Operation(काराकोरम) Tejas：蜷居在昆仑山脉的残喘枯象

By 红雨滴团队

Archived: 2026-04-05 14:59:58 UTC

概述

奇安信威胁情报中心曾在2021年曾经发表过《Operation Magichm：浅谈蔓灵花组织的CHM文件投放与后续操作》一文，时隔一年我们发现蔓灵花团伙（APT-Q-37）在四月份最新的攻击活动中使用了新的攻击手法和样本，除此之外文末还会对摩耶象（APT-Q-41）近期的钓鱼活动和响尾蛇（APT-Q-39）今年以来的基础设施进行分享。

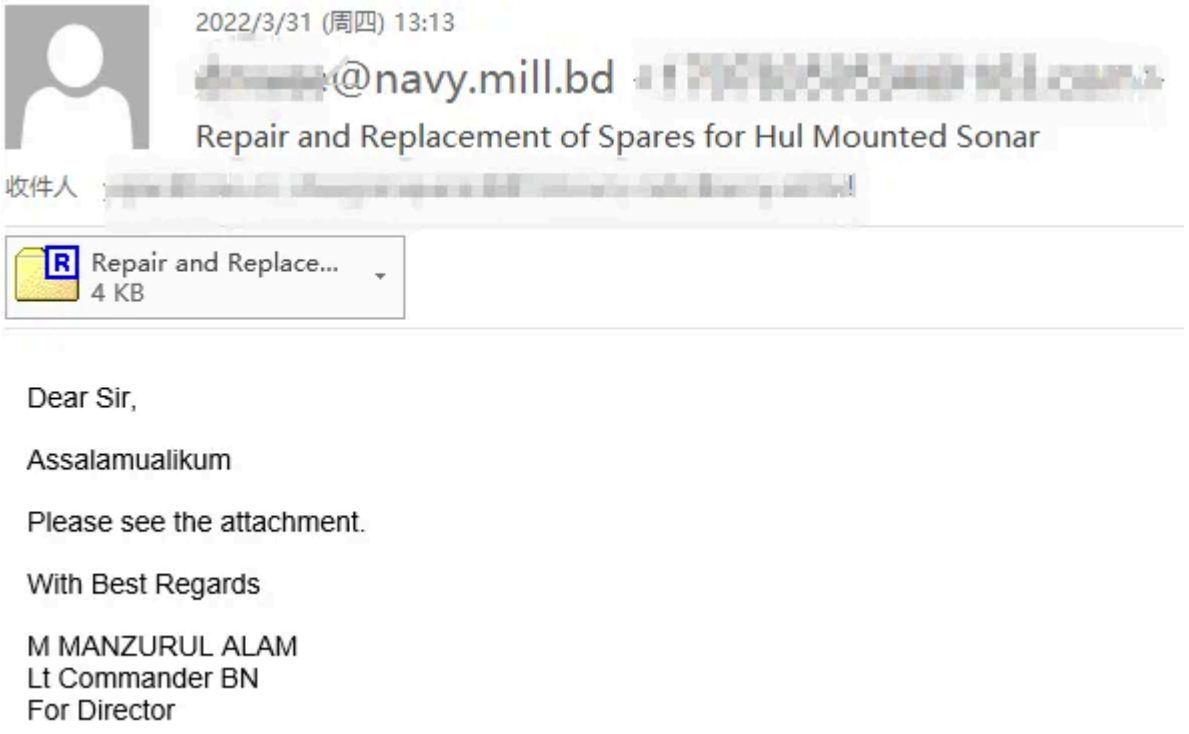
从南亚方向近两年的攻击活动来看，各个组织仍然处于“吃老本”的状态，没有推陈出新的倾向，存在针对11882和8570等古董漏洞的路径依赖，在木马免杀方向也非常不理想，往往被天擎查杀四五次后还未到达免杀状态。这令我们感到失望。我们推测产生这种现象的原因可能与南亚地区的安全环境有关。

与之前的文章类似，本文内容也仅仅是对在过去一段时间内攻击手法做一个分享。文末会分享相关组织历史或未启用的基础设施。

APT-Q-37(蔓灵花)

邮件分析

蔓灵花组织仿冒军贸客户（孟加拉海军）以维修船体声纳为主题向军工企业投递的带有chm附件的钓鱼邮件。



除了chm，蔓灵花还投递了带有DDE auto的文档作为附件。仿冒军工企业以推销反无人机系统为主题向军贸客户（孟加拉空军）投递钓鱼邮件。

攻击者拿到军贸客户的邮箱权限后，会在正常来往邮件中新增的一个恶意的DDE附件，以此来提高钓鱼的成功率。

正常PDF如下：

使用可信邮箱向列表全员发送带有新年祝福的SFX样本。

投递带有宏文档的钓鱼邮件

诱饵分析

DDE AUTO

由于Chm过于常见，故这里不做分析，DDE文档如下:

文件名	**MD5**	**类型**
Technical Proposal of Portable Anti-Drone System.docx	54ea5083ad67b15a249e07bb1a4fb3e0	DDE AUTO
China Great Wall Industry Corp (CGWIC) Profile and POC.docx	54ea5083ad67b15a249e07bb1a4fb3e0	DDE AUTO
Payment Detail.docx	54ea5083ad67b15a249e07bb1a4fb3e0	DDE AUTO
Invitation to Visit Bangladesh(Officials of Chinaship).docx	54ea5083ad67b15a249e07bb1a4fb3e0	DDE AUTO

REPAIR,REPLACEMENT OF SPARES FOR HULL MOUNTED SONAR (ESS-2)-BNS NISHAN.docx	54ea5083ad67b15a249e07bb1a4fb3e0	DDE AUTO

文档内容为空，故上述诱饵MD5均相同，只是投递对象略有不同。

DDE信息如下：

执行远程服务器上的msi文件，与chm诱饵文件下发的msi相同，值得一提的是DDE的手法与之前我们在《Operation(विक्रान्त)Vikrant：屹立于精神内景中的钢铁巨象》一文中披露的APT-Q-42腾云蛇组织相同，我们猜测可能是不同组织间武器共享或者组织人员间进行了合并。

SFX（JPG、DOC）

投递的SFX样本信息如下：

文件名	**MD5**	**类型**
2323orvttes.docx .exe	4069d394ff1e55fa9dde2f81567d681e	SFX
医疗保险报销单-样表和空白表.xls.zip	f69fa2d07e1ad0625af8a5ec44db327d	SFX
greetings.jpg.exe	dc269726626de55214f6f49f39ebc33a	SFX
APSCO Distance Training on “Satellite Constellations.docx.exe	6d6e144c182a0f0e43593e05dd990239	SFX

可以看到SFX中的内容出现了明显的变化，将exe文件替换为了chm，主要目的是为了免杀，诱饵内容如下

诱饵1：

诱饵2：

诱饵3：

宏文档

宏文档投递数相对较少。

文件名	MD5	类型
XX业务培训制度.rar	c44567e2b4b3c92dc871159481894917	宏

内容如下：

主要功能为创建计划任务

除了上述的手法，还会使用带有CVE-2018-0798的xlsx进行投递，相关内容如下：

PDF文件如下：

鉴于友商之前已经披露，且VT上有大量相似的样本，故不再赘述。

样本分析

最近我们观察到蔓灵花正在修改MSI木马，新型的MSI样本如下：

MD5	类型
9790ef74625b4f9b67bc64aa7eff0e4b	MSI
5be886f7a6cbc23a0a00bdb2153f435b	MSI

MSI中仅包含了一个名为Scan.vbs的恶意脚本

VBS脚本内容如下，与宏样本中的代码同源，创建计划任务。

今年以来我们捕获到的基于ArtraDownloader后台下发的插件

文件名	MD5	类型	功能
iexplorer	3268b2aeb16be4bb9b953257af74b805	VC++	键盘记录模块
stdrcl3	71e1cfb5e5a515cea2c3537b78325abf 058cff1c34118fe46a641286b4cdfc92	.net	轻量化远控
mthost2.exe mtstimuli msstimuli	a9ed771d128a6ccf67097b6ecd136885 c66a35a9c1778ab162e3718afbd8c3ac a70cb6a15e03284d59c0ae4e33324448	.net	下载者
sthost.exe	dbf780ef27a421211c69698837986738	.net	文件收集模块
sysmgrnew.exe sysmgr.exe asmsN asmsy asmsNN lsapip	a16d12819fc03a3b9f0b63786f26a4c7 ade9a4ee3acbb0e6b42fb57f118dbd6b b63e9710cb67f4a649a83929ed9f0322 ff2905648780aea95f578d11def872c4 f505ef12881fa57fcdd12ac59cf55fd8 660a678cd7202475cf0d2c48b4b52bab	VC++	文件收集模块

插件功能与之前类似，样本PDB信息如下：

PDB
g:\Projects\cn_stinker_34318\feb22\renewedstink\renewedstink\obj\Release\stimulies.pdb
g:\Projects\cn_stinker_34318\feb22\renewedstink\renewedstink\obj\Release\stimulies.pdb
C:\Users\Window 10 C\Desktop\COMPLETED WORK\stdrcl\stdrcl\obj\Release\stdrcl.pdb

除了ArtraDownloader的后台外，我们意外发现了基于CHM的后台。

由于请求时会在后面接机器名和用户名，所以通过Opendir可以看到后台页面为每台受害者都创建了一个目录。

攻击者通过FTP的方式向指定受害者目录下上传msi文件，实现木马的下发。

MuuyDownLoader在去年发布的《Operation Magichm 浅谈蔓灵花组织的CHM文件投放与后续操作》一文中命名，被认为是ArtraDownloader的替代品。

新活动的样本如下：

MD5	**类型**
6e4b4eb701f3410ebfb5925db32b25dc	VC++

与去年的样本执行流程类似，经过两层循环与服务器认证完成后通过/JvQKLsTYuMe/xAexyBbnDxW/fFsw47e5ss/目录下发插件。

我们不清楚MuuyDownLoader与ArtraDownloader是否有着完全相同的后台页面。但我们从MuuyDownLoader获取的插件与ArtraDownloader下发的插件是完全相同的。

基于奇安信大数据平台，蔓灵花组织在二月底至三月初时间段内利用.net节点疯狂下发插件，在我们没有更新天擎特征库的情况下，插件反复被杀，相关人员到达现场后发现了如下壮观的一幕。

这意味着攻击者的免杀水平有待提升。

APT-Q-41(摩耶象)

摩耶象投递的钓鱼邮件如下：

攻击者通过投递html或者压缩包中带有html的方式诱导受害者双击html。通过这种方式能够绕过针对eml内嵌URL检测

最终会跳转到钓鱼页面。输入账号密码后跳转到PDF文件，近期该团伙钓鱼使用的诱饵文件如下：

诱饵1：

诱饵2：

诱饵3：

诱饵4：

诱饵5：

诱饵6：

APT-Q-39 (响尾蛇)

响尾蛇组织在过去的一段时间内仍利用11882等古董漏洞和带有Lnk的压缩包进行鱼叉攻击。

近期友商公布了该组织最新的攻击手法，在报告中提到响尾蛇团伙仅仅针对上层释放流程进行了修改，释放的木马仍然是老架构，我们会在文末分享近期疑似响尾蛇针对巴基斯坦进行攻击的基础设施，但不排除这些基础设施在未来会攻击其他地区。

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。

（https://sandbox.ti.qianxin.com/sandbox/page）

IOC

APT-Q-37(蔓灵花)

MD5：

54ea5083ad67b15a249e07bb1a4fb3e0

4069d394ff1e55fa9dde2f81567d681e

f69fa2d07e1ad0625af8a5ec44db327d

dc269726626de55214f6f49f39ebc33a

6d6e144c182a0f0e43593e05dd990239

c44567e2b4b3c92dc871159481894917

9790ef74625b4f9b67bc64aa7eff0e4b

5be886f7a6cbc23a0a00bdb2153f435b

3268b2aeb16be4bb9b953257af74b805

71e1cfb5e5a515cea2c3537b78325abf

058cff1c34118fe46a641286b4cdfc92

a9ed771d128a6ccf67097b6ecd136885

c66a35a9c1778ab162e3718afbd8c3ac

a70cb6a15e03284d59c0ae4e33324448

dbf780ef27a421211c69698837986738

a16d12819fc03a3b9f0b63786f26a4c7

ade9a4ee3acbb0e6b42fb57f118dbd6b

b63e9710cb67f4a649a83929ed9f0322

ff2905648780aea95f578d11def872c4

f505ef12881fa57fcdd12ac59cf55fd8

660a678cd7202475cf0d2c48b4b52bab

6e4b4eb701f3410ebfb5925db32b25dc

C2：

rurushophoogtypnl.com

botanoolifeapp.net

maildataserver.com

deliverymailserver.com

ekoconect.com

pnptrafcroutsvc.net

epapbuizhost.net

svc2mcxwave.net

URL：

http://193.142.58.186/UihbywscTZ/45Ugty845nv7rt.php

APT-Q-39 (响尾蛇)

C2：

docuserve.ltd

doken.xyz

fdn-mac.net

gov-pk.net

filedownload.work

trik.live

norter.xyz

paf-gov.net

dawnpk.org

pak-gov.net

afg-refugee.net

slap-games.club

ministry-pk.net

nationpk.org

cssc.info

mofa-pk.co

paf-mail.com

pakgov.org

docuserve.cc

brwse.co

cvix.live

pakgov.net

kpt-pk.net

crclab-bahria.org

pkrepublic.org

mod-pk.com

watch-earn.live

civix.live

paknavy.live

点击阅读原文至**ALPHA 5.0**

即刻助力威胁研判
