3 月 9 日，中国区网络安全监测实验室（China RTL）监控到一起针对金融行业的 APT，此威胁会导致用户重要信息数据泄露。通过对收集的样本进行分析，我们可以得到以下关键信息。

该病毒具有 APT 特征：

1. 针对性：该病毒基本都是在证券、基金、银行等金融行业相关的客户环境中被发现
2. 潜伏性：从该病毒的显示的一些信息发现此文件可能在用户环境中存在一年以上或更久
3. 持续性：截止目前为止，该病毒作者仍然在对该病毒家族进行更新，以对抗安全软件对其进行的检测

技术指标：

对系统的修改：

1. 该病毒会将自身伪装为正常的系统文件，目前获取的样本文件的版本信息都十分规范并全面
   目前已知它会伪装为 Intel，Microsoft ,Adobe 等厂商的的文件
2. 在%windir%\system32\创建 MurocApc.dll （ 此为该恶意威胁的主要组件,目前被检测为 TROJ_JNCTN.A-CN,其他相关的文件目前被检测为 TROJ_JNCTN.A-CN, TROJ_JNCTN.B-CN, TROJ_JNCTN.C-CN, TROJ_JNCTN.D-CN, TROJ_JNCTN.E-CN)
3. 该病毒会在感染电脑中创建 \documents and settings\all users\application data\microsoft\opengl 文件夹
   用于存放主程序的副本以及其他一些组件。为了掩饰该文件夹的恶意性，它还会将一些安全软件的组件（例如 360safe 的组件）也复制到此文件夹中
4. 在系统中创建服务
   RemoteRegistry （修改了系统的服务）
   Lanmanserver （修改了系统的服务 ）
   SCPolicySvc （ 病毒创建的服务)
5. 将自身加载至注册表 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\以达到自启动目的

恶意行为：

1. 搜索系统中的 * .doc，*.xls,*.ppt ,*.xls,*.rtf,*.csv 类型文件并将它们上传至远端服务器
2. 截取用户桌面的 msn 聊天窗口，并提取其聊天对象的历史记录上传至远端服务器
3. 通过 hook 系统登录界面获取登陆系统的账号密码
4. 通过对一些正常网页中的 jpg 图片文件末尾插入数据来进行更新以及其它一系列数据交换行为（jpg 中的数据为加密代码)
5. 会注入以下系统服务，进程：
   dns.exe
   tcpsvcs.exe
   WINS.EXE
   inetinfo.exe
   msdtc.exe

svchost.exe

explorer.exe

6． 获得被感染终端的地理位置

7．通过1418端口接受远程指令。并可以通过被感染的计算机控制其他被感染计算机

采取的特殊技术和手段：

1. 反侦测报警

   该恶意程序有一套完整的警报系统，会对各种系统状况以及程序异常进行报警。例如：它自身携带一个杀毒软件的列表，当它扫描到系统中具有列表中的杀毒软件是它就会对远端控制者发出警报（但是该病毒并不会阻止或者破坏杀毒软件）

2. 采用 junction 技术

   该恶意程序在写入启动项时采用 junction 技术。用来隐藏自己真正的位置

3. 该病毒在发送日志时使用 https 协议

   该病毒传送日志时采用 https 协议，使得传输数据很难被破解

4．各个组件之间使用一个全局 map 进行控制，并且通过这个全局 map 通讯

该技术可以实现进程通讯,利用多进程协作让，各个功能在不同进程中实现以躲避行为监控之类的安全检测

5. 该恶意文件能够再 X86 和 X64 的多版本操作系统中运行

   Microsoft windows 2000

   Microsoft windows 2008

   Microsoft windows 7

   Microsoft windows 95

   Microsoft windows 98

   Microsoft windows Millennium Edition

   Microsoft windows NT

   Microsoft windows xp

如何确定自己感染了 TROJ_JNCTN.A-CN

1． 确认%windir%\system32\目录是否存在 MurocApc.dll

2． 确认是否存在\documents and settings\all users\application data\microsoft\opengl 文件夹

3． 确认注册表是否有以下键值

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\ZmEvMon

Startup = [Hidden]WLEventStartup

StartShell = [Hidden]WLEventStartShell

Shutdown = [Hidden]WLEventShutdown

DLLName = [Hidden]C:\Program Files\Microsoft\OpenGL\MurocApc.dll

如果电脑中存在以上内容可以确认该电脑感染了 TROJ_JNCTN.A-CN

趋势科技建议使用以下方法进行防护 TROJ_JNCTN.A-CN：

1．使用趋势桌面防毒产品对 \documents and settings\all users\application data\microsoft\opengl ，%windir%\system32\MurocApc.dll 进行爆发阻止

2． 开启 WRS Web 防护功能

3． 将防毒软件病毒码更新至最新

趋势科技提供专杀工具以清除此病毒：
http://support.trendmicro.com.cn/Anti-Virus/Clean-Tool/TROJ_JNCTN-CN/

目前趋势科技 wrs 已阻止该病毒用以更新以及数据交互的恶意链接
趋势科技最新中国区病毒码 8.864.60 已可检测该病毒目前发现的所有相关组件

由于此病毒仍然在不停更新，China RTL 也将持续更新解决方案