Acronis

白皮书

网络攻击方法及其对业务的影响

网络攻击及其工作原理

简介

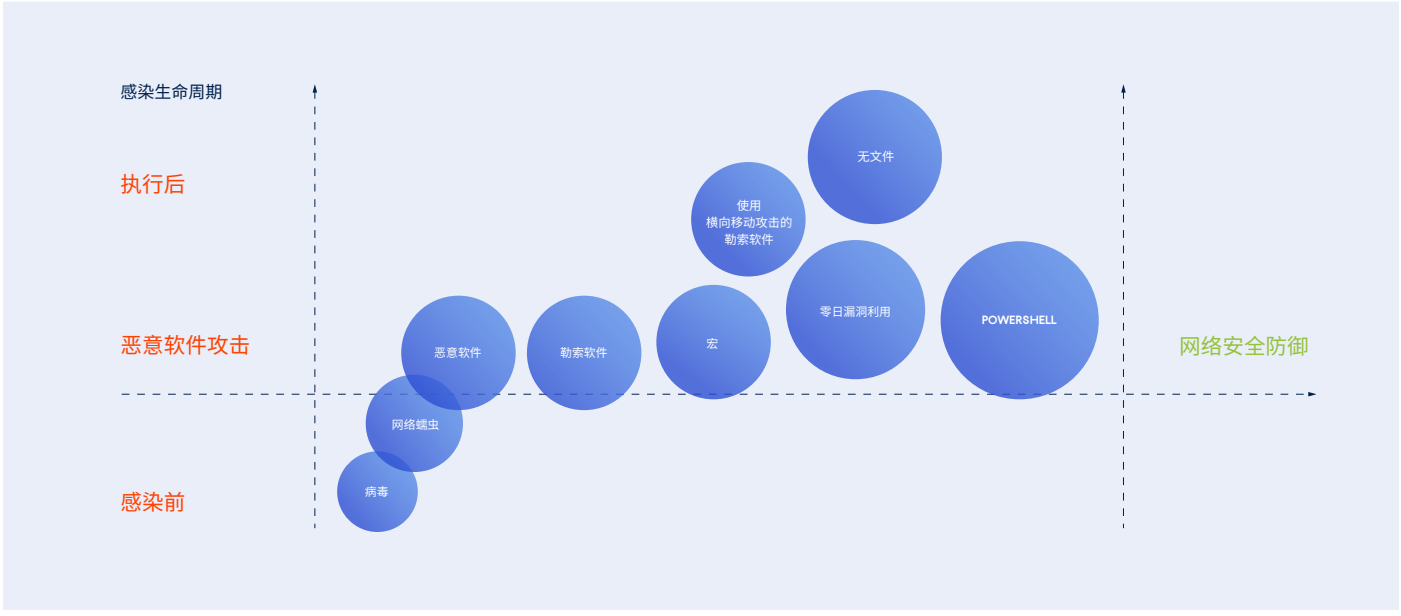
目前存在各种各样的网络威胁，虽然它们的攻击类型和途径各有不同，但都是为了渗透公司和家庭用户的网络安全防护。网络罪犯通常追求的目标是获得金钱、捕获数据或破坏系统，他们会使用大量的恶意软件和攻击途径来实现这些目标。卓越的网络安全保护和网络安全解决方案应该能够应对所有这些威胁。在本白皮书中，我们将介绍各种类型的威胁，网络安全保护与网络安全在这方面的区别，以及 Acronis Cyber Protection 解决方案如何通过抵御所有攻击途径来提供全方位网络安全保护。

什么是网络攻击?

笼统地讲，网络攻击是对计算机、智能设备或网络的数字攻击。网络罪犯使用各种攻击途径和方法来破坏和感染系统，最终实现其恶意目的。

区分大规模攻击和有针对性攻击很重要。大规模攻击通常是通过营销活动开展的，都包含一个“即服务”方案，受害者范围很广。营销活动可以是垃圾邮件、网络钓鱼、大规模感染合法网站等。这类攻击是自动发起的，每个人都可能成为受害者。有针对性攻击会事先专门挑选并分析受害者，此类攻击通常是手动发起的。最复杂的有针对性攻击是“高级可持续威胁”(APT)，这些攻击通常包含多个阶段，可能持续数个月，而且很难检测出来。

所有攻击都包含以下基本阶段：准备阶段、感染阶段和执行后阶段。如果您的安全解决方案无法对其中的某些阶段做出反应，则很可能会错过该威胁或太晚检测到该威胁。



攻击途径

目前存在多种攻击途径，因此，在安全防御策略中涵盖所有攻击途径非常重要。

最常见的攻击途径：

- 电子邮件（例如恶意附件）
- 路过式攻击（例如存在浏览器漏洞的网站）
- 暴露的服务（例如易受攻击的 RDP 服务器）
- 有效帐户（例如帐户接管）
- 供应链（例如软件更新劫持）
- 硬件（例如 USB 记忆棒）

首先，一个重要的攻击途径是电子邮件。攻击者可以通过 Web 电子邮件客户端和应用程序电子邮件客户端来发起攻击。电子邮件带来的威胁是多种多样的：恶意链接、恶意附件、社会工程等。我们稍后将讨论所有这些选项。

攻击者也可以通过利用软件和服务中的漏洞来发起攻击。存在漏洞总是不好的，但漏洞在被利用之前并不危险。遗憾的是，无论您是用户还是管理员，都无法确定漏洞是否会被利用。这就是您需要修补所有已知漏洞并在没有修补程序的情况下为应对零日漏洞和未知漏洞做好准备的原因。漏洞可能存在于暴露的服务器服务中，例如 Microsoft DNS 服务器，该服务器在 7 月份修补了远程代码执行漏洞 （CVE-2020-1350）。客户端应用程序（如 Web 浏览器）中也可能存在漏洞，当您访问恶意创建的网站时，这些漏洞可能会被利用，这种攻击被称为“路过式下载”攻击。

也可以通过帐户接管来发起攻击：网络罪犯获得对合法帐户的控制权，继而执行恶意操作。例如，如果网络罪犯猜出了密码并破坏了管理员帐户，则他们可以删除备份并复制机密信息。

还有一种攻击途径有点类似于帐户接管，它被称为“信任关系”或“供应链”攻击。您的合作伙伴或服务提供商会遭受攻击。如果您使用的应用程序的软件供应商受到攻击，则您可能会自动从他们的网站下载恶意更新。2019 年初，ASUS 就遭遇了这种情况，在受到攻击后，他们开始在不知不觉中分发受感染的驱动程序更新。

有时候，攻击者会利用物理设备（例如包含恶意软件的 USB 记忆棒）来发起攻击，方法是故意将它放在公共场所或靠近目标企业的位置，希望有人好奇地将它插入到他们的计算机上。

值得注意的是，不同的攻击途径可能会使用不同的攻击方法。谈到安全威胁时，人们通常会联想到这些攻击方法。

网络攻击方法

不同的攻击途径可能会使用不同的攻击方法。有些方法适用于各种群体（如社会工程），而其他方法（如嗅探）则允许网络罪犯找到有用信息来发起进一步攻击。

社会工程

社会工程就是指人为因素。攻击者创建了一个令人信服的故事，诱骗用户执行某些操作。这是目前最危险且最有效的网络攻击方法。人往往是安全中最薄弱的一环，只要您有足够的创造力，就可以说服人们去做几乎任何事情。

社会工程可以与帐户接管和伪装攻击相结合，这使得它很难被发现。例如，如果您老板的帐户被泄露了，则很难验证您收到的包含附件的电子邮件（其中指示您打开附件）是不是您老板本人发送的。这就是即使您对员工进行了网络钓鱼诈骗方面的培训，仍需要使用合适的网络安全解决方案的原因。

密码攻击

密码攻击是试图出于非法目的获取或使用用户密码的行为。网络罪犯可以使用密码嗅探器、字典攻击和破解程序来获取用户密码。虽然双因素身份验证在很大程度上是无用的，但在某些情况下，密码攻击足以让攻击者获得他们想要的东西。可以通过掌握简单的常识（不要向任何人透露您的密码、不要将密码写下来、不要在多个服务上使用相同的密码等）和使用较长的强密码或密码管理器来阻止密码攻击。

网络钓鱼和鱼叉式网络钓鱼攻击

网络钓鱼是一种使用看似来自可靠来源的欺诈性通信（电子邮件、消息、短信和网站）的攻击方法。攻击者冒充他人的合法服务品牌，利用这种固有的信任来诱使他人共享其凭据。例如，通过创建一个看起来像 Office 365 网络门户的页面，网络罪犯可以在后台窃取用户凭据。这是一种非常常见的攻击方法，通常与社会工程密切相关。网络钓鱼会导致您泄露机密数据（PII、信用卡号码等财务数据），让您安装恶意软件，或者访问受感染或恶意的网站。

鱼叉式网络钓鱼也有同样的目标，但专门针对的是在攻击之前通常通过社交网络加以分析的人。鱼叉式网络钓鱼通常非常有说服力，除非被网络安全产品检测到，否则很难被识别。

路过式攻击

路过式攻击是一种隐蔽而危险的恶意软件传播方法。如果您有朋友表示“我不点击任何链接，也不访问任何可疑网站”故而不需要网络安全解决方案，您就可以给他介绍一下“路过式攻击”。

典型路过式攻击的工作原理如下：网络罪犯利用配置不当或未修补的网站，将恶意脚本注入到其中的一个页面中。一旦用户访问该网站，该脚本就会利用浏览器或插件中的漏洞并在用户计算机上安装恶意软件。在大多数情况下，这些脚本都经过模糊处理，所以不容易检测出来。这些攻击被称为“路过式攻击”，因为除了访问被入侵的网站外，它不需要受害者执行任何操作。

利用零日漏洞

零日漏洞是一种软件漏洞，当它出现在大众视野中时，供应商还不知道该漏洞，因此没有可用的修补程序。也就是说，根本没时间通过修补实现自我防护。零日漏洞通常伴随着可能滥用该漏洞的零日漏洞利用行为。使用普通的网络安全解决方案很难检出到这种漏洞，因为它需要深厚的系统知识并需要持续监控所有应用程序。最终，每一个漏洞都会成为已知漏洞，并通过安全修补程序进行了修补。但是，这个过程有时可能需要几个月（甚至是几年）的时间。

SQL 注入攻击

结构化查询语言（SQL）经常用于服务器，包括 Web 服务器。SQL 注入意味着攻击者将恶意代码插入到使用SQL的服务器中，并强制该服务器显示其通常不会显示的信息。例如，攻击者只需通过将恶意代码提交到易受攻击的网站搜索框中并接收此 Web 应用程序的所有用户帐户，就可以执行 SQL 注入。

跨站点脚本 (XSS) 攻击

与 SQL 注入类似，跨站点脚本（XSS）也是一种注入漏洞，攻击者将恶意脚本发送到其他信誉良好的网站的内容中。之所以会发生这种情况，是因为网站配置糟糕或存在漏洞，这方便了攻击者将代码附加到 Web 应用程序，将恶意代码与动态内容捆绑在一起并发送到受害者的浏览器。这些漏洞可包括用多种语言（包括 JavaScript、Flash、HTML、Java 和 Ajax）编写的恶意脚本。

恶意软件攻击

许多网络攻击都涉及恶意软件。正如前面所述，恶意软件可以通过多种方式入侵系统：由用户下载和启动、通过路过式攻击静默安装、通过漏洞静默下载和执行等。

中间人 (MITM) 攻击

在中间人 (MitM) 攻击中，攻击者会拦截流量来窃取或修改所传输的数据（即登录信息、密码、财务数据等）。攻击者会冒充合法服务，像代理一样传递所有流量。这些攻击通常发生在不安全的公共 Wi-Fi 网络上，攻击者可以轻松地将自己安插在访问者设备与网络之间。然后，他们可以安装恶意软件或将用户重定向到恶意网站。据说 HTTPS 有助于阻止这些攻击，但事实并非如此。简单的 HTTPS 加密只能保护发往服务器端的流量，但不会验证服务器终端的真实性。

恶意软件类型

木马程序

有时称为特洛伊木马，木马程序是最常见的一种恶意程序。虽然木马程序不会像病毒一样复制，但也能造成很大的破坏。木马程序不仅可以发起攻击，还可以为未来的攻击创造后门。

勒索软件

这是一种非常流行的恶意软件，可防止访问系统数据。勒索软件通常会使用一种非常强大的加密算法对数据进行加密，使得您根本无法解密数据。您需要支付赎金（即加密货币）才能解密这些数据。如果您不支付赎金，攻击者还可能发出威胁警告，表示要公布或删除敏感信息。

病毒

这是一种恶意程序，能够让大多数媒体和最终用户错误地标记恶意软件程序。数字病毒会修改其他合法主机文件（或指向这些文件的指针），这样一来，当执行受害者的文件时，病毒也会被执行。纯病毒可以进行复制，但目前并不常见。

广告软件和 PUA（潜在不需要的应用程序）

这些软件程序不太危险但非常烦人，通常由狡猾的企业在营销活动中使用。它们通常在应用程序运行时显示为广告或横幅。

网络蠕虫

网络蠕虫的独特之处是它可以自我复制并通过网络传播。网络蠕虫十分危险，因为它们可以在没有最终用户交互的情况下传播。

Rootkit 和 Bootkit

这是很复杂的恶意程序，可以将自身隐藏在硬盘上的主引导记录中或隐藏在操作系统中。最初，Rootkit 是一组工具，用于实现对计算机或网络的管理员级访问。如今，Rootkit 已经十分少见，通常与恶意软件（如木马程序、网络蠕虫和病毒）相关，它们对用户和其他系统进程隐藏自身和自己的行为。

间谍软件

这种恶意软件旨在收集受害者计算机上的信息。间谍软件会在未经您同意或您不知情的情况下跟踪您的一切活动，并将信息直接传递给远程网络罪犯。它还可以通过互联网在您的系统上安装其他恶意应用程序。

脚本化恶意软件或恶意脚本

这种恶意软件以前被称为“宏病毒”。但是，它们通常是由合法程序执行来开展恶意活动的任何类型的脚本。近年来，它们被错误地与无文件攻击联系在一起。从名称上可以看出，该脚本仍然是硬盘或任何其他存储来源中的文件。

僵尸网络

您的计算机被某人控制来执行恶意活动，如传播恶意软件、拒绝服务和分布式拒绝服务攻击。单独的 bot 程序相对无害，尤其是在它没有连接到指挥控制服务器时。这就是将 bot 程序组合成僵尸网络的原因，因为僵尸网络可以造成极大的破坏，例如完全中断业务运营。

无文件攻击

无文件攻击是一种网络威胁，通常与恶意软件和漏洞相关。无文件攻击存在多种略有不同的定义。简单来说，无文件攻击是指磁盘上没有特定恶意文件的攻击。

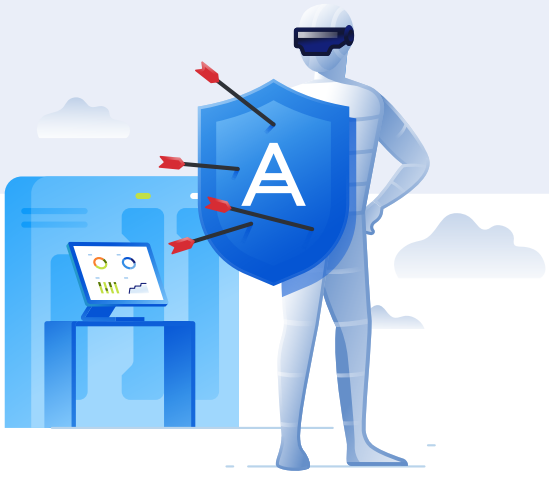
无文件攻击利用合法应用程序和进程执行恶意活动，如权限提升、负载传递、数据收集等。如果在无文件攻击中使用了预安装的合法软件，则这种攻击方法通常被称为“离地攻击”。我们经常可以看到，只有攻击链的某些阶段使用了无文件攻击方法，因此从技术角度讲，整个攻击并不是无文件的。

所有这一切都只在随机存取存储器（RAM）中发生，并且在计算机重新启动后不会留下任何痕迹。这意味着当发生此类攻击时，与恶意活动相关的任何内容都不会写入目标硬盘中，即，无文件攻击在很大程度上绕开了现有的安全检测技术（如基于文件的白名单、特征码检测、硬件验证等），因为它们几乎没有留下任何证据，数字取证调查人员以后也就无法识别和知晓这些攻击。

ACRONIS CYBER PROTECTION 解决方案如何应对这些攻击方法

使用网络安全和网络安全保护解决方案（如 Acronis Cyber Protect Cloud 或本地版本 Acronis Cyber Protect）来阻止这些潜在的网络攻击并确保系统和数据的安全，这一点非常重要。现代网络安全行业面临的问题是，很难找到一款能够帮您抵御所有这些威胁的产品，企业经常不得不使用多种解决方案或作出妥协，在安全外围留下一些漏洞，这样做既危险又不明智。普通的网络安全解决方案无法保护数据并提供快速恢复和良好的业务连续性。

Acronis Cyber Protection 解决方案将网络安全与数据保护功能相结合，它是可以解决几乎所有这些威胁的理想解决方案。它提供了创新的集成式多层保护，其中每个解决方案都采用了经过优化的技术，能够抵御本白皮书中提到的各种威胁。这就是我们所说的 Acronis Cyber Protection 方法。可以查看下表，其中涵盖了前面介绍的所有攻击途径和方法，以及对应的 Acronis 安全技术。



ACRONIS 安全技术			
攻击途径或方法	**前瞻阶段**	**主动阶段**	**被动阶段**
通过电子邮件发起的攻击		URL 过滤	URL 过滤、行为引擎、静态 AI 分析程序、云检测、漏洞利用防范
漏洞利用（包括零日漏洞）	漏洞评估和补丁管理	漏洞利用防护	
帐户接管			URL 过滤、行为引擎、静态 AI 分析程序、云检测、漏洞利用防范
信任关系或供应链攻击			URL 过滤、行为引擎、静态 AI 分析程序、云检测、漏洞利用防范
社会工程		URL 过滤	URL 过滤、行为引擎、静态 AI 分析程序、云检测、漏洞利用防范
网络钓鱼和鱼叉式网络钓鱼攻击		URL 过滤	URL 过滤
无文件攻击	漏洞评估和补丁管理	URL 过滤、行为引擎、云检测、漏洞利用防范	静态 AI 分析程序
路过式攻击		URL 过滤、行为引擎、漏洞利用防范	
恶意软件攻击		行为引擎、云检测、漏洞利用防范、Acronis Active Protection、静态 AI 分析程序	静态 AI 分析程序
中间人 (MitM) 攻击		行为引擎、云检测、URL 过滤	静态 AI 分析程序
密码攻击	双因素身份验证	蛮力检测	
僵尸网络		行为引擎、云检测	静态 AI 分析程序
篡改			Acronis Notary（通过区块链）
SQL 注入攻击		URL 过滤	
跨站点脚本 (XSS) 攻击		URL 过滤	

前瞻（或预防）阶段

您可以提前做好应对威胁的准备：修补系统、使用身份验证等。

主动阶段

安全技术检测系统中当前发起的主动威胁或攻击。

被动阶段

威胁可能已经存在于系统中，或者已执行攻击的第一个阶段。例如，您收到了一封网络钓鱼电子邮件。值得注意的是，即使系统中存在威胁，也不意味着系统受到任何损坏，因为要在很久以后才会下载实际负载。在这个阶段中，将会检测到该威胁。

正如您所见，ACRONIS 解决方案及其集成和多层安全堆栈可以抵御所有这些攻击方法，并确保系统和数据的安全。