攻击推理，一文了解“离地攻击”的攻与防

CCF计算机安全专委会 2022-09-26 15:30 发表于北京

以下文章来源于绿盟科技研究通讯 ，作者创新研究院

一、什么是“离地攻击”

关于“离地攻击”至今没有一个权威的定义。但是被广泛接受的“离地攻击”通常是指利用系统中已存在或比较易于安装的二进制文件来执行后渗透活动的攻击策略。说白了就是攻击过程不“落地”。

当前针对恶意软件，主要是利用恶意软件的静态二进制特征以及动态行为特征进行检测、分类与防御。攻击者为了规避这些检测方法，利用主机已有的二进制来执行相关的攻击活动，达到攻击过程不“落地”的效果，比如无文件攻击并不是指的完全没有文件，只是恶意文件不会写入磁盘。“离地攻击”比较常用的是Powershell，其并不是最新出现在的技术，由于其灵活的攻击策略，在att&ck中并没有专门的技术是针对“离地攻击”的。

文献[1]中通过对31,805,549个样本进行分析得到当前使用“离地攻击”策略的占比为26.26%。可以看出“离地攻击”策略将会成为恶意样本的主流攻击策略。

二、 “离地攻击”策略的相关事件

下面介绍几个经典的使用“离地攻击”策略的攻击事件。

2.1 PowerGhost[2]

PowerGhost是从2018年被发现使用powershell无文件方式进行攻击感染的挖矿以及DDOS病毒，其感染方式利用了永恒之蓝，MSSQL爆破，SSH爆破，wmi以及smb爆破远程命令执行等，同时对windows和linux进行攻击。一旦该病毒进入内网，会在内网迅速传播。

PowerGhost其实是一个经过了混淆处理的PowerShell脚本，其中包含的核心组件有：挖矿主程序、mimikatz、一个用于实现反射PE注入的模块、用于利用EternalBlue漏洞的

ShellCode以及相关的依赖库（msvcp120.dll和msvcr120.dll）。

这款恶意软件使用了各种“离地攻击”策略来隐藏自己的活动踪迹，并利用漏洞和远程管理工具（Windows管理工具）来远程感染目标设备。在实现感染的过程中，恶意软件会运行一个PowerShell脚本，下载了挖矿主程序之后，脚本会立即启动恶意软件，而不是直接将其存入主机的硬盘中。

基于主要的攻击过程分为如下几个阶段：

自动更新：PowerGhost会定期检查C&C服务器是否有新版本，有则自动下载并实现更新，而不会启动之前的版本。

传播：在mimikatz的帮助下，恶意软件会收集受感染系统的用户凭证，然后完成登录并通过WMI在本地网络中传播恶意软件副本。除此之外，PowerGhost还会利用EternalBlue漏洞（MS17-010, CVE-2017-0144）在本地网络中实现恶意传播。

提权：感染设备后，PowerGhost会利用漏洞MS16-032、MS15-051和CVE-2018-8120来在目标设备上实现提权。

持久化感染：PowerGhost会将所有模块存储为WMI类，挖矿主体会以PowerShell脚本的形式存储，每90分钟激活一次。

Payload：最后，该脚本会通过反射型PE注入来加载PE文件并启动挖矿程序。

在其中一个PowerGhost样本中，研究人员还发现了用于执行DDoS攻击的代码，显然PowerGhost的作者还想通过提供额外的DDoS攻击服务来赚取外快。

2.2 FTCode勒索软件[3]

FTCode勒索病毒是一款基于PowerShell脚本的勒索病毒，主要通过垃圾邮件进行传播。该病毒于2013年首次发现，现在已成为一种威胁度比较高的勒索软件。

FTCode 勒索病毒完全用PowerShell编写的，因此，其在windows上可以不需要加载任何组件直接对主机上的文件进行加密。为了规避杀软的检测，它通常将可执行代码加载到内存中。由于当前的windows版本基本上在win7之后的版本，因此像FTCode这种基于PowerShell的无文件恶意软件将会带来更大的危害。此勒索病毒攻击流程，如下图所示：

图1 FTCode勒索然健攻击流程

2.3 PowershellMiner挖矿软件[4]

PowershellMiner挖矿软件利用WMI+Powershell方式实现的无文件攻击行为，其目的是长驻内存挖矿。由于此攻击没有本地落地文件，难以察觉。PowershellMiner挖矿软件具备无文件攻击特性，所有模块功能均加载到内存中执行，没有本地落地文件。为了迅速在内网传播，采用了SMB弱口令爆破攻击和“永恒之蓝”漏洞攻击，二者只要有一种能成功，就可以横向感染到其它主机。病毒直接使用powershell.exe进行挖矿，CPU占用率达到87%，其脚本功能是从wmi类中读取挖矿代码并执行。

图2 PowershellMiner挖矿软件执行过程

如上图，原始病毒体为info*.ps1（64位系统对应info6.ps1，32位系统对应info3.ps1），其为Powershell脚本，被加载后内存存在4个模块，分别为挖矿模块、Minikatz模块、WMIExec模块、MS17-010攻击模块。

攻击顺序如下：

1.首先，挖矿模块启动，持续进行挖矿。

2.其次，Minikatz模块对目的主机进行SMB爆破，获取NTLMv2数据。

3.然后，WMIExec使用NTLMv2绕过哈希认证，进行远程执行操作，攻击成功则执行shellcode使病原体再复制一份到目的主机并使之运行起来，流程结束。

4.最后，如WMIExec攻击失败，则尝试使用MS17-010“永恒之蓝”漏洞攻击，攻击成功则执行shellcode使病原体再复制一份到目的主机并使之运行起来（每感染一台，重复1、2、3、4）。

此病毒采用的是WMI+Powershell的内存驻留方式，模块以服务形式存在，每5600秒可自动触发一次。

三. 离地攻击的检测

针对“离地攻击”的有效检测方法相对较少。下面介绍三种类型的经典方法：

3.1 基于命令行的检测方法

文献[5]针通过采集终端日志对命令行进行了分析，来检测“离地攻击”。由于“离地攻击”主要利用系统已有的二进制程序来执行相关的恶意操作，命令行是其关键的行为的体现。该方法的思想是根据“离地攻击”的特点，可以从包含二进制文件名与相关参数的命令行里推断出攻击行为。为了提高识别准确率，通过关联相关命令行的父子进行来利用上下文加强其检测效果。

本方法采用了主动学习的框架。首先，对原始的命令行进行序列化，利用NLP技术的词嵌入方法对其进行向量化。这里的嵌入表示考虑的命令行的上下文。然后，为了有效区分恶意的命令行，根据标记数据对每个命令行实体进行评分；最后，对聚合全的特征向量利用机器学习算法进行异常检测。

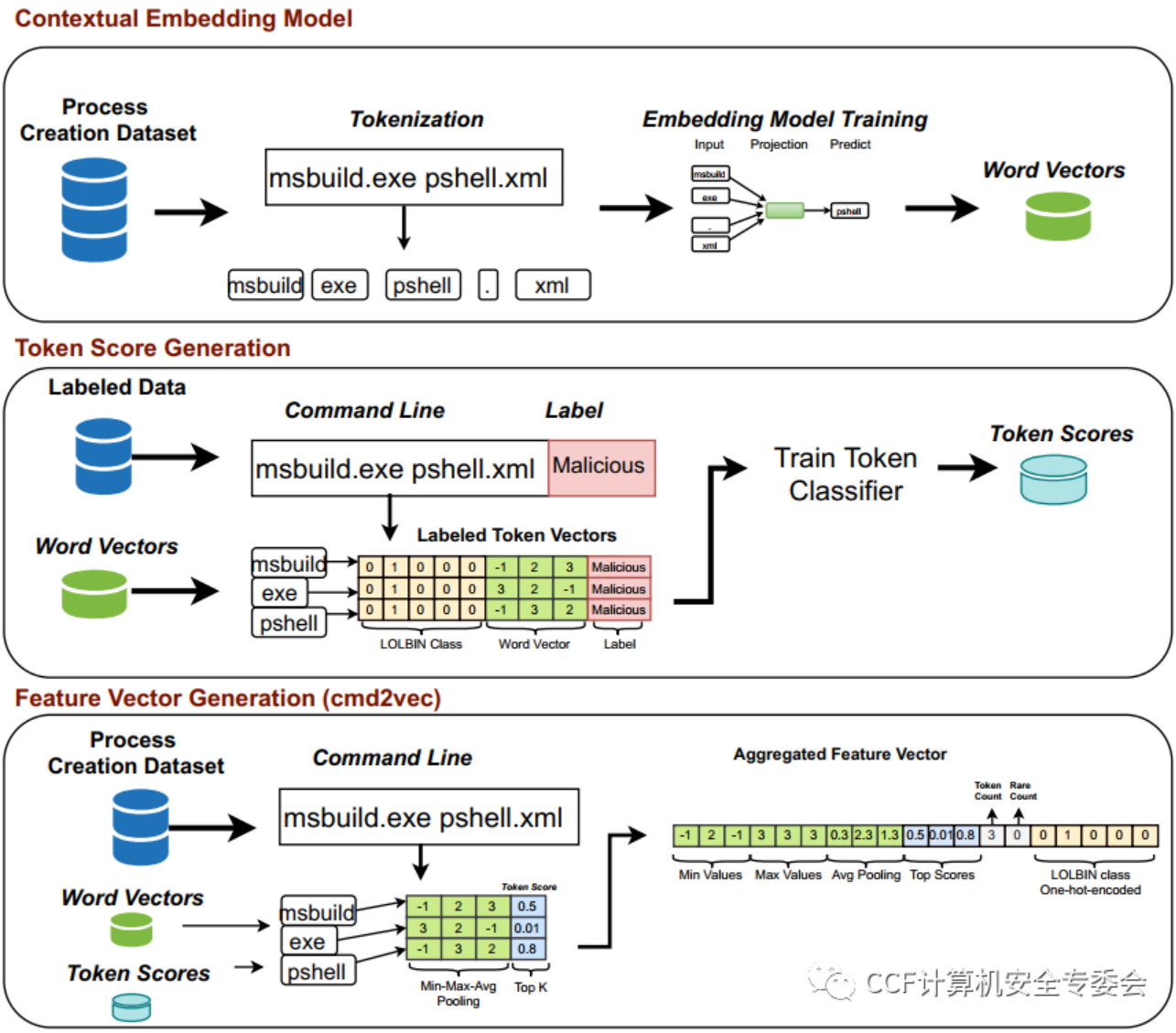

图3 cmd2vec技术流程图

3.2 混淆命令行的检测方法

通常“离地攻击”为了逃避检测，命令行是加入混淆机制的，这给检测带来了更大的挑战。然对这种情况，文献[6]提出了一种针对powershell混淆命令行的检测方法。

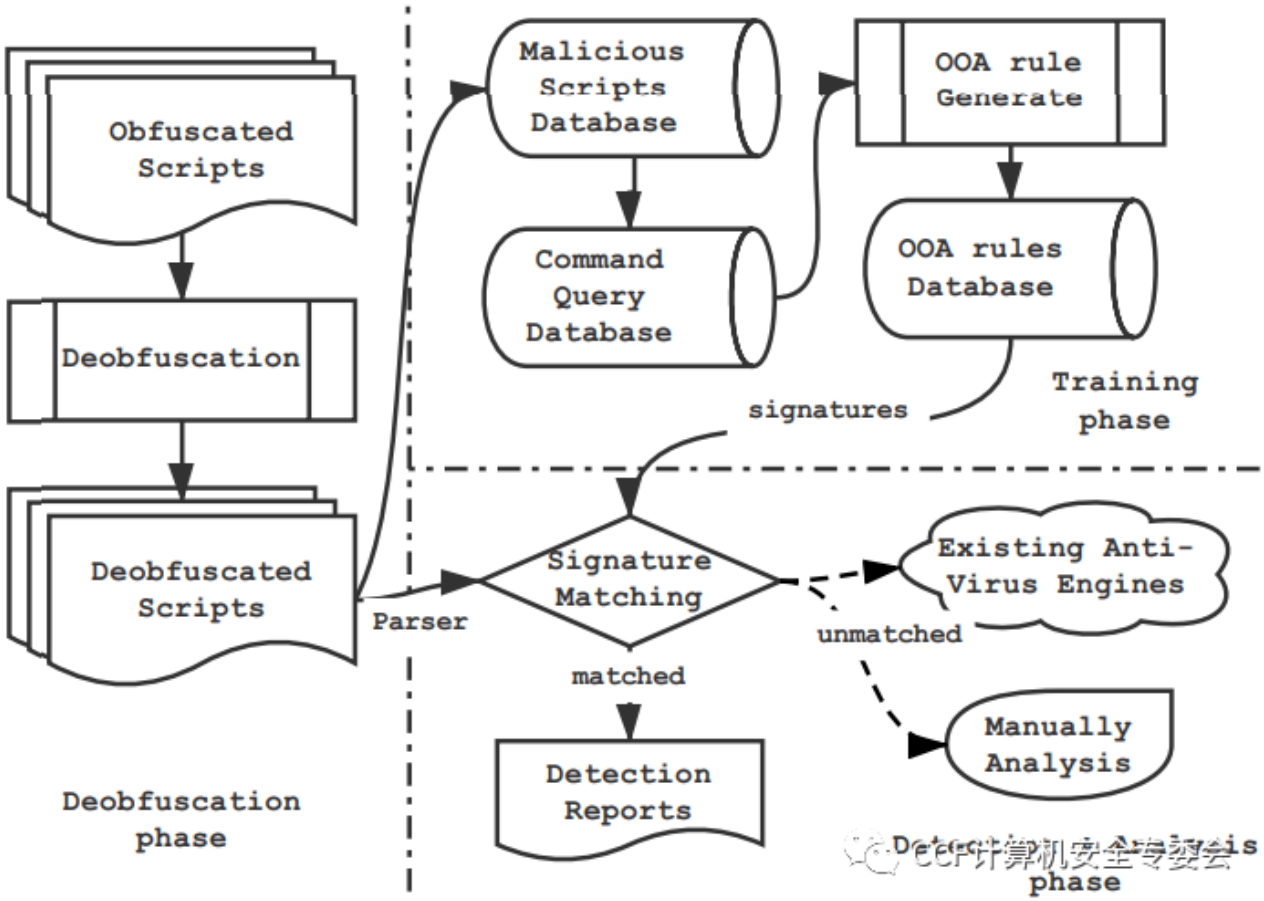

图4 混淆Powershell命令检测流程

一个混淆后的代码或脚本想要在机器上正确执行，肯定是要包含一个解混淆的逻辑，在执行之前将内容解析出来。该方法提出了一种有效的基于模拟器的解混淆方法。下面对本文方法进行系统介绍，主要包括五个步骤。

(1) 提取子树

(2) 基于子树的混淆检测

(3) 基于模拟器的解混淆

(4) 更新抽象语法树

(5) 后处理

该方案的具体实现过程如下：

首先，把混淆后的代码使用AST（抽象语法树）解析，根据一定的规则提取部分子树。判断哪些子树包含混淆代码，取出子树并量化。

然后，基于子树的混淆检测，通过基于token、字符串和AST三层特性的分类器来判断子树是否存在混淆。

其次，如果子树存在混淆，则基于模拟器开展解混淆，将原始代码片段还原。

再次，更新抽象语法树。接着进行解析，并将新生成的抽象语法树合并到原有抽象语法树中（子树栈），更新分类器的特征值。

最后，当没有剩余的混淆子树，整个解混淆工作基本完成，开展善后处理，使得混淆代码更具可读性。

3.3 基于溯源图的检测方法

文献[7]针对隐蔽性的恶意样本利用其行为模式进行，可以复用到“离地攻击”中。其流程如下图所示，整个流程主要有溯源图构建，特征抽取，嵌入表示以及异常检测，与已有的溯源图相关工作相差不大。其创新在于特征表示的时候加入了对稀有路径的处理，可以有效提高其针对恶意样本攻击路径的检测效果。

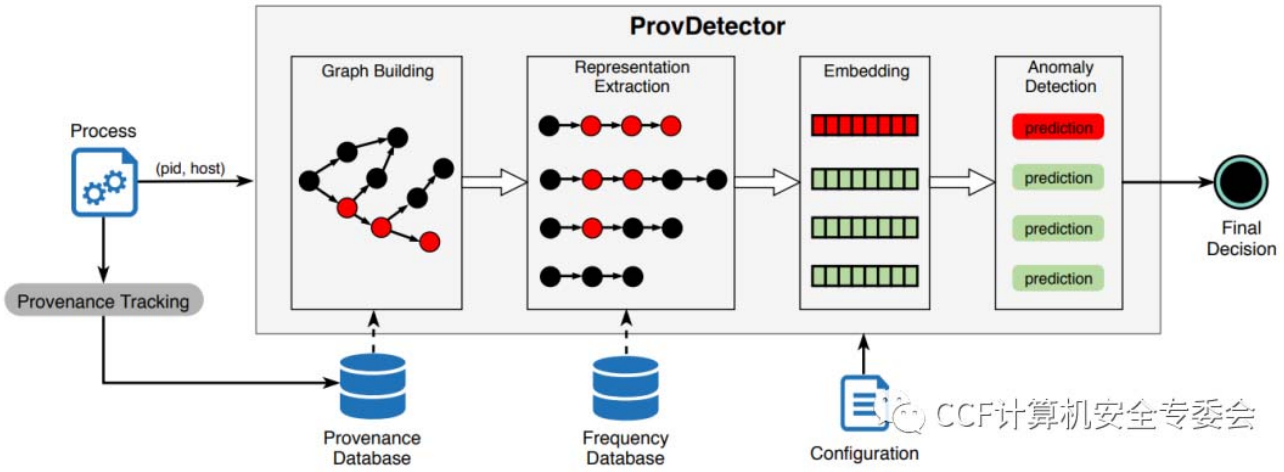

图5 ProvDetector检测流程

四、 总结

“离地攻击”已成为了一种不可忽视的攻击策略，通过文献中对当前主流检测设备的测试可以发现，几乎每个商用的检测软件都很难检测到“离地攻击”行为。但是通过分析可以得到“离地攻击”的行为与正常行为之间还是有一些差异的，利用溯源图分析就有可能成为检测“离地攻击”的手段。

由于“离地攻击”的特性导致它将成为未来攻击的主要手段。从检测的角度来看，它们代表了安全行业的一个挑战。

参考文献

1 F. Barr-Smith, X. Ugarte-Pedrero, M. Graziano, R. Spolaor and I. Martinovic, "Survivalism: Systematic Analysis of Windows Malware Living-Off-The-Land," 2021 IEEE Symposium on Security and Privacy (SP), 2021, pp. 1557-1574, doi: 10.1109/SP40001.2021.00047.
2 PowerGhost：一款在野的多功能挖矿恶意软件分析 https://www.freebuf.com/articles/system/181441.html.
3 https://www.telsy.com/the-ftcode-ransomware/
4 https://cloud.tencent.com/developer/news/149081
5 Ongun T， Stokes J W， Or J B，et al. Living-Off-The-Land Command Detection Using Active Learning[C]// 2021.
6 Li Z， Chen Q A， Xiong C，et al. Effective and Light-Weight Deobfuscation and Semantic-Aware Attack Detection for PowerShell Scripts[C]// 2019 ACM SIGSAC Conference on Computer & Communications Security (CCS ‘19). ACM, 2019.
7 Wang Q, Hassan W U, Li D, et al. You are what you do: Hunting stealthy malware via data provenance analysis[C]//Proc. of the Symposium on Network and Distributed System Security (NDSS). 2020.

本文转自绿盟科技，点击阅读原文查看完整内容

阅读原文