mp.weixin.qq.com /s/alaZxCd61gJNI9D01eQzgg

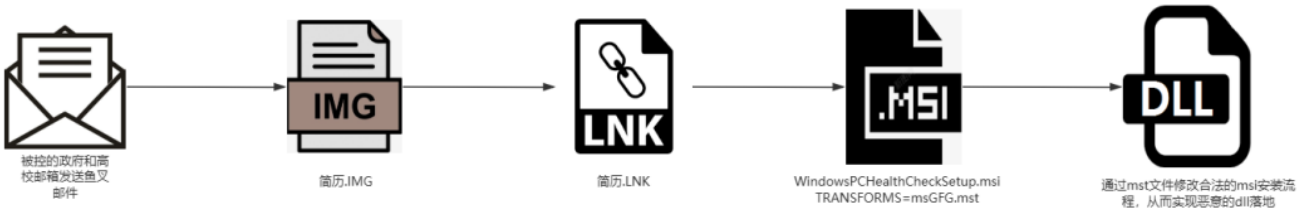
MSI 文件滥用新趋势：新海莲花组织首度利用 MST 文件投递特马

2024年11月04日 03:04

概述

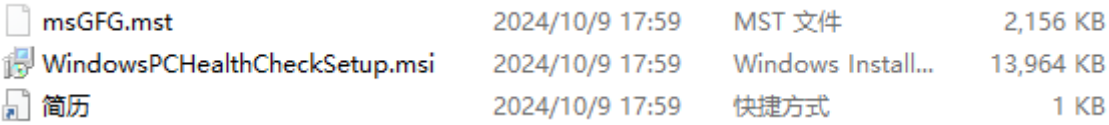
奇安信威胁情报中心在最近的日常运营过程中发现我们从 2022 年中就开始持续跟踪的新海莲花组织开始重新活跃，并使用了 MSI 文件滥用的新手法，尽管 MSI TRANSFORMS 技术理论上在 2022 年已经被披露[1]，但这是我们首次在针对国内政企的APT活动中捕获到。

我们目前将 APT-Q-31 (海莲花)组织分为两个攻击集合，经过我们长时间的观察新老海莲花每年通过轮战的方式交替针对国内开展间谍活动，两个攻击集合 TTP 完全不同，但是攻击资源共享。新海莲花组织上次活跃的时间为 2023 年末，至今正好一年。本次鱼叉邮件的活动的执行链如下：



我们建议政企客户在办公区和服务器区同时部署天擎EDR，在开启云查功能下可以实现对通用威胁的发现和拦截。

MST 文件介绍

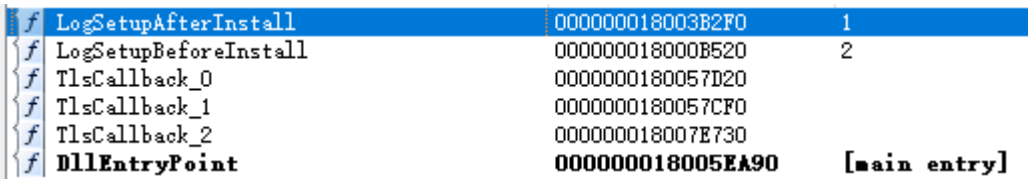


新海莲花组织通过 lnk 执行了如下命令行：

msiexec.exe /qn /i WindowsPCHealthCheckSetup.msi TRANSFORMS=msGFG.mst

其中 WindowsPCHealthCheckSetup.msi 为微软官方提供的合法安装包

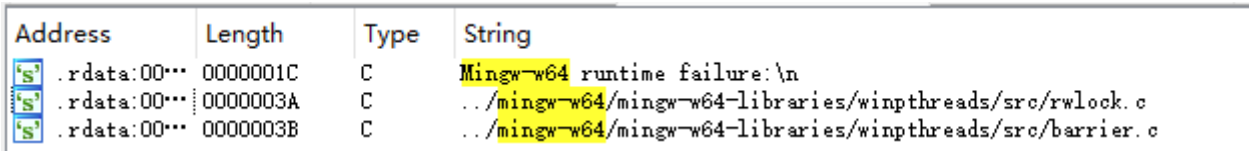
MSI TRANSFORMS 参数的恶意利用方式境外的博客中已经有过介绍[1], MST 内部的可执行模块一般会有两个导出函数分别为 LogSetupAfterInstall 和 LogSetupBeforeInstall，用来控制 msi 安装过程中的流程。



在这两个导出函数中可以实现落地额外的 DLL 和持久化操作：

```
526  v92 = v94;
527  strcpy((char *)v94, "PCHealthCheck");
528  v93 = 13i64;
529  String = (wchar_t *)v91;
530  v4 = (char *)sub_180048310(0x40ui64);
531  strcpy(v4, "HKEY_CURRENT_USER\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run");
532  String = (wchar_t *)v4;
533  v91[0] = 63i64;
534  v90 = 63i64;
535  sub_1800536D0(&String, &v92, 1i64, &Str);
536  if ( String != (wchar_t *)v91 )
537    j_j_free(String);
```

最终实现 DLL-Sideloading 的效果，内存加载的 payload 为一年不见的 RUST 特马，与 2023 年不同的点在于攻击者将 RUST 特马彻底 Shellcode 化，删除了之前使用通用 Shellcode 反射加载 PE 文件的流程，实现内存对抗。我们还观察到新海莲花在编写的十几种加载器中大部分都使用了 Mingw-w64 代码库进行开发，这个习惯从 2022 年一直持续到现在，而 2024 上半年老海莲花攻击集合释放的加载器中从未出现过该代码库。



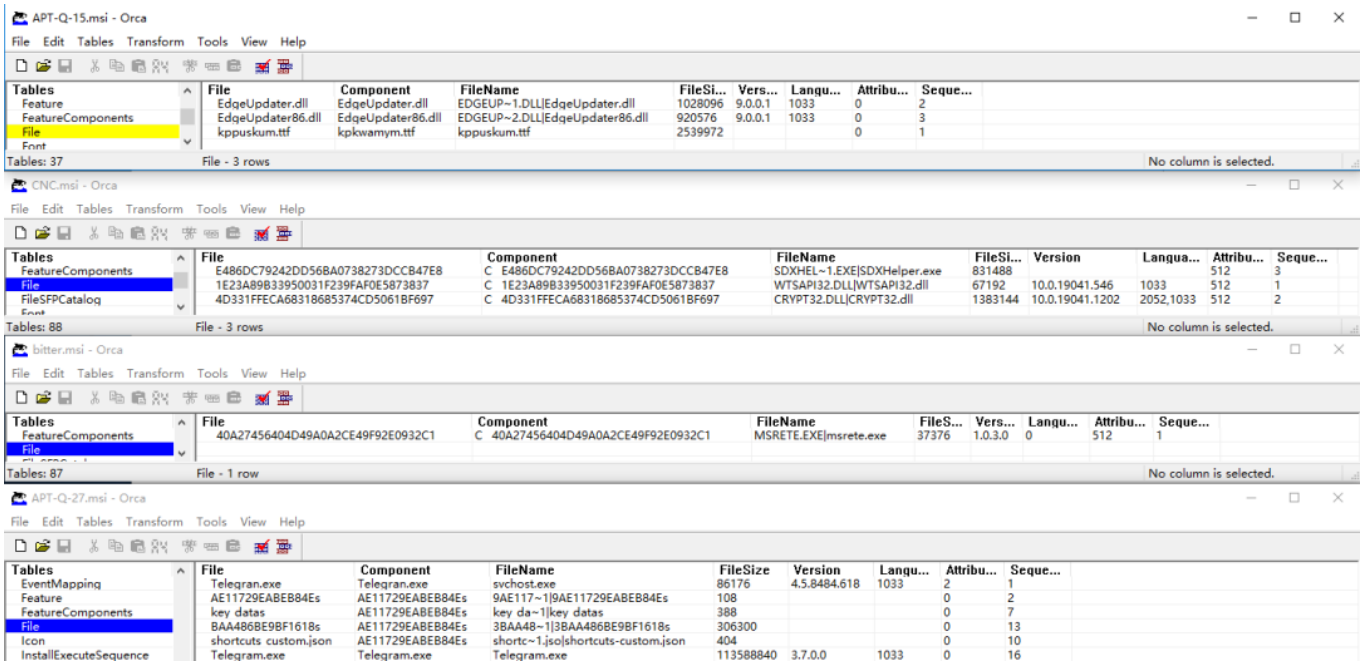
有关新海莲花组织在 2023 年所使用的复杂内存态 TTP，我们会在今年择机披露。

MSI 滥用情况

MSI 作为老生常谈的通用载荷近些年来一直在被各个威胁行为团体使用，分析方法和过程境外友商也都进行了分享[2]，我们从 MSI 利用手法的角度，浅谈一下最近两年各个方向的 APT 团伙对 MSI 的使用情况。

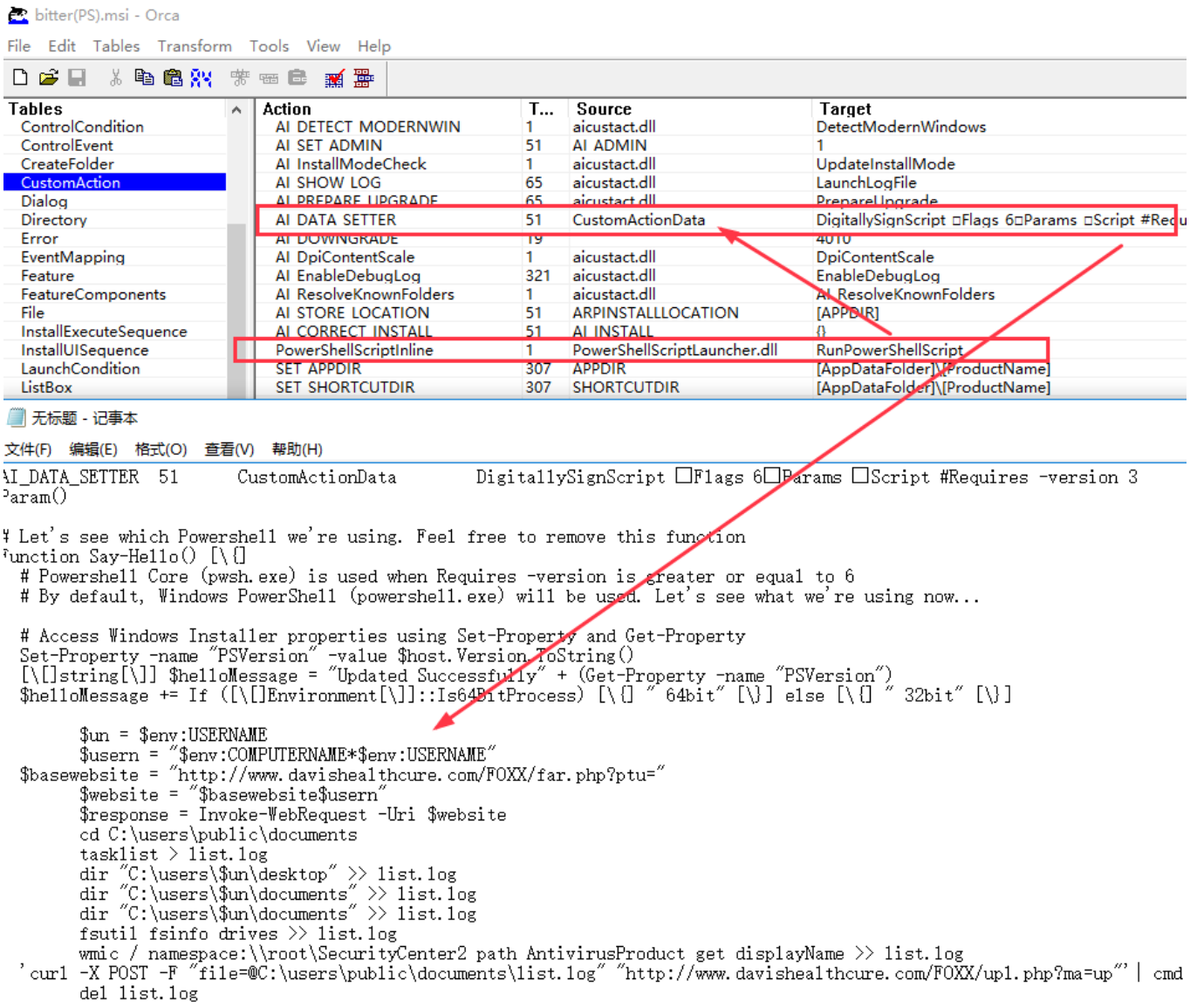
Media 表

Bitter、APT-Q-27、APT-Q-15(Darkhotel)、CNC 等 APT 组织将恶意组件压缩在 cab 中，在 MSI 安装过程中释放并执行，这也是目前最为常见的利用手法，缺点是恶意组件随着 MSI 的安装会落地在磁盘上，比较考验攻击者持续的免杀技术。

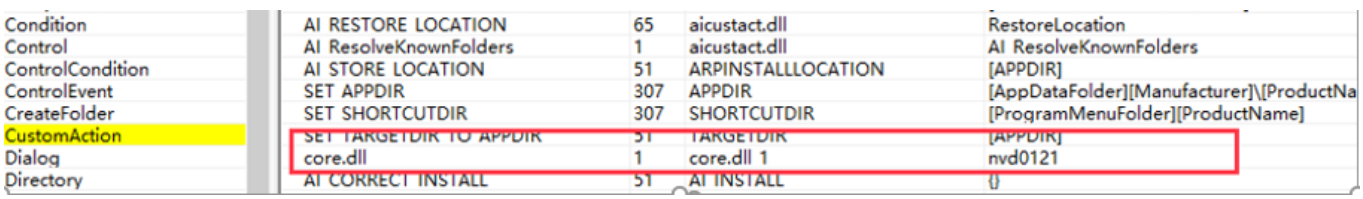


CustomAction 表

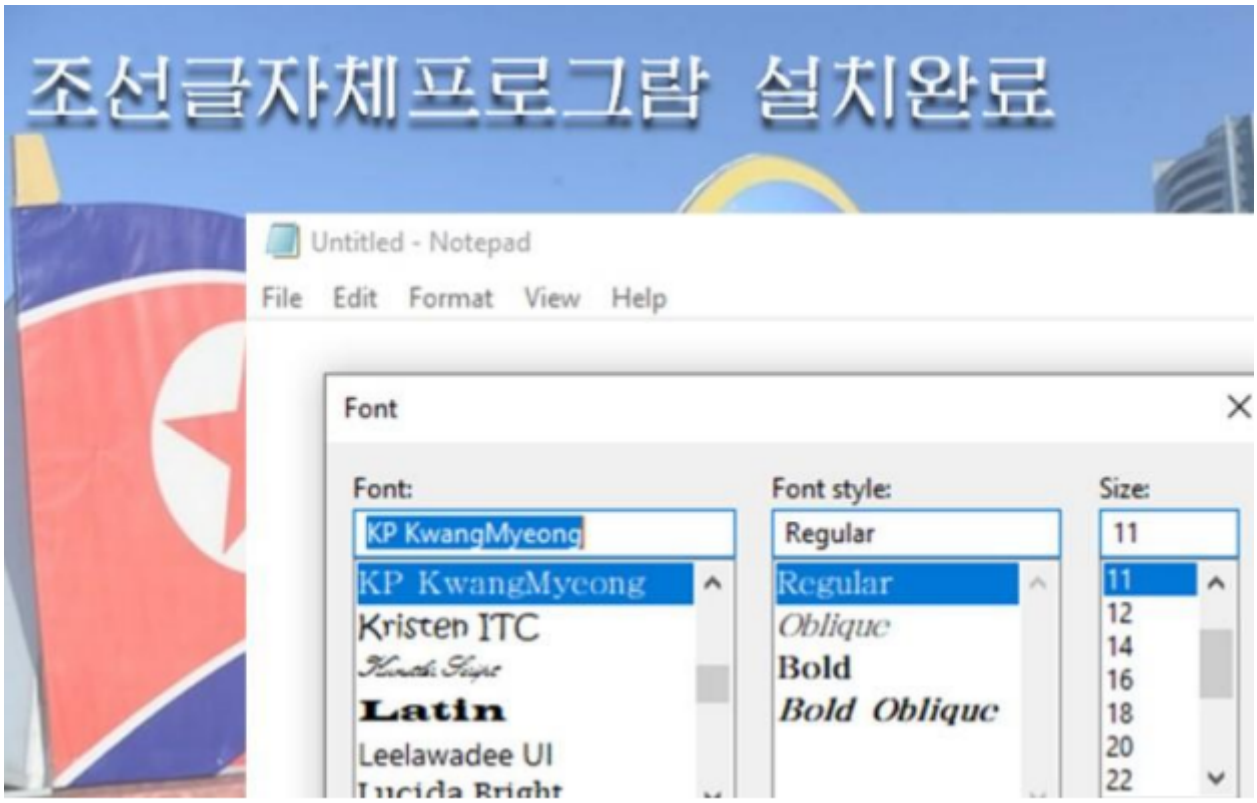
在 CustomAction 中支持各种类型的自定义操作，攻击者有较为丰富的操作空间，例如 Bitter 组织在 CustomAction 表中调用带有签名的第三方 Powershell 解释器执行 Powershell 脚本。



而APT-Q-15（Darkhotel）在针对朝鲜人的间谍活动中，投递恶意的朝鲜字体 MSI 安装包，将木马模块 core.dll 添加到 CustomAction表内，与 Media 表中插入的恶意模块相比，core.dll 在 MSI 安装过程中并不会落地，系统进程 msiexec 会启动一个独立的子进程内存加载该 DLL，从而达到 LOLBINS 的效果。



同时也不会影响 kpkm2024.ttf 字体的安装流程：



MST 文件

目前只观察到新海莲花组织在利用此技术。

总结

目前，基于奇安信威胁情报中心的威胁情报数据的全线产品，包括奇安信威胁情报平台（TIP）、天擎、天眼高级威胁检测系统、奇安信NGSOC、奇安信态势感知等，都已经支持对此类攻击的精确检测。

IOC

CC已经失效故暂不提供

MD5：

309a3a8f4d075d5d43d81d6357075b22

46623db76d5ff6b2ec5734fb84bade8e

参考链接

[1].https://mgeeky.tech/msi-shenanigans-part-1/

[2].https://intezer.com/blog/incident-response/how-to-analyze-malicious-msi-installer-files/