安全情报：定义 APT 活动

非官方中文译本 • 安天实验室 译注

文档信息			
原文名称	Security Intelligence: Defining APT Campaigns		
原文作者	Michael	**原文发布日期**	2014 年 6 月 21 日
作者简介	Michael 是洛克希德•马丁公司计算机事件响应小组的高级成员。他曾在各种场合演讲，包括 SANS、IEEE、每年 DC3 网络犯罪大会，并教授密码学的入门级课程。他目前的工作包括安全情报分析，新型事件响应工具和技术的开发。 请参阅文末的作者简介。		
原文发布单位	SANS Institute		
原文出处	http://digital-forensics.sans.org/blog/2010/06/21/security-intelligence-knowing-enemy#		
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。		

安全情报：定义 APT 活动

2014 年 6 月 21 日

APT 攻击的持续性表现在两方面：持续存在于受害者网络；不断尝试进入其他未感染领域。这些行为的重复性包括一致的属性，因为资源限制通常能够防止攻击者每次访问目标环境时的采用不同的行为。通过某种方法对攻击和这些共同属性进行建模，防御者就可以利用持续性来分析攻击者、制定响应策略、进行分析并投入资源。

活动

一个攻击可以分为 7 个阶段。在每个阶段中会出现一组高维度的信标—计算机科学家将其称为“属性”。例如，一个 C2 回调域名就是一个信标属性，talktome.bad.com 是这个信标的对应值。确定目标（侦察）、恶意负荷模糊的方法（武器化）负载的路径（传输）、负载调用的方法（利用）、后门隐藏在系统何处（安装）、与攻击者通信使用的协议（C2）、建立控制后攻击者的习惯（行为），这些都是这些信标的类别。分析人员在攻击中发现重要或独特的识别信标时非常重要的。在一些情况下，会有些共同信标，例如用于传输信息的最后一跳邮件中继，这在多数攻击中是很有意义的，web 邮件除外。在其他情况下，属性可以是唯一的和令人意外的，例如一些元数据、一个二进制后门字符串、一个可预见的畸形的 HTTP 请求（用于检查连接）。

通常，不止一次发现某个属性之前，我们无法确定该属性是否是重要的。图 1 展示了两个不同的攻击，一些类别可能存在重叠。通过识别多个攻击的相同属性，我们可以确定出共同属性。

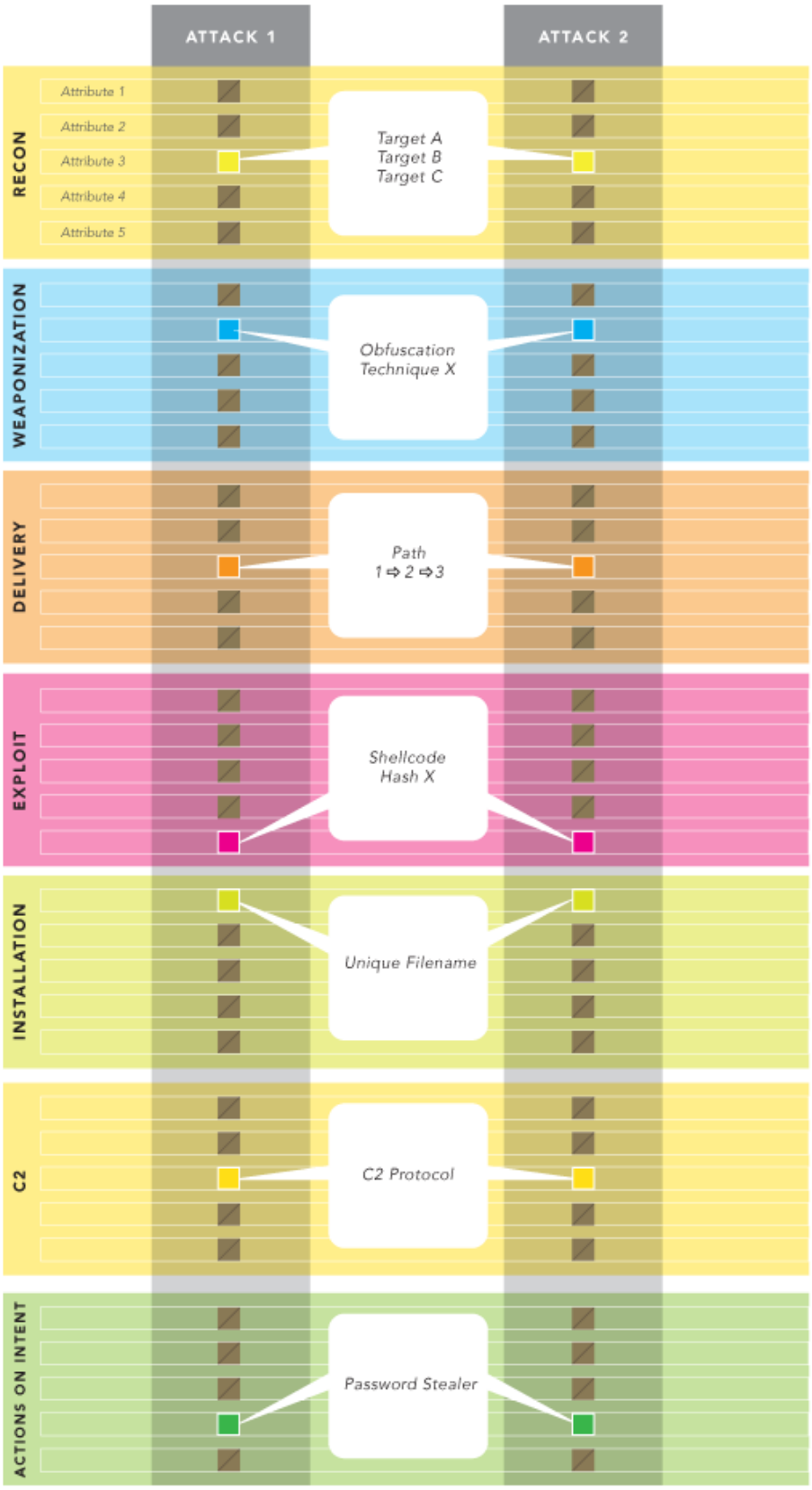
ATTACK 1
ATTACK 2
RECON
Attribute 1
Attribute 2
Attribute 3
Attribute 4
Attribute 5
Target A
Target B
Target C
WEAPONIZATION
Obfuscation
Technique X
DELIVERY
Path
1 ⇨ 2 ⇨ 3
EXPLOIT
Shellcode
Hash X
INSTALLATION
Unique Filename
C2
C2 Protocol
ACTIONS ON INTENT
Password Stealer

图 1：攻击对比

图 2 中的色块是感染点，代表着主要信标。信标重复的越多，其对攻击者越重要（这些信息通常是无法从防御数据中获得的），则该信标对我们的定义就越重要。事实上，我们这里的建模不是个体，而是成功与失败攻击的关联组。因此，“活动”一词比“攻击者”更合适，尽管我们偶尔会交叉使用这两个词。

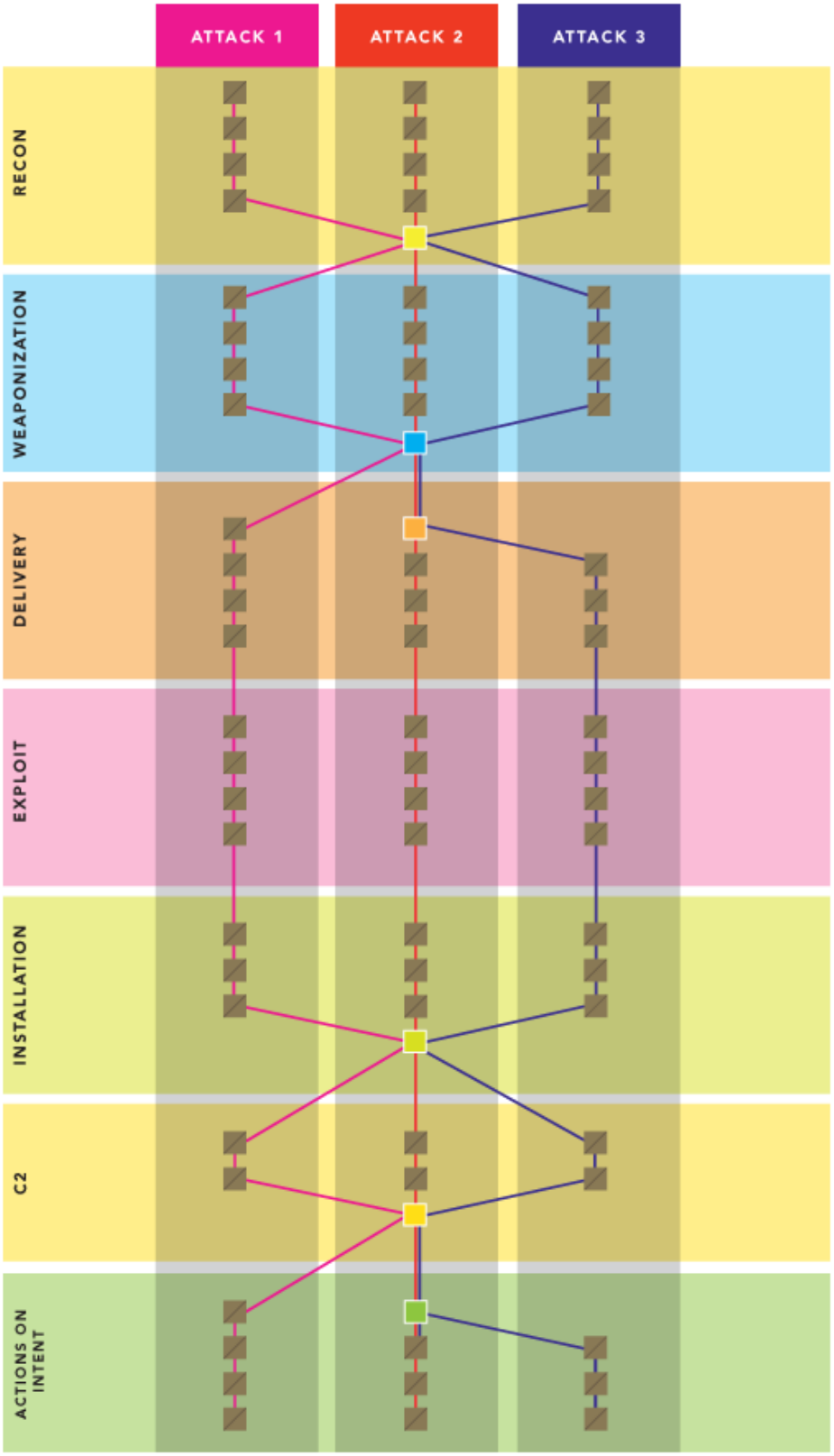

图 2：攻击活动中的关键信标识别

没有规则或者客观阈值来告知我们什么时候关攻击会演变成一个活动。最好的衡量方法是结果：如果一组信标有效地预测了未来发生的一些攻击，则它们的选择就是恰当的。如果一个活动的 TTP（战术、技术和程序）与一组信标高度脱节，则说明这组信标与良性活动相关，或者没有选好或者定义好。我们发现，如果三次或更多攻击企图与独特属性有关，则攻击者月难以改变这些属性，因此它们会存在于整个攻击链中，这种信标是了解“活动”的不错选择。

需要注意的是：攻击者会不断地调整策略。攻击活动不是静止的，关键信标及其对应值也非静止的。我们发现，有的攻击者在若干年中使用相同的传输和 C2 基础设施，而其它攻击者则会在传输和 C2 阶段将基础设施更改为高度可变的基础设施，但是定位和武器化技术保持不变。一些攻击者将使用同样的关键信标，例如传输和武器化阶段的工具，但是特殊信标值可能随着时间改变。如果不对复杂攻击进行持续和完整的分析，则对攻击活动的了解对于预测未来供给毫无帮助。

通过攻击链来收集情报

为了使数据库有助于将攻击联系起来，并识别关键信标，分析人员必须理解每个复杂攻击的所有阶段。初始检测可能发生于攻击链的任何一点都。即使攻击没有成功，检测也是第一步。

经典的应急响应方法是假设一个系统被攻破。在这种情况下，检测发生在安装和/或者执行恶意代码之后，攻击者成功的执行了很多攻击步骤。随着攻击活动沿着破坏链向前发展，相应的分析向后发展（图 3）。分析人员必须重建之前的每个阶段，这不仅需要合适的工具和基础设施，还需要高超的网络和主机取证技术。不成熟的响应团队通常会卡在传输到安装阶段中。如果不了解前面的阶段发生了什么，防御者就无法定义这些阶段的攻击，而响应也将是攻破之后的。当遭遇分析障碍时，整个攻击链的重建也会受影响，这些障碍代表需要仪器或者分析技术改进的领域。在所有领域配备开发者进行应急响应，这对于组织成功来说是很重要的。

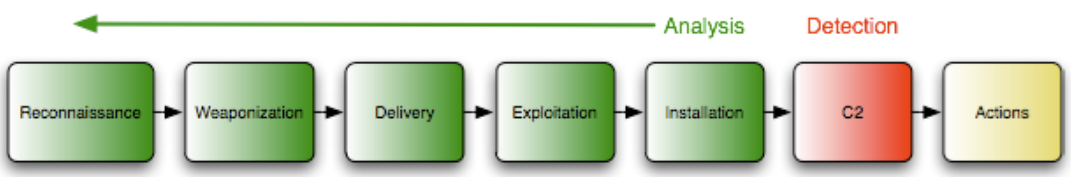

图 3：成功攻击的分析

随着响应组织的成熟，并且能够应对更充分的分析攻击，他们在攻破前的检测也更加成功。然而，正如攻破后响应涉及大量分析一样，匹配 APT 攻击特点的不成功的攻击尝试也需要予以调查。被攻击者成功执行的步骤必须也要重建，没有成功的步骤也要整合考虑，以开发最好的响应能力（图 4）。这在鉴别任何 TTP（战术、技术和程序）改变上都很重要，这些改变可能是因为一个成功的攻击。也许最引人注意的例子是识别 APT 攻击者在传输步骤中使用的零日漏洞（漏洞被调用之前）。

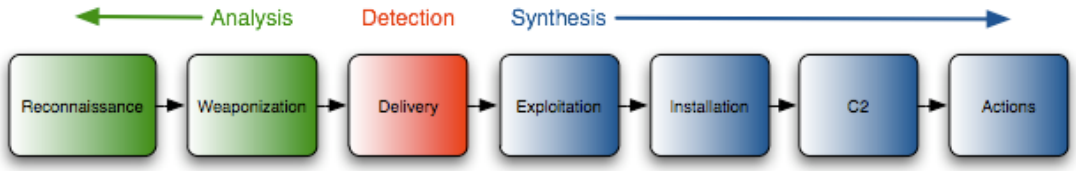

图 4：不成功攻击的分析和整合

整合清楚地展示了恶意代码逆向工程的核心技术。很可能已经投放了后门，即使是使用已知 C2 协议的已知家族也包括新信标（定义攻击者使用的基础设施）。例如 C2 回调 IP 地址和完全描述域名。可能恶意代码的微小变化就会产生新的唯一哈希值，或者一个变化会导致不同的可能唯一的安装文件名。虽然杀毒是检测 APT 攻击的坏例子，但是很多时候对于旧变种来说还是有价值的。例如，读者中有多少人分析过杀毒系统检测到的邮件呢？如果是为了检测特别 APT 活动的后门，邮件可以包括有价值的攻击者的传输属性，或者后续攻击使用的 C2 基础设施。

结论

检测活动使得攻击中的弹性检测和防御机制成为可能，涉及攻击链中的响应者，减少了成功攻击的数量。这应该是显而易见的，但值得重申的是，攻击的特定信标的缺乏阻碍了关键信标的识别。缺乏关键信标将导致无法定义攻击者，使得防御者只能在每次攻破后进行响应。总之，无法重建攻击应被认为是组织 CND（计算机网络防御）的失败，而系统攻破之前的基于情报的检测则是组织的成功。如本文所述，定义攻击活动是取得成功的有效途径。

作者简介

Michael 是洛克希德·马丁公司计算机事件响应小组的高级成员。他曾在各种场合演讲，包括 SANS、IEEE、每年 DC3 网络犯罪大会，并教授密码学的入门级课程。他目前的工作包括安全情报分析，新型事件响应工具和技术的开发。迈克尔拥有计算机工程学士学位和计算机科学硕士学位，目前正在攻读系统工程博士学位。他赢得了多种荣誉，包括 GCIA＃592（认证入侵分析师）和 GCFA＃711（认证数字取证分析师）金牌认证，而且是 ACM（美国计算机协会）的专业会员和 IEEE（美国电气和电子工程师协会）的成员。