使用Autoruns检查计划任务

在微软的Sysinternals实用工具（故障诊断工具套装）中，可运行于 Windows XP、Windows Server 2003 和更高版本的 Windows 操作系统。该软件还包括一个相同功能的命令行版本 Autorunsc，可以把结果报表以 CSV 格式输出。

简介

Autorunsc 是自动运行的命令行版本。 它的用法语法为：

```
用法: autorunsc [-a <*|bdeghiklmoprsw>] [-c|-ct] [-h] [-m] [-s] [-u] [-vt] [[-z]
|[user]]]

参数 说明
-a  自动启动条目选择:
*   全部。
b   启动执行。
d   Appinit DLL。
e   资源管理器加载项。
g   (Vista 和更高) 的边栏小工具
h   图像劫持。
i   Internet Explorer 加载项。
k   已知 DLL。
l   登录启动 (这是默认) 。
m   WMI 条目。
n   Winsock 协议和网络提供程序。
o   编 解码 器。
p   打印机监视器 DLL。
r   LSA 安全提供程序。
s   自动启动服务和未禁用的驱动程序。
t   计划的任务。
w   Winlogon 条目。
-c  将输出打印为 CSV。
-ct 将输出打印为制表符分隔的值。
-h  显示文件哈希。
-m  如果与 -v) 一起使用，则隐藏 Microsoft 条目 (签名条目。
-s  验证数字签名。
-t  在规范化 UTC (YYYYMMDD-hhmmss) 中显示时间戳。
-u  如果已启用 VirusTotal 检查，则显示由 VirusTotal 未知或未检测的文件，否则仅显示未签名的
文件。 (有的有签名的文件不一定是安全的所以如果是安服分析建议去掉-u)
-x  将输出打印为 XML。
```

```
-v[rs]  基于文件哈希查询恶意软件的 VirusTotal 。 添加“r”以打开包含非零检测的文件的报表。 如果指定了“s”选项，则报告为以前未扫描的文件将上传到 VirusTotal。 请注意，扫描结果可能不可用 5 分钟或更多分钟。
-vt 在使用 VirusTotal 功能之前，必须接受 VirusTotal 服务条款。 如果尚未接受条款，并且省略此选项，系统会以交互方式提示你。
-z  指定要扫描的脱机Windows系统。
user    指定将显示自动运行项的用户帐户的名称。 指定“*”以扫描所有用户配置文件。
```

下载

https://learn.microsoft.com/zh-cn/sysinternals/downloads/autoruns
https://download.sysinternals.com/files/Autoruns.zip

目录结构

微软官方下载的Autoruns.zip以及类似应急框架中安装Autoruns都是类似。主体包含：Autoruns.exe、Autoruns64.exe、Autorunsc.exe、Autorunsc64.exe等等，其中`Autoruns*`是图形界面程序，而`Autorunsc*`是命令行执行的版本。

一个实际应用的例子

上午同事收到客户的需求，希望提供个能够批量执行计划任务检查的程序或者脚本。在查找了些材料后，我们锁定到了autoruns上，因为autoruns一来是微软官方推荐工具之一，另一方面因为其有命令行功能，实际使用的时候可以根据需求一个命令来输出结果，根据前文我们知道，使用autoruns我们可以做到使用-a t指定查询计划任务，然后通过-vt或者-v功能针对所有计划任务中的程序进行vt的杀毒软件信息查询。

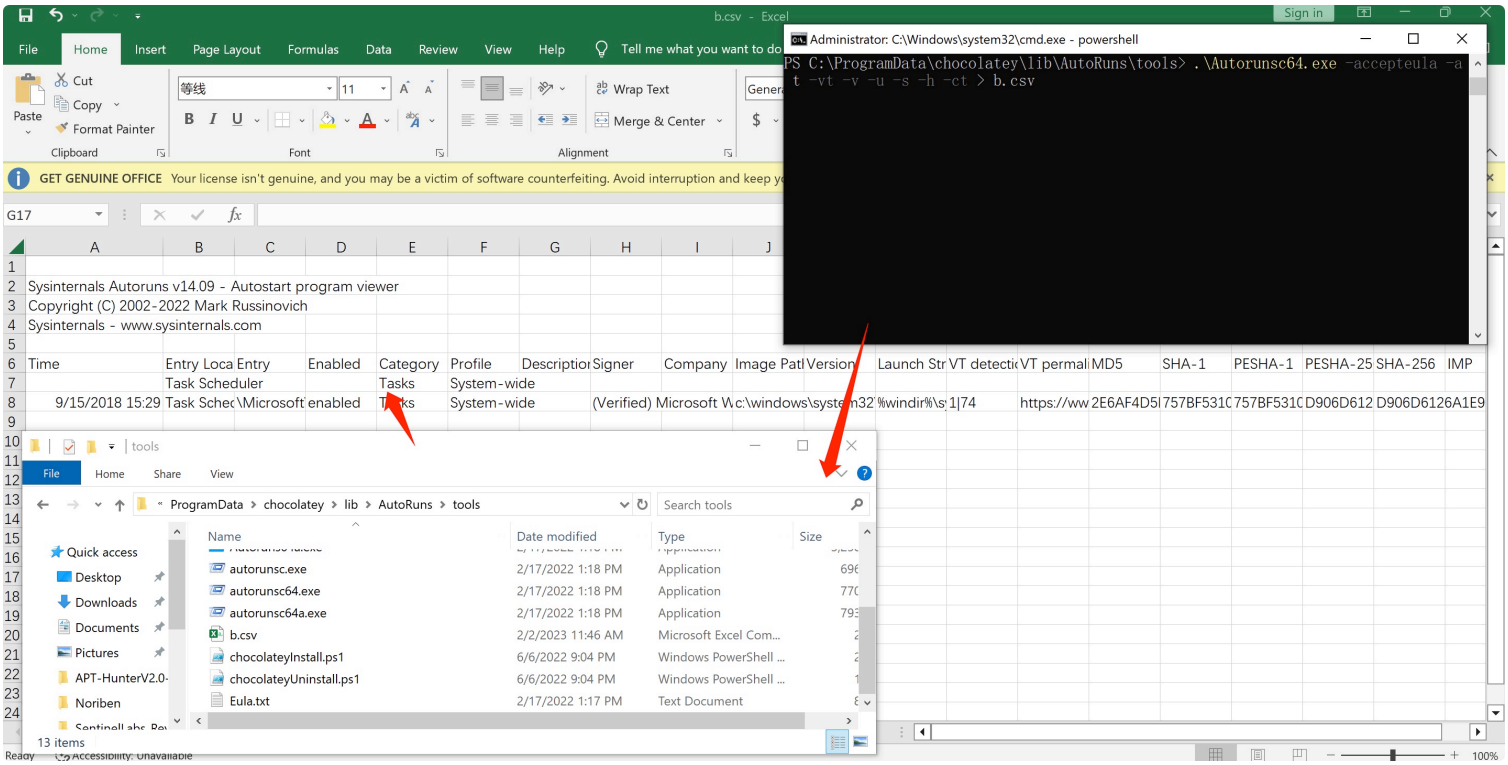
那么思路有了我们来探究下如何实现。

```
.\Autorunsc64.exe -accepteula -a t -vt -v -u -s -h -ct > b.csv
```

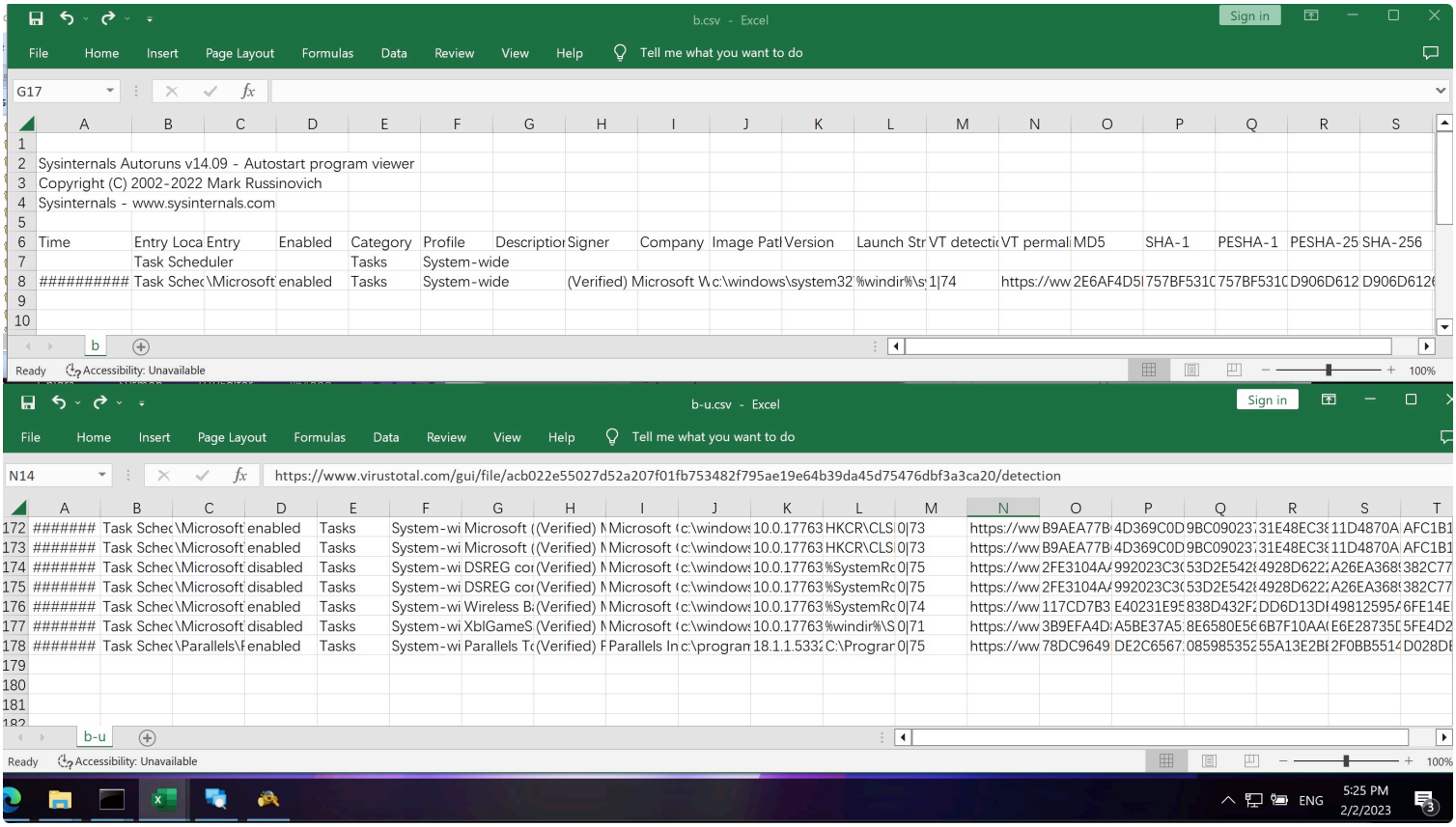
其中-accepteula是必须的，意为自动接受微软的软件的协议license，想要实现无人干预执行就需要带上此参数配置。
-a t则指定对计划任务进行检查
-vt 接受vt条款
-v 是使用virustotal进行文件hash查询文件结果
-h 显示文件hash

-ct 导出csv格式表格，并且加入分隔符，阅读方便。
-u 有的有签名的文件不一定是安全的所以如果是安服分析建议去掉-u,加上-u显示的就只有未签名的项目，和不加-u相比会差很多内容

最后结果如下。



注意：
加上-u显示的就只有未签名的项目，和不加-u相比会差很多内容


b.csv - Excel
Sign in
File Home Insert Page Layout Formulas Data Review View Help Tell me what you want to do
G17
Sysinternals Autoruns v14.09 - Autostart program viewer
Copyright (C) 2002-2022 Mark Russinovich
Sysinternals - www.sysinternals.com
Time Entry Loca Entry Enabled Category Profile Description Signer Company Image Path Version Launch Str VT detecti VT permali MD5 SHA-1 PESHA-1 PESHA-25 SHA-256
########## Task Schec \Microsoft enabled Tasks System-wide (Verified) Microsoft W c:\windows\system32 %windir%\s 1|74 https://ww 2E6AF4D5 757BF531 757BF531 D906D612 D906D612
Task Scheduler Tasks System-wide
b
Ready Accessibility: Unavailable
100%

b-u.csv - Excel
Sign in
File Home Insert Page Layout Formulas Data Review View Help Tell me what you want to do
N14
https://www.virustotal.com/gui/file/acb022e55027d52a207f01fb753482f795ae19e64b39da45d75476dbf3a3ca20/detection
######## Task Schec \Microsoft enabled Tasks System-wi Microsoft ((Verified) M Microsoft c:\windows 10.0.17763 HKCR\CLS 0|73 https://ww B9AEA77B 4D369C0D 9BC09023 31E48EC3 11D4870A AFC1B1
######## Task Schec \Microsoft enabled Tasks System-wi Microsoft ((Verified) M Microsoft c:\windows 10.0.17763 HKCR\CLS 0|73 https://ww B9AEA77B 4D369C0D 9BC09023 31E48EC3 11D4870A AFC1B1
######## Task Schec \Microsoft disabled Tasks System-wi DSREG cor (Verified) M Microsoft c:\windows 10.0.17763 %SystemRo 0|75 https://ww 2FE3104A 992023C3 53D2E542 4928D622 A26EA368 382C77
######## Task Schec \Microsoft disabled Tasks System-wi DSREG cor (Verified) M Microsoft c:\windows 10.0.17763 %SystemRo 0|75 https://ww 2FE3104A 992023C3 53D2E542 4928D622 A26EA368 382C77
######## Task Schec \Microsoft enabled Tasks System-wi Wireless B (Verified) M Microsoft c:\windows 10.0.17763 %SystemRo 0|74 https://ww 117CD7B3 E40231E9 838D432F DD6D13DI 49812595 6FE14E
######## Task Schec \Microsoft disabled Tasks System-wi XblGameS (Verified) M Microsoft c:\windows 10.0.17763 %windir%\S 0|71 https://ww 3B9EFA4D A5BE37A5 8E6580E5 6B7F10AA E6E28735 5FE4D2
######## Task Schec \Parallels\I enabled Tasks System-wi Parallels To (Verified) P Parallels In c:\program 18.1.1.533 C:\Prograr 0|75 https://ww 78DC9649 DE2C6567 08598535 55A13E2B 2F0BB551 D028DE
b-u
Ready Accessibility: Unavailable
100%
ENG 5:25 PM 2/2/2023