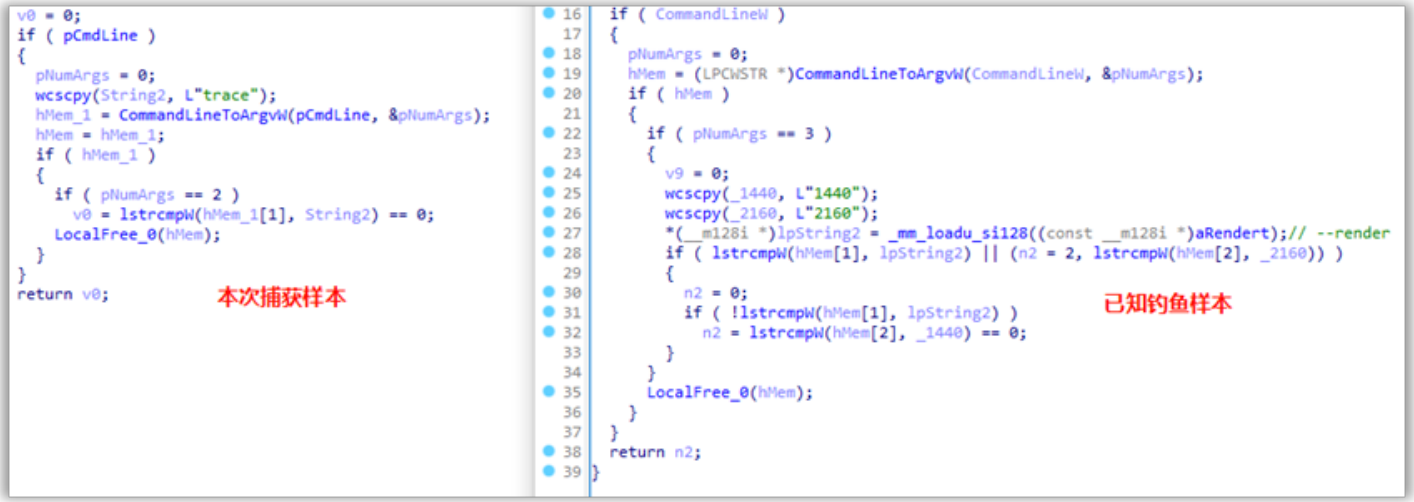
www.ctfiot.com /271395.html

疑似APT-C-00（海莲花）投递Havoc木马

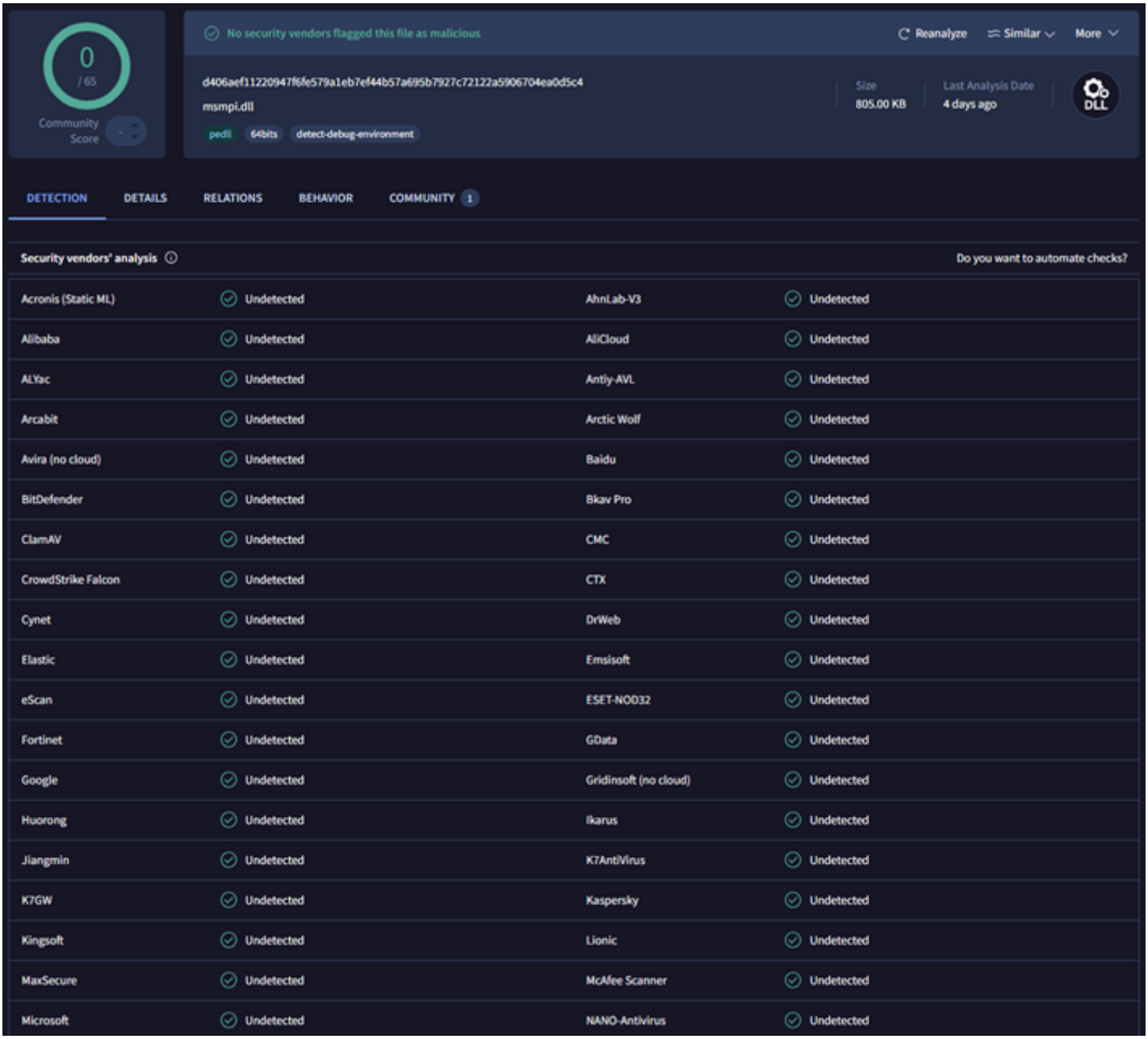


APT-C-00
海莲花

APT-C-00（海莲花）组织，是一个有政府背景的境外黑客组织，攻击目标主要是东亚国家的企业和政府部门。360高级威胁研究院一直持续跟进监测海莲花组织的最新攻击。

一、概述

近日360高级威胁研究院在日常威胁狩猎中捕获了一个可疑的木马加载器，经分析发现开发环境和执行流程与海莲花组织较为相似。目前依旧保持着0检出的优异免杀效果。



二、样本分析

MD5 64062595582c36d0aed322e98108ff4b
文件类型 DLL动态链接库
文件大小 824,320 Bytes

样本入口使用哈希算法动态获取需要使用的API函数。

```
*Sleep_0 = GetProcAddr4Hash(hKernel32, 391933954i64);
*lstrlenW = GetProcAddr4Hash(hKernel32, 809107012i64);
*LocalFree_0 = GetProcAddr4Hash(hKernel32, 1110266646i64);
*CloseHandle_0 = GetProcAddr4Hash(hKernel32, 3246825067i64);
*GetLastError_0 = GetProcAddr4Hash(hKernel32, 3202147271i64);
*CreateMutexW = GetProcAddr4Hash(hKernel32, 3335458567i64);
*GetCommandLineW = GetProcAddr4Hash(hKernel32, 1666048647i64);
*GetCurrentProcess_0 = GetProcAddr4Hash(hKernel32, 4149929963i64);
*LoadLibraryExA = GetProcAddr4Hash(hKernel32, 58198585 2i64);
*VirtualProtect_0 = GetProcAddr4Hash(hKernel32, 1970603793i64);
*GetConsoleWindow = GetProcAddr4Hash(hKernel32, 1469303412i64);
*FatalExit = GetProcAddr4Hash(hKernel32, 2502003714i64);
*LoadLibraryA = GetProcAddr4Hash(hKernel32, 4102247903i64);
*lstrcmpW = GetProcAddr4Hash(hKernel32, 80879235 7i64);
*GetProcAddress_0 = GetProcAddr4Hash(hKernel32, 1810725059i64);
v19 = *GetProcAddress_0;
if ( !*GetProcAddress_0 )
  return 0i64;
v20 = &cbKey[3];
strcpy(cbKey, "6'-ACI`BNBH_SChNDHFSDYIeWIIZB_");
do
{
  v20[1] ^= cbKey[&v20[1i64
                     - &cbKey[3]
                     - &v20[1i64 - &cbKey[3]] / 3
                     - (((0xAAAAAAAAAAAAAAABui64 * &v20[1i64 - &cbKey[3]]) >> 64) &
  ++v20;
}
while ( v20 != &cbKey[29] );
*RtlAddVectoredExceptionHandler = v19(hKernel32, &cbKey[3]);
if ( *LoadLibraryA )
{
  hUser32 = LoadLibraryA("user32");
  hShell32 = LoadLibraryA("shell32");
}
if ( !hUser32 )
  return 0i64;
*ShowWindow = GetProcAddr4Hash(hUser32, 1060019746i64);
if ( !hShell32 )
  return 0i64;
ProcAddr4Hash = GetProcAddr4Hash(hShell32, 2949986778i64);
hAdvapi32 = ::hAdvapi32;
*CommandLineToArgvW = ProcAddr4Hash;
if ( !::hAdvapi32 )
  return 0i64;
*RegCloseKey = GetProcAddr4Hash(::hAdvapi32, 97459290 2i64);
*RegOpenKeyExW = GetProcAddr4Hash(hAdvapi32, 1894003958i64);
*RegSetValueExW = GetProcAddr4Hash(hAdvapi32, 3121069284i64);
*RegQueryValueExW = GetProcAddr4Hash(hAdvapi32, 518293454i64);
```

导出函数MPI_Init中创建互斥体”GlobalMicrosoftMPI”确保单实例运行，命令行参数校验用于规避常规自动化流程，当参数检查通过后将启动命令行添加至注册表自启动项”HKCUSOFTWAREMicrosoftWindowsCurrentVersionRunMicrosoftMPI”实现持久化，最后将执行Shellcode的函数设为VEH异常处理的回调函数等待调用时机。

调用位于0x1800760F0处的导出函数，加载系统文件certmgr.dll，使用模块镂空的方式将Shellcode代码替换certmgr模块.text节的代码。

Shellcode为反射加载Havoc RAT[1]。

三、关联分析

样本为DLL文件，且大部分导出函数指向同一函数地址，推测样本本身是以白利用方式加载，符合海莲花组织的常用技战术。

样本使用Mingw-w64开发，符合海莲花组织近年的开发环境。

本次捕获样本与此前已知钓鱼样本均使用了相同的算法在初始化阶段动态获取API地址。

海莲花组织的加载器在执行初始化步骤时，通常会有创建互斥锁、检查命令行、持久化等流程。如持久化此前使用过加载器直接写注册表和解密执行Shellcode写注册表自启动项，又如释放诱饵文档的步骤，有时会在钓鱼压缩包中由加载器打开诱饵文档，有时则内嵌在加载器中释放打开。每轮攻击略有不同，但大致类似。

四、ATT&CK

持久化	防御规避
(TA0003)	(TA0005)
注册表启动项/启动文件夹	DLL侧加载
(T1547.001)	(T1574.002)
	挖空进程执行代码
	(T1055.012)

总结

警惕不明链接和附件：不要轻易点击电子邮件或短信中的链接，特别是那些来自不熟悉或可疑来源的消息。即便是熟悉的人发送的，仍需仔细确认。

员工安全意识培训：定期对员工进行网络安全培训，模拟钓鱼攻击，帮助员工识别钓鱼邮件和其他网络威胁。

网络分段和隔离：将关键业务系统、数据存储和员工网络分开，使用防火墙和访问控制列表来限制各段之间的访问，从而防止攻击者在入侵后横向移动。
定期审查和修复漏洞：定期进行安全审查和渗透测试，及时发现和修复漏洞，减少被利用的可能性。

附录 IOC

MD5

64062595582c36d0aed322e98108ff4b

2ca07512ba04df5d2d22a2c97d83cd5f

860c9bc3c291de45856218c2059e1117

ca1376132df84cb3be08d43114ad32d7

2da7798e8f7fbeafefbd297e3be5b21b

6725c332b0fe684fbc94df399ab726bc

963448d96d81138413f192dd80558d76

C&C

144.202.46.221[:]443

46.37.124.147[:]80

参考

[1]https://github.com/HavocFramework/Havoc

团队介绍

TEAM INTRODUCTION

360高级威胁研究院

360高级威胁研究院是360政企安全集团的核心能力支持部门，由360资深安全专家组成，专注于高级威胁的发现、防御、处置和研究，曾在全球范围内率先捕获双杀、双星、噩梦公式等多起业界知名的0day在野攻击，独家披露多个国家级APT组织的高级行动，赢得业内外的广泛认可，为360保障国家网络安全提供有力支撑。

本篇文章来源于微信公众号: 360威胁情报中心