APT攻击基础科普

0x00 APT的历史起源背景

APT这个词汇最早起源于：2005年英国和美国的CERT组织发布了关于有针对性的社交工程电子邮件，放弃特洛伊木马以泄露敏感信息的第一个警告，尽管没有使用"APT"这个名字。但 "先进的持续威胁"一词被广泛引用，2006年的美国空军Greg Rattray上校经常被引用为创造该术语的个人。后来，在Stuxnet震网事件就是专门针对伊朗的核计划的黑客攻击就是一个APT攻击例子。在计算机安全领域以及越来越多的媒体中，APT这个术语几乎总是用来指向针对政府，公司和政治活动家的黑客攻击的高级持续模式，而且也延伸到涉及到群体这些攻击背后。作为一个术语，高级持续威胁（APT）可以被转移焦点到攻击出现次数。一个常见的误解是APT只针对西方国家。西方国家可能会更多地宣传针对西方国家的技术性APT，但许多国家的行为者都将网络空间安全作为收集有关个人和群体的情报的手段。在美国，网络司令部的任务是协调美国军方，应对高级持续网络威胁，也就是APT攻击。

同时，许多消息来源都觉得一些APT组织实际上隶属于或者代表着民族和国家。否则很难持有大量信息和资源，三类机构容易面临高级持续威胁的高风险，即：高等教育,金融机构,政府机构。

实际上，一个APT是有一套隐匿和持续攻击的框架的，往往针对特定的实体由一人或多人策划（一般是多人）。APT通常针对高价值目标出于商业或政治动机进行实施的。APT在长时间的攻击中依旧会尽可能的保证高度隐蔽性。而"高级"意味着使用恶意软件来攻击系统漏洞的复杂技术。"持续"过程表明，APT攻击组织外部和控制系统正在持续监测和提取特定目标的数据。"威胁"过程表明攻击会损害目标利益。

APT通常是指一个组织，甚至可能一个政府支持下的组织，因为APT团体是一个既有能力也有意向持续而有效地进行攻击的实体。所以APT通常用来指网络威胁，特别是使用互联网进行间谍活动，利用各种情报搜集技术来获取敏感信息，但同样适用于诸如传统间谍活动或攻击等其他威胁。其他公认的攻击媒介包括受感染的媒体，供应链和社会工程。这些攻击的目的是将自定义的恶意代码放在一台或多台计算机上执行特定的任务，并在最长的时间内不被发现。了解攻击者文件（如文件名称）可帮助专业人员进行全网搜索，以收集所有受影响的系统。个人，如个人黑客，通常不被称为APT，因为即使他们意图获得或攻击特定目标，他们也很少拥有先进和持久的资源。

0x01 APT攻击定义

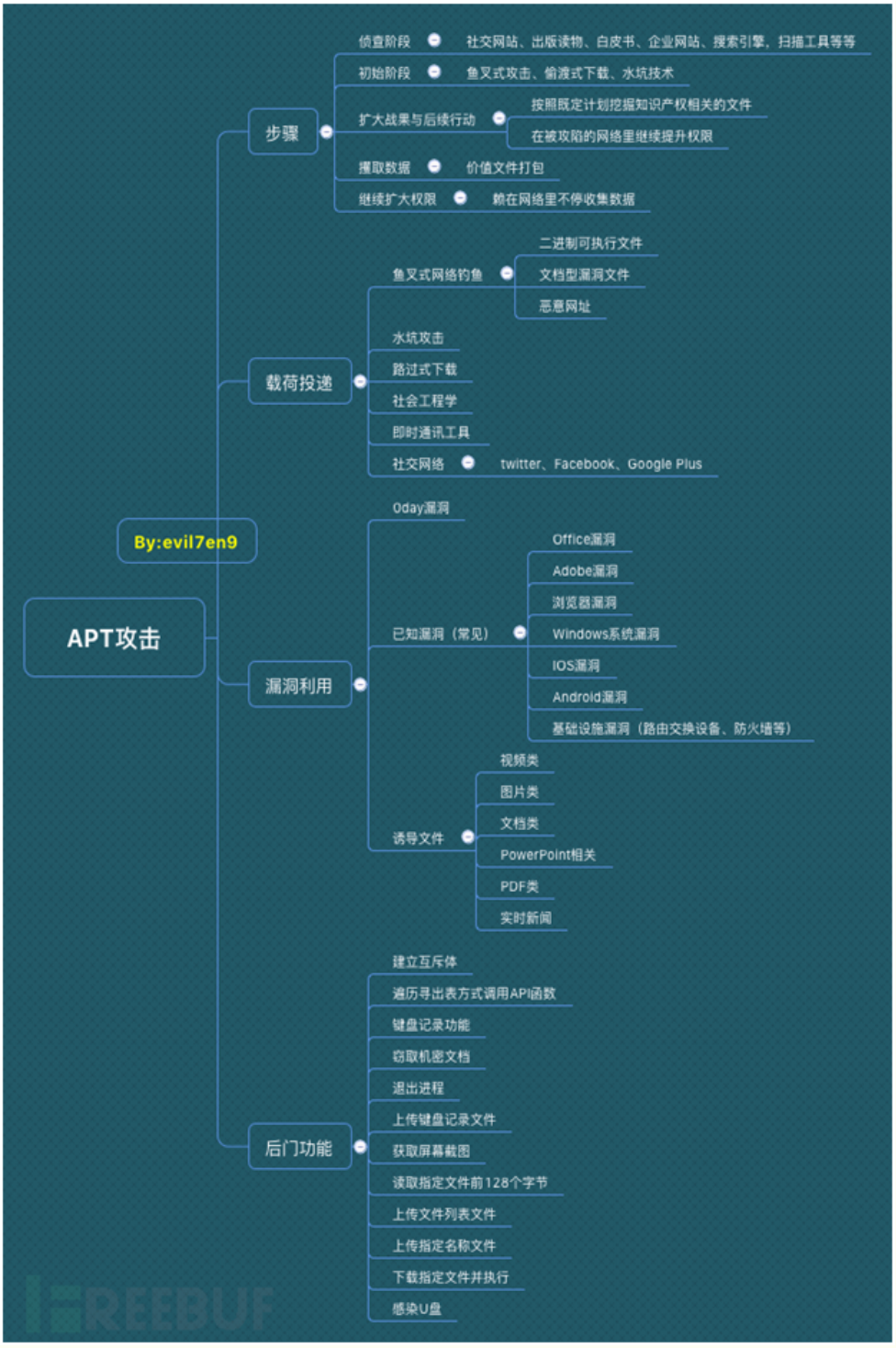
APT攻击（Advanced Persistent Threat，高级持续性威胁）是指组织(特别是政府)或者小团体利用当下先进的攻击手法对特定目标进行长期持续性的网络攻击。APT攻击的高级体现在于精确的信息收集、高度的隐蔽性、以及使用各种复杂的网络基础设施、应用程序漏洞对对目标进行的精准打击。攻击人员的攻击形式更为高级和先进，称为网络空间领域最高级别的安全对抗。APT是黑客以窃取核心资料为目的，针对客户所发动的网络攻击和侵袭行为。

APT(高级长期威胁)包含三个要素：高级、长期、威胁。高级强调的是使用复杂精密的恶意软件及技术以利用系统中的漏洞。长期暗指某个外部力量会持续监控特定目标，并从其获取数据。威胁则指人为参与策划的攻击。

APT攻击的原理相对于其他攻击形式更为高级和先进，其高级性主要体现在APT在发动攻击之前需要对攻击对象的业务流程和目标系统进行精确的收集。在此收集的过程中，此攻击会主动挖掘被攻击对象受信系统和应用程序的漏洞，利用这些漏洞组建攻击者所需的网络，并利用0day漏洞进行攻击

0x02 APT攻击手法

APT的攻击手法，在于隐匿自己，针对特定对象，长期、有计划性和组织性地窃取数据，此类攻击行为是传统安全检测系统无法有效检测发现，前沿防御方法是利用非商业化虚拟机分析技术，对各种邮件附件、文件进行深度的动态行为分析，发现利用系统漏洞等高级技术专门构造的恶意文件，从而发现和确认APT攻击行为。由于APT的特性，导致难发现、潜在威胁大，一旦被攻击将导致企业、政府、医疗组织等等的大量数据被窃取，公司重要财务、机密被盗窃。



0x03 APT攻击方式

APT组织常用的攻击手法有：**鱼叉式网络钓鱼、水坑攻击、路过式下载攻击、社会工程学、即时通讯工具、社交网络**等

鱼叉式网络钓鱼（Spear phishing）指一种源于亚洲与东欧，只针对特定目标进行攻击的网络钓鱼攻击。当进行攻击的骇客锁定目标后，会以电子邮件的方式，假冒该公司或组织的名义寄发难以辨真伪之档案，诱使员工进一步登录其账号密码，使攻击者可以以此借机安装特洛伊木马或其他间谍软件，窃取机密；或于员工时常浏览之网页中置入病毒自动下载器，并持续更新受感染系统内之变种病毒，使使用者穷于应付。由于鱼叉式网络钓鱼锁定之对象并非一般个人，而是特定公司、组织之成员，故受窃之资讯已非一般网络钓鱼所窃取之个人资料，而是其他高度敏感性资料，如知识产权及商业机密。

(1) **鱼叉攻击（Spear Phishing）**是针对特定组织的网络欺诈行为，目的是不通过授权访问机密数据，最常见的方法是将木马程序作为电子邮件的附件发送给特定的攻击目标，并诱使目标打开附件。

随笔分类

kali渗透(11)
web渗透(16)
安全运维(9)
代码审计(1)
红蓝对抗
漏洞复现(15)
漏洞总结(8)
内网渗透(28)
企业安全建设(7)
淫技技巧(10)
应急响应
域内渗透(10)

随笔档案

2018年12月 (9)
2018年11月 (3)
2018年10月 (2)
2018年9月 (5)
2018年8月 (11)
2018年7月 (3)
2018年6月 (5)
2018年5月 (7)
2018年3月 (9)
2018年1月 (1)
2017年12月 (4)
2017年11月 (4)
2017年9月 (4)
2017年8月 (10)
2017年7月 (5)
2017年6月 (6)
2017年5月 (15)
2017年4月 (6)
2017年3月 (1)
2017年2月 (2)
2016年11月 (1)
2016年10月 (2)

相册

image(1)

友情链接

evi1cg
klionsec
klionsec博客
SOMD5

最新评论

1. Re:ThinkPHP 5.x远程命令执行漏洞分析与复现
你好，我想请问你的docker是怎么搭建的。
就是那个.yml
具体是那条指令能麻烦说一下吗?
--奶奶奶奶奶糖

2. Re:Meterpreter命令详解
大佬啊,幸苦
--weigr

3. Re:MSF下ms17_010_psexec模块使用技巧
2003用这个好像不需要管道的 我清册成功

(2)**水坑攻击（Water Holing）**是指黑客通过分析攻击目标的网络活动规律，寻找攻击目标经常访问的网站的弱点，先攻下该网站并植入攻击代码，等待攻击目标访问该网站时实施攻击。水坑攻击（Watering hole）是一种计算机入侵手法，其针对的目标多为特定的团体（组织、行业、地区等）。攻击者首先通过猜测（或观察）确定这组目标经常访问的网站，并入侵其中一个或多个，植入恶意软件，最后，达到感染该组目标中部分成员的目的。 由于此种攻击借助了目标团体所信任的网站，攻击成功率很高，即是针对那些对鱼叉攻击或其他形式的钓鱼攻击具有防护能力的团体。

下图给出了OceanLotus使用鱼叉攻击和水坑攻击的基本方法。

(4)**路过式下载（Drive-by download）:**用户不知道的情况下下载间谍软件、计算机病毒或者任何恶意软件。路过式下载可能发生在用户访问一个网站、阅读一封电子邮件、或者点击一个欺骗性弹出式窗口的时候。例如，用户误以为这个弹出式窗口是自己的计算机提示错误的窗口或者以为这是一个正常的弹出式广告，因此点击了这个窗口。

(5)**社会工程学:** 在计算机科学中，社会工程学指的是通过与他人的合法地交流，来使其心理受到影响，做出某些动作或者是透露一些机密信息的方式。这通常被认为是一种欺诈他人以收集信息、行骗和入侵计算机系统的行为。在英美普通法系中，这一行为一般是被认作侵犯隐私权的。社会工程学是一种通过人际交流的方式获得信息的非技术渗透手段。不幸的是，这种手段非常有效，而且应用效率极高。然而事实上，社会工程学已是企业安全最大的威胁之一。

360发布的《摩诃草APT组织大揭秘》报告中，发现了摩诃草近年来大量使用即时通讯工具（主要是腾讯的QQ聊天工具）和社交网络（Facebook）进行载荷投递的攻击方式；即时通讯工具以发送二进制可执行程序为主，这类程序主要伪造成MP4格式的视频文件；社交网络（Facebook）的载荷投递一般是分为：SNS蠕虫、放置二进制格式可执行恶意程序或文档型漏洞文件。

在确定目标公司后，APT组织会开始收集目标的一切信息，如：公司用户的电子邮箱，手机号码，通讯软件号码、姓名、你的工作岗位接着APT组织会对目标开始构造钓鱼文档并准备投放，当内部工作人员打开恶意文档了之后，电脑会触发相关的漏洞为apt成员打开了一道通往内部网络的大门，这时候他们会开始寻找存放着信息的服务器并开始攻击服务器拿到自己想要的东西后，在植入木马进行权限维持。

0x04 APT的特点

目标 – 威胁的最终目标，即你的对手

时间 – 调查、入侵所花的时间

资源 – 所涉及的知识面及工具（技能和方法也有所影响）

风险承受能力 – 威胁能在多大程度上不被发觉

技能与方法 – 所使用的工具及技术

行动 – 威胁中采取的具体行动

攻击源头 – 攻击来源的数量

牵涉数量 – 牵涉到多少内部或外部系统，多少人的系统具有不同重要性

信息来源 – 是否能通过收集在线信息识别出某个威胁

0x05 APT攻击实现

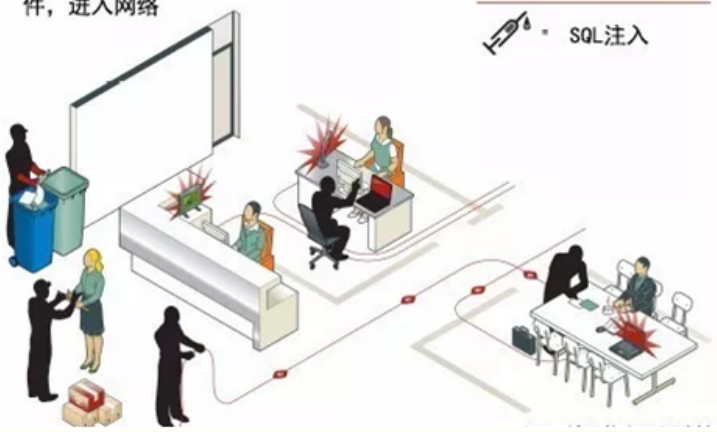
APT攻击精心策划，精心执行。 它们通常分为四个阶段：**入侵**，**发现**，**捕获**和**渗出。** 在每个阶段中，可以使用各种技术，如下图示。

1. 入侵

攻击者通过使用社会工程向易受攻击的系统和人员提供有针对性的恶意软件，进入网络

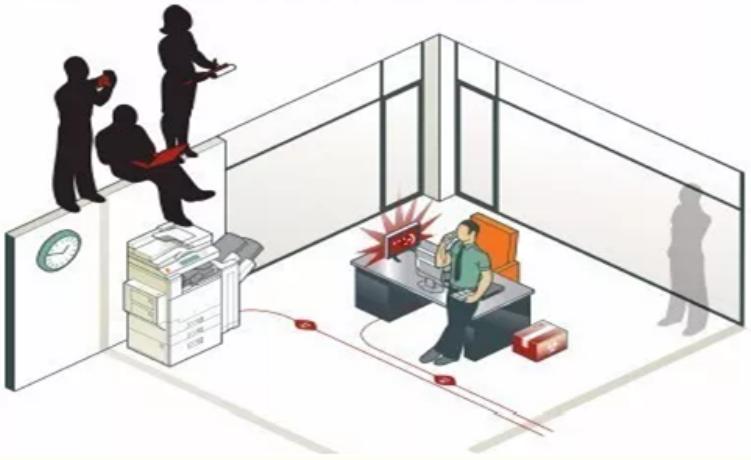
攻击方式

- 社会工程学
- 零日漏洞
- SQL注入



2. 发现

一旦进入，攻击者就会保持“低而缓慢”，以避免发现。然后他们将组织的防御从内部映射出来，并制定一个战斗计划，部署多个并行杀伤链，以确保成功。



0x06 APT攻击的生命周期

APT的幕后黑手会对组织团体的金融财产、知识产权及名誉造成持续变化的威胁，其过程如下： 因一个目标开始盯上特定组织团体试图入侵到其环境中（如发送钓鱼邮件） 利用入侵的系统来访问目标网络部署实现攻击目标所用的相关工具隐藏踪迹以便将来访问。

2013年，美国网络安全公司麦迪安（Mandiant）发布了关于2004至2013年间的一例APT攻击的研究结果，其中的生命周期与上述相似：

初始入侵 – 使用社会工程学、钓鱼式攻击、零日攻击，通过邮件进行。在受害者常去的网站上植入恶意软件（挂马）也是一种常用的方法。

站稳脚跟 – 在受害者的网络中植入远程访问工具，打开网络后门，实现隐蔽访问。

提升特权 – 通过利用漏洞及破解密码，获取受害者电脑的管理员特权，并可能试图获取Windows域管理员特权。

内部勘查 – 收集周遭设施、安全信任关系、域结构的信息。

横向发展 – 将控制权扩展到其他工作站、服务器及设施，收集数据。

保持现状 – 确保继续掌控之前获取到的访问权限和凭据。

任务完成 – 从受害者的网络中传出窃取到的数据。

麦迪安所分析的这起入侵事件中，攻击者对受害者的网络保有控制权的平均时间为一年，最长时间为五年。

0x07 APT攻击阶段

APT攻击会更加系统，分布，协作，一般分成：信息收集，武器化部署，传递载荷，利用，安装，命令和控制，执行

而杀伤链一般是6个阶段：发现-定位-跟踪-瞄准-入侵-完成，APT攻击模型Cyber-Kill-chain与之对应

0x08 APT分析模型

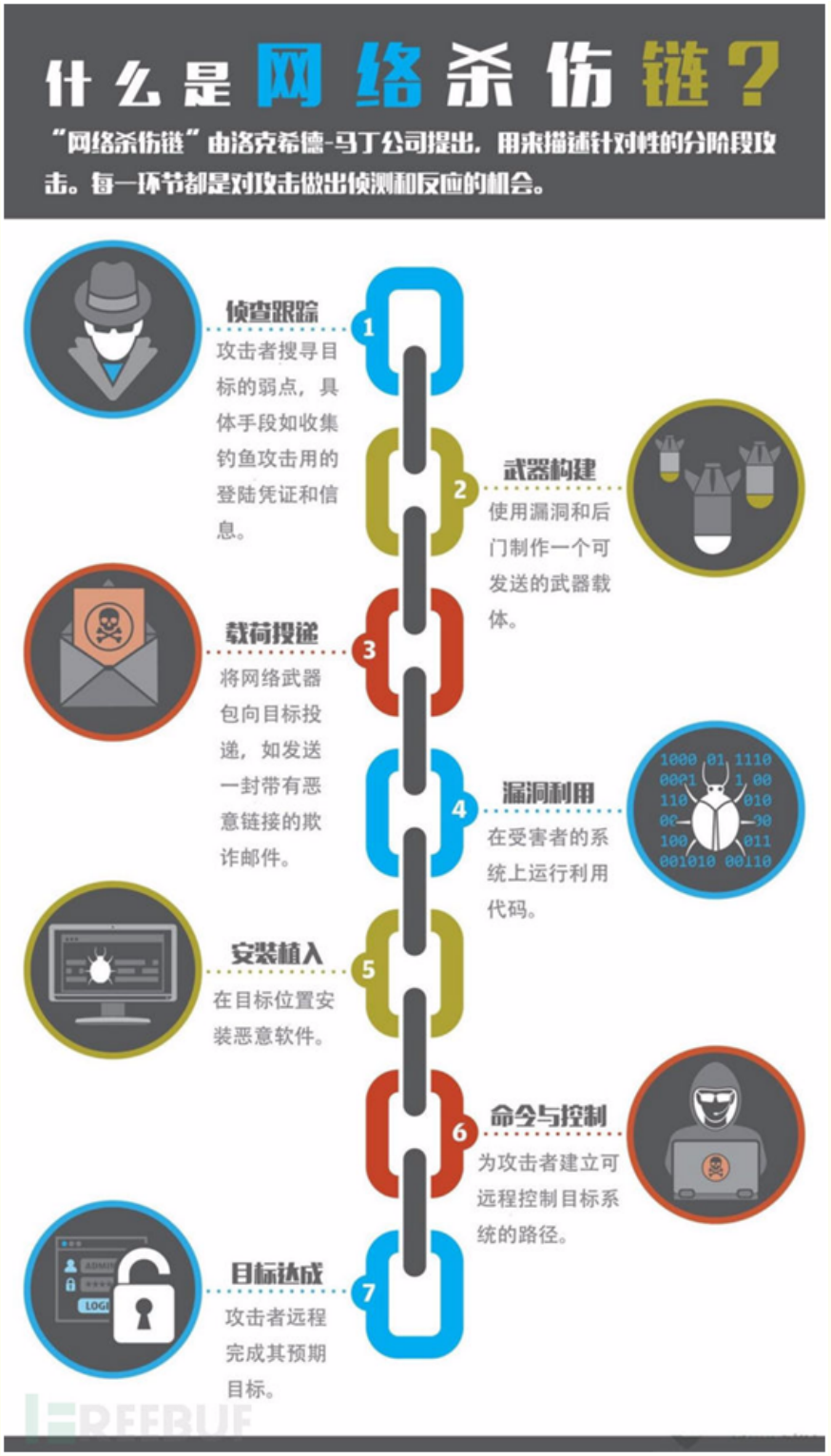
这里借用两个分析模型，一个是kill-chain七层模型，一个是钻石模型

一、什么是网络攻击杀伤链（Cyber-Kill-Chain）

“杀伤链”这个概念源自军事领域，它是一个描述攻击环节的六阶段模型，理论上也可以用来预防此类攻击（即反杀伤链）。杀伤链共有“发现-定位-跟踪-瞄准-打击-达成目标”六个环节。

在越早的杀伤链环节阻止攻击，防护效果就越好。例如，攻击者取得的信息越少，这些信息被第三人利用来发起进攻的可能性也会越低。

洛克希德-马丁公司提出的网络攻击杀伤链Cyber-Kill-Chain与此类似，本质是一种针对性的分阶段攻击。同样，这一理论可以用于网络防护，具体阶段如下图所示：



这就像传统的盗窃流程。小偷要先踩点再溜入目标建筑，一步步实行盗窃计划最终卷赃逃逸。要利用网络杀伤链来防止攻击者潜入网络环境，需要足够的情报和可见性来明了网络的风吹草动。当不该有的东西出现后，企业需要第一时间获悉，为此企业可以设置攻击警报。

另一个需要牢记的点是：在越早的杀伤链环节阻止攻击，修复的成本和时间损耗就越低。如果攻击直到进入网络环境才被阻止，那么企业就不得不修理设备并核验泄露的信息。

要想明确杀伤链技术是否适合自己的企业，不妨通过杀伤链模型的几个阶段入手，来发现企业应当核实的问题。

这就像传统的盗窃流程。小偷要先踩点再溜入目标建筑，一步步实行盗窃计划最终卷赃逃逸。要利用网络杀伤链来防止攻击者潜入网络环境，需要足够的情报和可见性来明了网络的风吹草动。当不该有的东西出现后，企业需要第一时间获悉，为此企业可以设置攻击警报。

另一个需要牢记的点是：在越早的杀伤链环节阻止攻击，修复的成本和时间损耗就越低。如果攻击直到进入网络环境才被阻止，那么企业就不得不修理设备并核验泄露的信息。

要想明确杀伤链技术是否适合自己的企业，不妨通过杀伤链模型的几个阶段入手，来发现企业应当核实的问题。

二、Cyber-Kill-Chain攻击杀伤链

对于混迹于安全圈的我们来说，洛克希德-马丁的网络杀伤链（Cyber-Kill-Chain，也被我们称网络攻击生命周期），专门用来识别和防止入侵。然而，攻击模式会一直变化，就拿Valut7来说，里面提到的攻击模型，都是在08年就已经开始在使用，而却在16年，17年才被曝光，可想而知，攻防之间的时间差是多么的严峻，所以我不给予希望一个Kill-Chain能够带来多大的安全防护，而重在开拓视野，最好能未雨绸缪，如今，Valut8已经曝光，企业安全，似乎远远没有我们想象的那么安静。

网络攻击杀伤链模型用于拆分恶意软件的每个攻击阶段，在每个阶段有对应的特征用于识别，但用我后面会提到的一句：堵不如疏，殊途同归，具体如何，后面会具体说说我自己的理解，现在先简单说说Cyber-Kill-Chain的每个阶段。

三、网络攻击杀伤链的各个阶段

Kill Chain模型将攻击者的攻击过程分解为如下七个步骤：

侦察（Reconnaissance） - 攻击者开始探测目标可能存在的弱点或不良配置

组装（Weaponization） - 攻击者开始构建一个可以传递给受害者的有效载荷（它可以是PDF文件或Office文档）

投送（Delivery） - 攻击者通过电子邮件，网页链接或可移动媒体将有效载荷发送给目标

利用（Exploit） - 有效载荷将在受害者的网络上执行

植入（Installation） - 有效载荷将下载其他远程访问工具，并安装它们以建立持久后门

命令和控制（Command and Control） - 在受害者和攻击者之间创建一个通道

收割（Actions） - 执行预期目标（如加密文件，窃取数据等）

1. ECONNAISSANCE 识别目标，信息收集

在这个阶段，犯罪分子试图确定目标的好坏。他们从外部了解企业的资源和网络环境，并确定是否值得攻击。最理想的情况是，攻击者希望目标防备薄弱、数据价值。罪犯可以找到的信息门类，以及这些信息如何被使用。

企业的信息价值往往超出他们想象。雇员的姓名和详细信息（不仅是企业网站，而且包括社交网站的信息）是否在网端存储？这些信息可以用来进行社会工程用途，比如，让人们透露用户名或密码。企业的网站服务器或物理位置是否接入网络吗？这些也可以用于社会工程，或帮助攻击者缩小企业环境漏洞的寻找范围。

这个层面上的问题很难处理，社交网络的普及让它变得尤为棘手。将敏感信息隐藏起来是一个廉价的改善方式，虽然这也增加信息调用的时间成本。

攻击方防御方特点攻击方的攻击计划阶段。他们进行研究，以了解其目标，使他们能够实现自己的目标探测侦察，因为它发生是非常困难的，但是，当守军发现侦察 - 事后甚至好 - 它可以揭示了攻击方的意图。常用攻击/防御方式获取电子邮件地址，确定员工社交媒体网络，收集新闻稿，合约奖励，会议出席者名单，探索放在公网上运行的服务器收集网站访问者日志警报和历史搜索，与网站管理员合作对其现有浏览器进行分析，建立浏览异常、行为独特的检测机制，优先周围的防御，特别是基于技术和人的侦察活动。

2. WEAPONIZATION 武器化准备工作

这些阶段是攻击者用工具攻击被选目标的具体过程，他们收集的信息将被用于恶意行为。他们手头的信息越多，社会工程攻击就越无缝可击。通过员工在LinkedIn上的信息，他们可以用鱼叉式钓鱼获得公司内部资源。或者，他们可以把远程访问木马提前嵌入可能会录入重要信息的文件里，以诱使接收者运行它。如果他们知道用户或服务器运行的软件信息，比如操作系统版本和类型，他们在企业网络里渗透和布置的把握就大大增加。

就这些阶段的防御而言，企业应当参照标准安全专家的建议去做。

企业的软件是否达到最新？这需要具体到每台终端上的每个应用。大多数公司都有某个小角落还用着老式台式机，系统仍然用的是Windows 98。如果这台设备接入网络，无异于对攻击者门洞大开。

企业使用电子邮件和网页过滤功能吗？电子邮件过滤可以有效阻止攻击中常用的文档类型。如果企业的文件必须用某种标准发送，比如密码保护的ZIP文件，这可以让用户了解文件是否无误。网页过滤则可以防止用户访问已知的不良网站或域名。

企业禁用USB设备吗？从安全的角度来看，让文件不需许可就运行绝非什么好主意。最好在运行前，确保给用户有时间暂停和思考他们所看到的情况。

企业使用端点保护软件的最新功能吗?虽然端点保护软件不是为了应对新型针对性攻击而设计，但是它们常常根据已知的可疑行为或软件漏洞来捕捉威胁。

3. 传递：传递载荷，启动运行

攻击方防御方特点在攻击方向目标传达了恶意软件之后。都将开始执行进一部分攻击操作。这是防御方阻止该操作的第一个也是最重要的机会。有效性的关键措施是阻断入侵尝试和工具传递的重要部分常用攻击/防御方式攻击方控制下传递载荷：直接针对Web服务器，攻击方释放载荷：恶意电子邮件，恶意软件的USB存储，社交媒体互动，“水坑式”钓鱼网站攻击分析和理解载荷传递的介质 - 关注上层的基础设施主要是关键基础设施，了解目标服务器和相关人员，他们的角色和责任，可用的信息，根据攻击方载荷情况推断攻击方的意图，分析“军火库”攻击载荷在传递区域检测新的恶意代码，分析在一天中的什么时间段对方开始行动，收集电子邮件和网络日志，还原取证。即使后期检测到入侵，防御方必须能够确定何时以及如何开始传递载荷。

4. 利用获取目标访问权限

攻击方防御方特点攻击方利用一个漏洞来获得访问权限（实际上可能会运用多个漏洞）。“0day”指的就是此步骤中使用的攻击漏洞。这里部署的一般是传统的防御措施，同时针对“0day”，“1day”，“Nday”等类型的漏洞增加弹性，定制化的防御能力常用攻击/防御方式软件，硬件，或人类的脆弱性，获取或发现“0day”漏洞，攻击方利用基于服务器的安全漏洞，受害者触发漏洞：点击恶意电子邮件，点击恶意链接用户安全意识培训和员工的电子邮件测试。以及邮箱服务器防护，Web开发人员的对于安全编码培训，定期扫描漏洞和渗透测试，端点防御措施：限制管理员权限，使用Microsoft EMET，自定义端点规则阻断shellcode执行，端点登录审计过程，取证确定攻击源。

5. 安装:在目标建立堡垒

通常情况下攻击方安装一个持续后门或植入，可以长时间访问目标的工具终端防御检测和记录“异常”安装活动。恶意软件分析过程中分析安装阶段的行为可以缓解攻击。常用攻击/防御方式Web服务器上安装木马后门，在目标客户端安装后门和植入，在目标上创建持续运行的服务，或者自启的服务和进程等等，有些攻击者会让一些“时间点”的文件，让恶意软件看起来它就是操作系统安装的一部分。一个好的建议：关注通用软件安装路径，例如RECYCLER，了解恶意软件是需要特权账户还是一般用户的权限，终端接入审计：去发现异常文件的创建，所有的摘录证书，主要是包含签名的可执行文件，了解恶意软件的编译时间，以确定它是旧的还是新出现的恶意软件。

5. 命令和控制(C2):远程控制和植入

一旦威胁在企业的网络环境里扎根，它的下一个任务是给老窝打电话并等待指示。它可能下载额外的组件，更有可能的是通过C&C通道联系一个僵尸网络主控机。无论哪种方式，这都要求网络流量，这意味着企业必须扪心自问：防火墙是否设置了新项目进行网络通信的警报?

如果威胁已经实现了这些，它将对机器进行更改并将耗费IT工作人员对大量精力。有些公司或行业要求诊断受影响的机器上哪些数据被窃取或篡改。受影响的机器需要进行清洗或重置。如果数据已经备份，或者有可以快速加载到机器的标准企业模式，修复工作的成本和时间损耗就会有所降低。

有些攻击会另辟蹊径

去年的攻击状况已经充分证明了一点：攻击者不会严格按照游戏流程来一一他们可能跳过步骤、添加步骤，甚至重复之前的步骤。最近的一些最具破坏性的攻击事件都是如此，这些攻击之所以能绕过安全团队耗费多年精心打造的防御体系，是因为它们有不同的流程安排。

“符合洛克希德-马丁公司的杀伤链的恶意行为被重点关注，这也让某些攻击隐形了。”Kudelski Security的全球管理服务副总裁Alton Kizziah说。
数据中心安全的领军者Alert Logic的合伙人、产品营销高级经理Misha Govshteyn指出：“杀伤链从来不能彻底符合我们看到的种种攻击。”

根据2017年威瑞森的数据泄露调查报告，今年，网络程序攻击成为了数据泄露的最常见形式，在数据泄露案例中占到了近三分之一。常见方法是利用应用程序自身的漏洞。最近的Equifax数据泄露事件就是典型例子。这种攻击很难发现。在两个月里，Equifax未在网站上发现可疑的网络流量。“通常到了数据外泄的时候，企业才能察觉。”Positive Technologies的网络安全弹性主管Leigh-Anne Galloway说。“或者，可能需要一个第三方的实体，例如某个客户，来提醒企业出了问题。”Equifax泄露案可以追溯到Apache Struts Web服务器软件中的一个漏洞。如果公司安装了这个漏洞的安全补丁，这个问题可能会避免，但是有时软件更新本身就是恶意攻击的桥梁，9月发生的CCleaner被黑事件就是一例。零日漏洞也是大麻烦。根据Contrast Security的共同创始人兼首席技术官杰夫·威廉姆斯的观点，平均每个软件应用和api拥有26.8个严重漏洞。“这是一个惊人的数字，”他说。“公众对Equifax感到愤怒，但事实是，几乎所有的公司在应用程序层都是不安全的。我们发现，世界各地有成千上万的IP地址正在进行的应用攻击尝试，这一现象正在扩散。”

要抵御这类攻击，企业必须缩短补丁的安装延迟。“过去的时候，直到应用程序漏洞被披露后的数周或数月，针对性的攻击才会出现，”他说，“但是今天，安全窗口已经只有一天左右，而在2018年，这一时间可能进一步缩减到几个小时。”他补充说，企业也需要开始将安全控件直接嵌入到应用程序里。这被称为应用程序的运行自保，Gartner预测这一细分市场的复合年增长率为9%。

“安全需要更贴近应用程序，需要深入了解程序的核心进程和内存使用量，”Virsec Systems的创始人和首席技术官Satya Gupta说。“新的流程控制技术将嵌入到应用程序层面，能理解应用的协议和环境，可以将可接受的应用程序流程绘制出来（就像谷歌地图）。如果应用程序应该从A点走到B点，但是却出现了一段意外的路程，那么肯定出错了。”

攻击者也可以利用被泄露的身份信息或强度弱的密码。这一过程不需要安装恶意软件，也不用与C&C服务器通信，不会产生横向操作。“寻找一份泄露的数据库或Amazon S3数据意味着攻击可以简便完成，从而避免和防御者交锋。”Obsidian Security的首席技术官Ben Johnson说。根据RedLock本月发布的一份报告，53%的组织使用Amazon S3等云存储服务，这至少导致了一个意外结果，即数据暴露在公众面前。今年夏天的早些时候，Skyhigh Networks报道称，7%的企业使用的所有AWS S3数据可以无限制访问，另有35%的企业未对数据加密。由于数据是通过合法渠道传出，数据防泄露可能无法检测这种行为。Govshteyn说：“企业需要专门的工具来保护针对网络应用程序的攻击。”DOS攻击也难以被杀伤链解释。“攻击者仍需选择目标，所以必须进行侦察阶段。”Cybereason的首席安全官Sam Curry说。但是在准备之后，攻击者将直接跳转到中断阶段。他补充说DOS攻击也可能只是攻击的第一步，用来掩盖其他恶意行为。“当系统崩溃时，攻击者可以创建一个漏洞，”他说，“或者创建一个高信噪的筛选器，来掩盖痕迹或破坏系统的信号发现能力。”他说，攻击者也可以添加步骤到游戏流程里。例如，他们可以花时间清理痕迹、设置中断、传播虚假数据，或安装未来用得上的后门。他们也可以重新安排各步骤的顺序，或者重复之前的步骤。这不是一个简单的线性过程。这通常更像树状或根系的分支和蔓延，这一过程很复杂，会发生很多事情。

攻击方防御方特点恶意软件将打开通信信道，以使攻击方远程操作目标。向C2目标开放双向通信通道基础设施；防御的最后一个最佳时机-阻止C2操作：“通过阻断C2通道”。如果攻击方不能通过通信信道发出命令，相应的防御方就可以实现阻断C2攻击常用攻击/防御方式最常见的C2渠道涉及web，DNS和电子邮件协议，C2基础设施可能被攻击方或目标自身所拥有通过全面的恶意软件分析工具去发现部署和执行了C2的基础设施强化网络：汇总所有存在的互联网点，规范所有类型的代理流量（HTTP，DNS等）；自定义C2模块：网络代理协议；代理类模块，包括“none”或“未分类”的域；DNS穿透和域名服务器毒化防御；实施开源研究发现新的C2攻击方式。

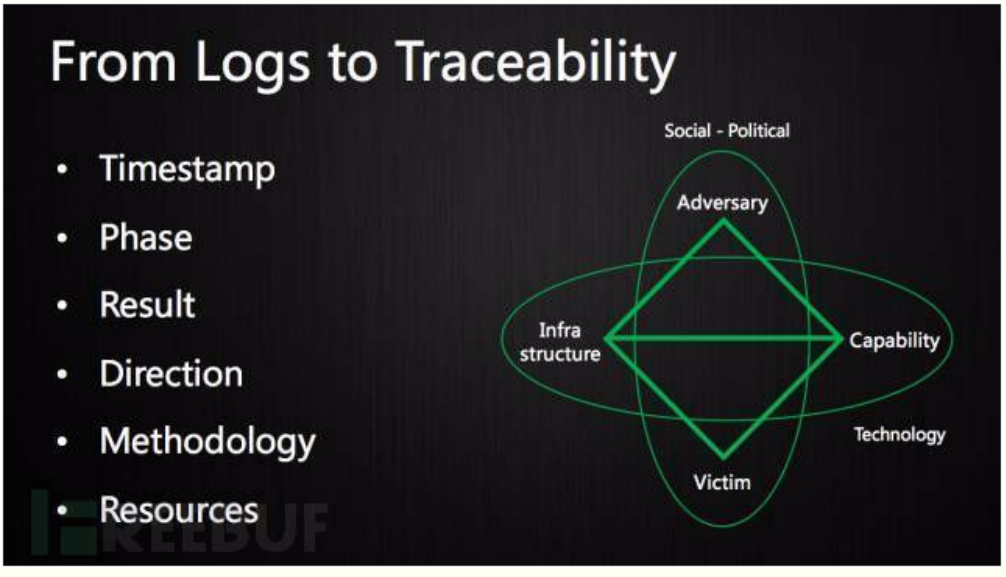
6. 行动:使命必达，不达目的，誓不罢休

在拒绝服务攻击案例中，中断不一定是攻击的最后一步。在攻击者成功地破坏、瘫痪或渗入系统后，攻击者可以重复这一过程。也可以转移到另一个阶段——盈利。Preempt Security的首席执行官 Ajit Sancheti 认为，攻击者可能采取任意形式的组合。比如，他们可以通过破坏基础设施来进行广告欺诈或发送垃圾邮件、向企业勒索赎金、出售他们在黑市上获得的数据，甚至劫持基础设施出租给其他罪犯。“攻击的盈利已经急剧增加。”他补充说，比特币的使用让攻击者更简便、安全地得到钱，这导致了攻击动机的变化。不同群体的数量参与也让黑市上被盗数据的消费变得更加复杂。这也为企业、执法部门和其他组织创造了合作破坏这一过程的机会。以被盗的支付卡信息为例。“一旦信用卡数据被盗，这些数据必须被测试、出售、用于获取商品或服务，反过来这些商品或服务必须转换为现金。”Splunk公司的安全研究主管Monzy Merza说。这一切都早已超出了传统网络杀伤链的范畴。黑市生态系统也在影响了网络攻击周期中的攻击准备环节。攻击者们会分享身份凭证列表、漏洞或被修改的应用程序。

攻击方防御方特点激活键盘接入激活键盘接入，入侵者完成任务的目标。接下来会发生什么将取决于谁是在键盘上。较长的攻击方有CKC7访问，更大的影响。包括网络数据包捕获，进行损失评估 - 防御方必须通过取证去尽可能快地检测到这一阶段常用攻击/防御方式收集用户凭据，权限提升，内部侦查，横向内网渗透，收集和传出数据，破坏系统，覆盖或破坏数据，偷偷修改数据制定事件响应流程，包括行政参与和沟通计划。检测数据泄露，横向传输，未经授权证书的使用。即时响应分析反馈所有事件告警。预先部署监控节点端点快速分流。网络包捕获，还原攻击活动。让专家进行事件损害评估

四、钻石模型

钻石模型是一个针对单个事件分析的模型，核心就是用来描述攻击者的技战术和目的，具体的钻石模型如下图所示：



钻石模型由三部分组成：置信度、元数据、社会-政治影响和技战术组合

社会政治影响：处于钻石模型上下两个顶点，上顶点表示攻击者，下顶点表示受害者也就是目标。攻击者和受害者之间的某种利益冲突或者是社会地位对立则会产生攻击的意图和发起攻击的原因，纵切面表示的就是社会政治影响。说大白话就是根据这俩人去发现攻击的意图。

技战术组合：技战术组合位于整个钻石模型的横切面，横切面的两个顶点分别为基础设施和技术能力，这里的基础设施和技术能力其实都是相对于攻击者而言的。

元数据：这个其实就是左边列出来的，攻击时间、攻击阶段、攻击结果、攻击方向、攻击手段、攻击资源利用。

置信度：也就是以上你分析出结果的可信程度。

钻石模型想要表达的其实就是针对单个安全事件，我们可以得到攻击者为什么想要攻击目标，打算用什么手段去攻击目标。

0x09 APT常用漏洞

1、Office漏洞

Office漏洞依然是大部分APT组织最喜爱的漏洞，Office在个人办公电脑使用量大，对针对性目标是最佳的外网入口，效果也是最直接的。你可能想到了办公套件这类神器，正所谓：最大的漏洞不是存在于任何系统上面，而是人。

CVE编号	漏洞类型	使用组织
CVE-2009-2496	堆损耗远程代码执行漏洞，又称作“Office Web 组件堆损耗漏洞“	丰收行动
CVE-2010-3333	RTF分析器堆栈溢出漏洞，又称”RTF栈缓冲区溢出漏洞”	
CVE-2012-0158	Microsoft Windows Common Controls ActiveX控件远程代码执行漏洞，栈内存拷贝溢出漏洞，又称“MSCOMCTL.OCX RCE漏洞”	摩诃草 蔓灵花 白象 Rotten Tomato
CVE-2013-3906	Microsoft Graphics组件处理特制的TIFF图形时存在远程代码执行漏洞	摩诃草 白象
CVE-2014-1761	Microsoft Word RTF文件解析错误代码执行漏洞	摩诃草 Pitty Tiger 白象 Rotten Tomato
CVE-2014-4114	OLE包管理INF 任意代码执行漏洞	摩诃草 白象
CVE-2015-1641	RTF解析中的类型混淆漏洞	MONSOON 摩诃草 白象 奇幻熊 Rotten Tomato 丰收行动
CVE-2015-2545	EPS图形文件任意执行代码	Rotten Tomato
CVE-2015-2546	UAF（释放后重用）漏洞	

CVE编号	漏洞类型	使用组织
CVE-2016-7193	RTF文件解析漏洞，可远程执行任意代码	
CVE-2017-0199	首个Microsoft Office RTF漏洞	暗黑客栈
CVE-2017-0261	EPS中的UAF漏洞	摩诃草 白象 Turla
CVE-2017-0262	EPS中的类型混淆漏洞	摩诃草 白象
CVE-2017-11826	OOXML解析器类型混淆漏洞	东亚某组织
CVE-2017-11882	“噩梦公式”公式编辑器中的栈溢出漏洞，可远程代码执行	白象 响尾蛇 寄生兽 摩诃草 人面马 黑凤梨
CVE-2017-8464	解析快捷方式时存在远程执行任意代码的高危漏洞	
CVE-2017-8570	OLE对象中的逻辑漏洞 (CVE-2017-0199的补丁绕过)，“沙虫”二代漏洞	白象 寄生兽 摩诃草
CVE-2017-8759	.NET Framework中的逻辑漏洞	
CVE-2018-0802	“噩梦公式二代”利用office内嵌的公式编辑器EQNEDT32.EXE发起攻击	黑凤梨
CVE-2018-8174	利用浏览器0day漏洞的新型Office文档攻击	

2、Adobe 系漏洞

Adobe系列包括Adobe Reader、Acrobat、Flash Player，Flash Player因为其跨平台，使用广泛，一直也受到各大APT组织的关注。

CVE编号	漏洞类型	影响版本	使用组织
CVE-2007-5659	Adobe Acrobat/Reader PDF文件 多个缓冲区溢出漏洞	Adobe Acrobat 8 Adobe Reader 8 Adobe Reader 7	丰收行动
CVE-2008-2992	Adobe Reader util.printf() JavaScript函数栈溢出漏洞	Adobe Acrobat < 8.1.3 Adobe Reader < 8.1.3	丰收行动

CVE编号	漏洞类型	影响版本	使用组织
CVE-2009-0927	Adobe Acrobat和Reader Collab getIcon() JavaScript方式栈溢出漏洞	Adobe Acrobat 9 Adobe Acrobat 8 Adobe Acrobat 7.0 Adobe Reader 9 Adobe Reader 8 Adobe Reader 7	丰收行动
CVE-2009-4324	Adobe Reader和Acrobat newplayer() JavaScript方式内存破坏漏洞	Adobe Acrobat <= 9.2 Adobe Reader <= 9.2	丰收行动
CVE-2010-0188	Adobe Reader和Acrobat TIFF图像处理缓冲区溢出漏洞	Adobe Acrobat < 9.3.1 Adobe Acrobat < 8.2.1 Adobe Reader < 9.3.1 Adobe Reader < 8.2.1	丰收行动
CVE-2010-3653	Adobe Shockwave Player Director文件rcsL块解析内存破坏漏洞	Adobe Shockwave Player 11.5.8.612	丰收行动
CVE-2012-0773	Adobe Flash Player / AIR NetStream类任意代码执行或拒绝服务漏洞	Adobe Flash Player 11.x Adobe AIR 3.x	The mask
CVE-2013-0640	Adobe Acrobat和Reader远程代码执行漏洞	Adobe Acrobat 9.x Adobe Acrobat 11.x Adobe Acrobat 10.x Adobe Reader 9.x Adobe Reader 11.x Adobe Reader 10.x	丰收行动
CVE-2014-0497	Adobe Flash Player远程代码执行漏洞	Adobe Flash Player 12.x Adobe Flash Player 11.x	暗黑客栈
CVE-2015-5119	Adobe Flash Player ActionScript 3 ByteArray释放后重用远程漏洞	Adobe Flash Player <= 18.0.0.194 Adobe Flash Player <= 18.0.0.194 Adobe Flash Player Extended Support Release 13.x Adobe Flash Player Extended Support Release 13.0.0.296 Adobe Flash Player for Linux 11.x Adobe Flash Player for Linux 11.2.202.468	蓝白蚁 Hacking Team

CVE编号	漏洞类型	影响版本	使用组织
CVE-2015-8651	Adobe Flash Player整数溢出漏洞	Adobe Flash Player < 18.0.0.324 Adobe Flash Player < 11.2.202.559 Adobe Flash Player 20.x-20.0.0.267 Adobe Flash Player 19.x Adobe AIR < 20.0.0.233	暗黑客栈
CVE-2016-0984	Adobe Flash远程代码执行漏洞	Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306	BlackOasis
CVE-2016-4117	Adobe Flash Player 任意代码执行漏洞	Adobe Flash Player <= 21.0.0.226	奇幻熊
CVE-2016-7855	Adobe Flash Player 释放后重利用远程代码执行漏洞	Adobe Flash Player <= 23.0.0.185 Adobe Flash Player <= 11.2.202.637	
CVE-2017-11292	类型混淆漏洞导致的远程代码执行	Adobe Flash Player Desktop Runtime Adobe Flash Player for Google Chrome Adobe Flash Player for Microsoft Edge and Internet Explorer 11 Adobe Flash Player Desktop Runtime	黑色绿洲 Lazarus
CVE-2018-4878	Adobe Flash Player释放后重利用远程代码执行漏洞	Adobe Flash Player <= 28.0.0.137	Lazarus

3、IE漏洞

浏览器是用户接入互联网的门户，IE浏览器是Windows系统的默认浏览器，IE浏览器漏洞的使用一直也受各大组织喜爱。

CVE编号	漏洞类型	影响版本	使用组织
CVE-2010-0806	Microsoft IE畸形对象操作内存破坏漏洞	Microsoft Internet Explorer 7.0 Microsoft Internet Explorer 6.0 SP1 Microsoft Internet Explorer 6.0	丰收行动

CVE编号	漏洞类型	影响版本	使用组织
CVE-2010-3962	Microsoft IE CSS标签解析远程代码执行漏洞	Microsoft Internet Explorer 8.0 Microsoft Internet Explorer 7.0 Microsoft Internet Explorer 6.0	丰收行动
CVE-2012-4792	Microsoft IE mshtml!CButton对象释放后重用代码执行漏洞	Internet Explorer 6Internet Explorer 7Internet Explorer 8	摩诃草
CVE-2014-0322	Microsoft Internet Explorer释放后重用远程代码执行漏洞	Microsoft Internet Explorer 10	Pitty Tiger
CVE-2016-7279	Microsoft Internet Explorer/Edge远程内存破坏漏洞	Microsoft Edge	
CVE-2017-8618	Microsoft Internet Explorer远程代码执行漏洞	Microsoft Internet Explorer 9 Microsoft Internet Explorer 11 Microsoft Internet Explorer 10	
CVE-2018-0978	Microsoft Internet Explorer远程内存破坏漏洞	Microsoft Internet Explorer 9-11	
CVE-2018-8113	Microsoft Internet Explorer安全限制绕过漏洞	Microsoft Internet Explorer 11	
CVE-2018-8178	Microsoft Internet Explorer/Edge 远程内存破坏漏洞	Microsoft Edge Microsoft ChakraCore	

4、防火墙设备漏洞

2016年8月13日客组织ShadowBrokers声称攻破了为NSA开发网络武器的黑客团队Equation Group，并公开其内部使用的相关工具，EXBA-extrabacon工具，该工具基于0-day漏洞CVE-2016-6366，为Cisco防火墙SNMP服务模块的一处缓冲区溢出漏洞

CVE-2016-6366（基于Cisco防火墙SNMP服务模块的一处缓冲区溢出漏洞），目标设备必须配置并启用SNMP协议，同时必须知道SNMP的通信码，漏洞执行之后可关闭防火墙对Telnet/SSH的认证，从而允许攻击者进行未授权的操作。

CVE编号	漏洞说明
CVE-2016-6366	SNMP服务模块的一处缓冲区溢出漏洞
CVE-2016-6367	远程代码执行

5、SMB通信协议漏洞

EternalBlue工具使用了SMB协议中的三处漏洞，其中主体的越界内存写漏洞隶属于微软MS17-010补丁包中的CVE-2017-0144，通过该集成的工具，攻击者可以直接远程获取漏洞机器的控制权限。

EternalBlue中的核心了漏洞为CVE-2017-0144，该漏洞通过SMB协议的SMB_COM_TRANSACTION2命令触发，当其中的FEALIST字段长度大于10000时将导致内存越界写，由于SMB_COM_TRANSACTION2命令本身FEA LIST的长度最大为FFFF，因此这里就涉及到第二处漏洞，即SMB_COM_TRANSACTION2可被混淆为SMB_COM_NT_TRANSACT，从而实现发送一个FEA LIST字段长度大于10000的SMB_COM_TRANSACTION2命令，实现越界写，最后通过第三个漏洞进行内存布局，最终实现代码执行。

CVE编号	漏洞说明
CVE-2017-0143 CVE-2017-0144 CVE-2017-0145 CVE-2017-0146 CVE-2017-0148	SMB协议漏洞

6 、OOXML类型混淆漏洞

OOXML是微软公司为Office2007产品开发的技术规范，现已成为国际文档格式标准，兼容前国际标准开放文档格式和中国文档标准“标文通”，Office富文本中本身包含了大量的XML文件，由于设计不当，在对其中的XML文件进行处理的时候，出现了严重的混淆漏洞，最典型的包括CVE-2015-1641，CVE-2017-11826，这里我们选择近年来最流行的OOXML类型混淆漏洞CVE-2015-1641作为典型代表。

2015年4月，微软修补了一个CVE编号为CVE-2015-1641的Office Word类型混淆漏洞。OfficeWord在解析Docx文档displacedByCustomXML属性时未对customXML对象进行验证，造成类型混淆，导致任意内存写，最终经过精心构造的标签以及对应的属性值可以造成远程任意代码执行。这是第一个利用成功率非常高且被APT组织频繁使用的OOXML类型混淆漏洞。

CVE-2015-1641中，由于OfficeWord没有对传入的customXML对象进行严格的校验，导致可以传入比如smartTag之类的对象，然而smartTag对象的处理流程和customXML并不相同，如果customXML标签被smartTag标签通过某种方法混淆解析，那么smartTag标签中的element属性值会被当作是一个地址，随后经过简单的计算得到另一个地址。最后处理流程会将moveFromRangeEnd的id值覆盖到之前计算出来的地址中，导致任意内存写入。然后通过写入可控的函数指针，以及通过Heap Spray精心构造内存布局，最终导致代码执行。

CVE编号	漏洞说明
CVE-2015-1641	customXML对象类型混淆
CVE-2017-11826	XML中的idmap标签计算错误导致混淆

7 、EPS（EncapsulatedPost Script）脚本解析漏洞

EPS全称EncapsulatedPost Script，属于PostScript的延伸类型，适用于在多平台及高分别率输出设备上进行色彩精确的位图及向量输出，因此在Office中也引进了相应的支持，但是自2015年起多个Office中EPS相关的漏洞被利用，其中包括CVE-2015-2545，CVE-2017-0261，CVE-2017-0262，最终导致微软不得不禁用Office中的EPS组件，而此处我们选择以CVE-2017-0262作为典型代表。

2017年5月7日FireEye研究员在文章EPSProcessing Zero-Days Exploited by Multiple Threat Actors中披露了多个EPS0-day漏洞的在野利用，其中就包含CVE-2017-0262，CVE-2017-0262为ESP中forall指令中的一处漏洞，由于forall指令对参数校验不当，导致代码执行。

CVE-2017-0262的利用样本中首先对实际的EXP进行了四字节的xor编码，key为c45d6491：

漏洞的关键点在于以下一行的代码，在EPS中forall指令会对第一个参数中的每一个对象执行处理函数proc（即第二个参数），此处由于对第二个参数的类型判断不严格，导致0xD80D020这个攻击者之前通过堆喷控制的内存地址被作为处理函数的地址，从而esp堆栈被控制，致使最后的代码执行：

```
1 array 226545696 forall % 226545696 = 0xD80D020
```

CVE编号	漏洞说明
CVE-2015-2545	UAF漏洞
CVE-2017-0261	Save，restore指令中的UAF漏洞
CVE-2017-0262	forall参数类型校验不严格导致代码执行

8、Windows提权漏洞

在对Office办公软件的EPS（EncapsulatedPost Script）组件进行漏洞攻击的过程中，由于Office 2010及其高版本上的EPS脚本过滤器进程fltldr.exe被保护在低权限沙盒内，要攻破其中的低权限沙盒保护措施，攻击者就必须要使用远程代码执行漏洞配合内核提权漏洞进行组合攻击。所以我们选择Win32k.sys中的本地权限提升漏洞（CVE-2017-0263）这一个配合EPS类型混淆漏洞（CVE-2017-0262）进行组合攻击的提权漏洞作为典型代表。

CVE-2017-0263漏洞利用代码首先会创建三个PopupMenus，并添加相应的菜单。由于该UAF漏洞出现在内核的WM_NCDESTROY事件中，并会覆盖wnd2的tagWnd结构，这样可以设置bServerSideWindowProc标志。一旦设置了bServerSideWindowProc，用户模式的WndProc过程就会被视为内核回调函数，所以会从内核上下文中进行调用。而此时的WndProc则被攻击者替换成了内核ShellCode，最终完成提权攻击。

引入了"沙盒"保护的常客户端程序有：IE/Edge浏览器、Chrome浏览器、Adobe Reader、微软Office办公软件等等。而客户端程序漏洞如果配合Windows提权漏洞则可以穿透应用程序"沙盒"保护。

CVE编号	漏洞说明
CVE-2015-2546	Win32k内存损坏特权提升漏洞
CVE-2016-7255	Win32k本地权限提升漏洞
CVE-2017-0001	Windows GDI权限提升漏洞
CVE-2017-0263	Win32k释放后重用特权提升漏洞

9 、Flash漏洞

Flashplayer因为其跨平台的普及性，一直为各个APT组织关注，从2014年起，Flash漏洞开始爆发，尤其到2015年，HackingTeam泄露数据中两枚0-day漏洞CVE-2015-5122/CVE-2015-5199，Flash漏洞相关的利用技术公开，Flash漏洞开始成为APT组织的新宠，尽管之后Adobe和Google合作，多个Flash安全机制陆续出炉（如隔离堆，vector length检测），大大提高了Flash漏洞利用的门槛，但也不乏出现CVE-2015-7645这一类混淆漏洞的怪咖。这里我们选择不久前发现的在野0-day CVE-2018-4878作为这类漏洞的典型代表。

2018年1月31日，韩国CERT发布公告称发现Flash0day漏洞（CVE-2018-4878）的野外利用，攻击者通过发送包含嵌入恶意Flash对象的Office Word附件对指定目标进行攻击。

CVE-2018-4878通过Flash om.adobe.tvsdk包中的DRMManager对象进行攻击，如下代码所示，triggeruaf函数中创建一个MyListener对象实例，通过initialize进行初始化，并将该实例设置为null，之后的第一个LocalConnection().connect()会导致gc回收该实例内存，第二次LocalConnection().connect()时触发异常，在异常处理中会创建一个新的MyListener实例，内存管理器会将之前MyListener对象实例的内存分配给新对象，即此处的danglingpointer，设置timer，在其回调函数中检测uaf是否触发，成功则通过Mem_Arr进行站位：

CVE编号	漏洞说明
CVE-2017-11292	UAF
CVE-2018-4878	UAF

10、iOS三叉戟漏洞

iOS三叉戟漏洞是指针对iOS9.3.5版本之前的iOS系统的一系列0 day漏洞，其利用了3个0 day漏洞，包括一个WebKit漏洞，一个内核地址泄露漏洞和一个提权漏洞。通过组合利用三个0 day漏洞可以实现远程对iOS设备的越狱，并且安装运行任意恶意代码。

iOS三叉戟漏洞利用载荷可以通过访问特定的URL触发，所以可以通过短信、邮件、社交网络或者即时通讯等发送恶意链接诱导目标人员点击打开链接实现漏洞的触发。由于WebKit JavaScriptCore库存在任意代码执行漏洞，当Safari浏览器访问恶意链接并触发恶意的JavaScript载荷执行，其利用代码进入Safari WebContent进程空间。其随后利用另外两个漏洞实现权限提升，并越狱掉iOS设备。最后三叉戟漏洞可以实现下载和运行用于持久性控制的恶意模块。

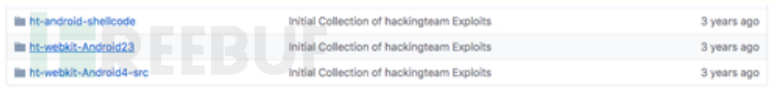
iOS三叉戟漏洞涉及3个0 day漏洞，其CVE编号及相关信息如下表所示：

CVE编号	漏洞说明
CVE-2016-4655	内核信息泄露
CVE-2016-4656	提权
CVE-2016-4657	WebKit远程代码执行

11、Android浏览器remote2local漏洞利用

Android浏览器remote2local漏洞利用是2015年7月Hacking Team遭受入侵并泄露内部源代码资料事件后，其泄露源代码中包含了针对Android 4.0.x-4.3.x系统版本的浏览器的攻击利用代码，其可以达到远程代码执行，并执行提权代码提升至root权限，最后达到静默安装恶意程序的目的。该漏洞利用代码几乎可以影响当时绝大多数主流的Android设备和系统版本。

该漏洞利用的组合了GoogleChrome的三个N-day漏洞和针对Android系统的提权漏洞完成完整的利用攻击过程。



该Android浏览器漏洞利用主要因为WebKit中关于XML语言解析和XSLT转换的libxslt库，其利用过程实际上是基于多个漏洞的组合利用过程。其首先利用一个信息泄露漏洞获取内存地址相关信息，并利用内存任意读写构造ROP攻击最终实现执行任意代码的目的。其最后执行提权代码，该漏洞利用中使用的提权漏洞为CVE-2014-3153，其产生于内核的Futex系统调用。当提权获得root权限以后，执行静默安装恶意APK应用。

Hacking Team的针对Android浏览器的remote2local漏洞利用工具结合了3个针对浏览器的漏洞和2个用于提权的漏洞。

CVE编号	漏洞说明
CVE-2011-1202	信息泄露
CVE-2012-2825	任意内存读
CVE-2012-2871	堆溢出
CVE-2014-3153	提权漏洞
CVE-2013-6282	内核任意地址读写

0x10 APT具体攻击手法

1、信息搜集

1.1.公开信息搜集

目标主要域名、二级三级域名与IP以及端口开放情况
目标经营范围、合作对象、是否存在外包
目标暴露在公网的邮箱、账号密码、手机号码等敏感信息
目标上级路由出口、ASN节点下IP范围
目标是否托管，如托管，则确定托管供应商
目标国家行业普遍使用的软件，如聊天工具，文件传输工具，SSH连接工具，下载工具等
确定打击范围，确定所要获取的信息归属目标企业哪个部门，哪个人手里
确定具体打击范围后，搜集精准目标的个人爱好，如喜欢吃的水果或零食，个人爱好，常浏览哪个网站，目

标家人是谁，家人什么工作，家人的以上各种信息

搜集目标所在国家生活作息习惯，如几点上班，几点吃饭，几点休息，目标所在国家密码规律习惯等

确定目标邮箱等信息后，尝试从公开或私有社工库中查询目标已经泄露的密码

搜集以上信息后针对目标密码规律进行生成针对性密码

1.2.非公开信息

可尝试对目标常浏览站点进行渗透，获取目标密码

搜集以上信息后使用目标泄露的密码尝试登陆，注意目标作息时间!

对目标企业或机构公开邮箱搜集后，根据MX记录找到邮箱地址并利用目标所在国家密码行为习惯进行爆破

如爆破成功，第一时间查找是否有VPN账号密码信息，如没有，则检查是否存在其它业务系统或远程连接账号密码信息

如果进入的邮箱中有VPN账号密码信息，切记先不要尝试连接，先搞清楚目标主体VPN连接方式，如有操作文档，先看一遍操作文档

进入目标或目标主体其他人员邮箱后，搜集目标主体日常相关工作，如会议主题、文档、内容，日常工作安排、人员调动

进入目标或目标主体其他人员邮箱后，搜集目标主体的内部系统连接方式，如url、认证方式等

如果你够细心，你会发现一些员工的日常行为习惯或说话语气口吻等个人提点

如VPN、账号密码都没有的情况下，则查看相同企业邮箱往来邮件头部信息，邮件头会包含发件人IP等信息

1.3.运用社会工程学

如果不能确定具体人员，则可对目标主体公开且对外联系邮箱发送邮件获取目标出口IP，可根据以上搜集的信息制定邮件钓鱼攻击，举个例子，如国内每个企业都要交税和社保五险一金，当社保或公积金管理机构发布新的规章制度时，各企业都会进行关注

可尝试与目标建立长期的联系，以朋友或合作伙伴身份去了解目标的行为习惯、日常轨迹或忧喜哀愁，并制定攻击手段与计划

可利用目标心里白名单的弱点进行攻击，如目标家人或朋友邮箱、即时聊天工具对目标发送带有木马的链接、软件、邮件

发送钓鱼邮件或含有木马的邮件附件时，可结合暗示心理学进行攻击

2、悄悄撕出一条口子

如果以上信息搜集后，有了目标的VPN或目标企业人员PC被成功控制后，该如何做到不惊动目标?

2.1.web应用

可以先尝试目标是否存在phpinfo.php,info.php等敏感的信息泄露，因为这种文件如果是使用的phpinfo()函数，是可以显示目标域名真正IP的，一步错，步步错，如果你不仔细的进行信息搜集，说不定最后你干掉的只不过是对方使用的CDN节点,CDN厂商知道了也会骂娘的

按照个人经验来讲，第一，确定目标是否有可以上传shell或命令执行的漏洞，如果有，则不需要费那么大的周折去攻破

按照漏洞危害来寻找和挖掘：命令执行、文件上传、文件下载、注入，当然，文件下载，可以把目标源代码弄回来进行审计，注入则可能需要寻找后台或者破解加密后的密码，其中的细节想必不用我说，各位也都了解

那么，如果真的到了可以上传web后门那一步，则切记，不可使用网络公开的"大马"或一句话后门，如果使用了，则还需要承担你所使用的后门存在后门的可能，还有最主要的是，目前公开的，都已经在个大防护产品"病毒库"里了，你刚上传，就会被拦截或报警，就算侥幸成功，流量检测这一关也会过不了，目标网络防护low的一逼另说，还有个不能用的原因，那就是，TM的China黑客超级喜欢用一句话后门.....

如果需要扫描，可以适当的检查下有没有MS17-010这种漏洞，反正扫描的时候动作尽量要小

2.1.邮箱

如果成功进入目标主体其他人员邮箱， 切记，翻看邮件后，对原有的未读邮件标记为未读，更不可删除邮箱内任何邮件，哪怕是垃圾邮件也不可！！！

进入邮箱后，用最快的速度把联系人详细信息拖出来，后续可参考1.2进行

2.2.VPN

如果有了目标VPN信息，并且熟悉了操作文档后，切记一定要模拟正常员工登录，要让目标主体VPN认证系统留下的记录看起来是VPN账号主人在连接，连接成功后，不要对所在网段一顿乱扫，要不然你都不知道你是怎么死的，可以先尝试访问之前搜集到的url或认证系统，如果可以访问，则证明成功进入目标内部，当然其它情况另说

如果需要扫描，可以适当的检查下有没有MS17-010这种漏洞，反正扫描的时候动作尽量要小

如果可以确定具体目标内部IP，则可谨慎对其进行渗透，成功进入后，可尝试获取目标内部存活主机，记住不要用nmap这种并大量大而且开源的工具，如果有流量检测，必死，亦不可直接ARP、DNS欺骗，如果你这样做，那么你必惊动目标，可尝试arp -a看下ARP缓存列表或netstat -an 查看当前网络连接

如果成功获取目标内部存活主机后，首先排除个人PC不能动！如想继续，可以尝试使用VPN密码去登录存活server的3389或SSH，当然前提要注意目标所在地理位置的生活作息习惯，要不然管理人员在线你尝试成功了，管理被踢了肯定是不正常的

2.3.水坑

如果第一部分信息搜集结果比较完善的话，相信你已经掌握了具体目标常浏览的站点了，此时可以对这些站点进行渗透，等待目标上钩

原因?

A：拿下目标常浏览站点后，可以利用目标浏览器漏洞直接拿下其PC权限

B：可以冒充客服或管理人员以各种理由让对方交出权限，如对目标IP浏览行为进行拦截，并配上对应提示，然后以测试网络连通性为由给对方发送“专业”检测软件，还可以以送礼物为由邮寄“特殊”的U盘、平板电脑、手机

C：就算目标不上钩，你也可以得到目标在该站点的密码，如果多拿下几个，就可以发现目标的密码规律进行爆破，如果是无法“解密”的加密密码，亦可以告诉目标账户有风险，然后让其去你给的站点修改密码，可以是官方站点，但是需要抓包，也可以是钓鱼站点，比如利用HTML的a标签进行视觉欺骗

2.4.个人PC

如果拿到了目标PC的控制权，切记不可触动目标电脑上的杀软，要不然他一时兴起来个在线云查杀，你不得蹲墙角哭去，可以先将目标电脑的特殊文件进行窃取，如.doc .xls .zip .txt等你感兴趣的文件，不要修改目标电脑上明显的文件内容或属性，如果比如要修改，那么，记得把修改时间调下。

可以准备百度木马，防止目标会接触那些物理隔离并且无法访问公网的计算机

如果目标拿着自己的电脑接入公司的网络，也不要大范围扫描，可以适当的检查下有没有MS17-010这种漏洞，动作要小

2.5.不知道用啥标题了

简单明了，结合以上几点需要谨慎又谨慎的注意事项后，直接纵向杀入，要拿数据就拿数据，要控目标就控目标，别墨迹，越墨迹越容易暴露，但是，动作要小！！！

3、稳固权限

想长期控制，肯定是要稳固权限的，要不然哪天掉了总不能按照一开始的口子进去再这种嗅探种马社工吧，麻烦又容易暴露，下边说下几点

3.1.定制后门

为什么？说点实际的，如果你后门叫svchost.exe，中英文之类的系统里肉眼看上去没问题，但是TM的法语就不行了，坑爹的大坑，就说administrators用户组吧，中英文里管理员用户组是这个，但是TM的法语里却是别的，具体的我忘了是什么，不信自己安装个法语的试下

3.2.精简勿用开源

为什么精简？目标网络内网中的内网，传输速率小的可怜，你生成个几兆的后门传上去？？？

越精简体积越小，支持的功能越少，越减少暴露几率，当然看程序员水平

为什么说不要用开源的，呃，不在乎暴露的话你随便..

3.4.不带任何特征

不要用你母语，要不然，xxx国家黑客入侵xxx机构xxx企业窃取机密，外交也会尴尬吧...

不要带有任何组织或个人称呼之类的东西，无论是后门还是控制端，给你们看个例子:http://www.freebuf.com/articles/network/183631.html

3.5.通信要隐秘

如果走http通道，数据不要直接在cookie里这么慢明显的地方

DNS也是一样，能加密的加密，别明文

心跳包别太明显，流量检测不是闹着玩的

别没事就连上去，会增加暴露几率，如非必要，尽量不要连接

3.6.不落地

原因？自己去想

4、传输数据

回传数据也是要注意的，如果对方都下班睡觉了，你去下载内部数据，流量还那么大，傻子都知道有问题

尽量在对方正常运营时间内用正常的请求去下载，如果内容太大，也不要急于求成

不要用迅雷之类的软件去下载，1.会缓存到他们的server上，同时会暴露你的地理位置，因为你怎么知道迅雷之类的软件没有被控？？？

传输文件要加密，同时尽量不要再目标server上安装软件，能免安装就免安装

0x11 APT防御手段

目前业界比较流行的防御APT思路有三种：

1、采用高级检测技术和关联数据分析来发现APT行为，典型的公司是FireEye；

2、采用数据加密和数据防泄密(DLP)来防止敏感数据外泄，典型的公司是赛门铁克；

3、采用身份认证和用户权限管理技术，严格管控内网对核心数据和业务的访问，典型的公司是RSA。

企业应对防御具体措施：

（1）网络设备和服务

1. 合理配置边防设备，例如防火墙。具备基本的出入过滤功能，条件允许的实况下使用屏蔽子网结构。防火墙策略按照默认拒绝。如果愿意安装入侵检测系统更好。

2. 使用有相关安全技术的路由器，例如很多新的路由器有一定的抗ARP攻击的能力。

3. 善于使用代理服务器（例如反向代理）、web网关（例如一些检测xss的软件）

4. 内部的办公工作，设计为只有内网用户可以进行。有子公司的情况下，使用VPN技术。

5. 邮件系统要具有防假冒邮件、防垃圾邮件的基本能力。

6. 全网内的终端机器，至少使用可靠可更新的安全反病毒软件。

7. 不必要的情况下，企业内部不要配置公共Wifi。如果需要，限制公共Wifi的权限，使用有效密码，至少使用WPA2的安全设置，条件允许可以隐藏SSID。

8. 企业内部的通讯使用加密，对抗监听和中间人。

（2）安全管理

1. 企业建立安全策略，分配职责，雇佣背景清晰的安全工作人员。

2. 企业制度允许的情况下，合理运用强制休假、岗位轮换的方法。

3. 企业有一定权限的管理人员（例如人事部门），要合理分权，最小权限，不能集中某一些人都有最高的权限，特别领导同志要主动放弃最高权限。

4. 入职和离职的时候要仔细检查，例如离职时要有人监督他收拾东西离开，避免最后一刻留下后门，还要及时清除他的账户。使用证书的企业，还要停止他的证书。

5. 要建立日志审核的制度，有专门的人员审核边防设备记录的重要信息。

6. 企业架设合理的打卡、门禁制度，作为确定用户的上下班时间，在其不在职时间的奇怪访问，很可能是攻击。

7. 员工定期清理自己的桌面（不是电脑桌面），目的是确保秘密的文件没有被随意放置。

8. 员工系统使用强密码，使用要求密码的电脑屏保。

9. 员工使用的电子设备有基本的防盗能力，至少有锁屏图案，最好有远程数据抹除，如果有全设备加密更好。

10. 及时更新公司的操作系统到稳定的安全版本，这样可以有效对抗新攻击。特别是web服务器。

11. 设立一定的监督记录，例如员工不要使用电驴这些可能泄漏敏感信息的内容。

12. 雇佣有资质的单位，对员工进行安全培训，使员工明白基本的安全知识。

（3）物理安全

1. 建筑要有一定的防盗设计，例如人造天花板的设计、重要的门有B型以上的锁。

2. 高度机密的环境下，可以使用电磁屏蔽的技术，一般用于机房。

3. 雇佣必要的保安人员，设置摄像头。

（4）Web安全

1. 企业的Web服务器很可能受到攻击，应该配置基本的安全防护软件，尽量使用适当硬化的系统（有条件的情况下配置Linux而不是Windows，并删除不必要的功能和服务）。

2. 企业的Web应用，如果自身没有安全开发的能力，应该外包给有资质，特别是经济情况正常的企业完成。要避免为了节省费用，使用小家的企业去做。

3. 内网如果有Web服务（如内部办公，应该和外网适当分离。

4. 隐藏一些可能泄漏服务器软件类型和版本的信息。

（5）长期的安全维护

1. 雇佣有能力的、安全底细清楚的安全人员，或者咨询外面的公司。

2. 定期使用缺陷扫描仪、端口扫描仪等等进行检查。

3. 有条件的企业，应该配置蜜罐或者蜜网。

4. 建立安全基准，有助于识别未知的安全攻击

0x12 APT攻击参考资料

https://github.com/kbandla/APTnotes

https://ti.360.net/blog/

https://www.threatminer.org/

https://x.threatbook.cn/

渗透测试中心
关注 - 0
粉丝 - 68
+加关注

« 上一篇：内网终端安全建设（转）

posted @ 2018-12-21 02:17 渗透测试中心 阅读(84) 评论(0) 编辑 收藏

刷新评论 刷新页面 返回顶部