk-report. p. 12.

[ii] M-Trends Report (March 2012). Mandiant Corporation. Retrieved from http://www.mandiant.com/. p. 2.

[iii] Percoco, Nicholas; et al (February 2012). Trustwave 2012 Global Security Report. Trustwave Corporation. Retrieved from https://www.trustwave.com/global-security-report. p. 10.

[iv] Baker, Wade; et al (March 2012). Verizon Business 2012 Data Breach Investigations Report. Verizon Business. Retrieved from http://www.verizonbusiness.com/Products/security/dbir/. p. 49.

[v] Verizon Business 2012 Data Breach Investigations Report. p. 49.

[vi] Verizon Business 2012 Data Breach Investigations Report. p. 51.

[vii] Verizon Business 2012 Data Breach Investigations Report. p. 57.

[viii] Rashid, Fahmida (October 8, 2011). *eWeek.com*. U.S. Strategic Drone Fleet Infected by Stealthy Keylogger Malware. Retrieved April 17, 2012 from http://www.eweek.com/c/a/Security/US-Strategic-Drone-Fleet-Infected-by-Stealthy-Keylogger-Malware-561651/.

[ix] Online Trust Alliance (January 2012). 2012 Data Protection & Breach Readiness Guide. Retrieved from https://www.otalliance.org/resources/incident/2012DataBreachGuide.pdf. p. 4.

[x] EMC Corporation 10-Q, Quarterly report pursuant to sections 13 or 15(d). Filed on 08/05/2011. Filed Period 06/30/2011

[xi] King, Rachael (June 8, 2011). Bloomberg. EMC’ s RSA Security Breach May Cost Bank Customers $100 Million. Retrieved April 15, 2012, from http://www.bloomberg.com/news/2011-06-08/emc-s-rsa-security-breach-may-cost-bank- customers-100-million.html.

[xii] Osaw, Juryu (May 9, 2011). Wall Street Journal Online. As Sony Counts Hacking Costs, Analysts See Billion-Dollar Repair Bill. Retrieved April 15, 2012 from http://online.wsj.com/article/SB10001424052748703859304576307664174667924.html.

Triumfant