威胁发现与响应专家

Leader in Threat Detection and Response

2020

疫情阴影笼罩下的2020年APT组织活动

ThreatBook 微步在线

邮箱： contactus@threatbook.cn

电话： 400-030-1051

北京： 北京市海淀区海淀街道苏州街 49-3 盈智大厦 3 层

上海： 上海市浦东新区盛荣路 88 弄盛大天地源创谷 6 号楼 306 室

深圳： 深圳市南山区海德三道海岸大厦东区 A 座 509

广州： 广州市天河区体育东路 116 号财富广场东塔 2401 A

ThreatBook 微步在线

01

概述

2020 年是不平凡的一年。年初，在中国全民投入抗击“新冠病毒”的战役之际，白象、响尾蛇、蔓灵花、海莲花、绿斑、蓝宝菇等一批长期窥伺我国的 APT 组织却趁火打劫，借疫情话题对我国有关部门和人员发起了更为猛烈的网络攻击；而当“新冠病毒”开始在全球范围内肆虐时，APT29、WellMess、Silence、Lazarus、Kimsuky 等组织则将目光瞄准了疫苗研发机构，试图盗取新冠疫苗开发和测试有关信息和知识产权；年末，美国的财政部、商务部及其他政府机构遭遇国家级 APT 组织的供应链攻击事件，再一次让人们意识到网络安全对国家安全的重要意义。

微步在线作为唯一连续三次入选Gartner全球威胁情报市场指南的中国公司，一直持续关注对 APT 攻击的研究。通过自研的黑客画像、威胁狩猎和追踪溯源系统，实现了对全球数十个活跃 APT 组织的持续追踪。本报告以地域维度对主流 APT 组织在 2020 年期间的活动情况进行了概述，主要内容包括：

- 自新冠疫情爆发以来，各 APT 组织纷纷以疫情话题作为诱饵来实施攻击活动，我国作为 APT 攻击的主要受害者，遭受到了具有印度、越南、台湾、俄罗斯等国家和地区背景黑客的 APT 攻击。
- 大多数被曝光的 APT 活动仍通过钓鱼网站、鱼叉式攻击和水坑攻击及 Nday 漏洞等常见手法实施，高级攻击手法仅在特定组织的活动中出现。
- 假旗战术。部分 APT 组织会伪装成其他组织实施攻击活动，主动误导分析者来掩盖自身活动并嫁祸他人。
- 跨平台攻击。多个 APT 组织展现出了在 Windows、Linux、macOS、Android 等多平台实施攻击活动的能力。
- 复杂供应链攻击活动曝光。2020 年的供应链攻击活动较多，其中尤以 SolarWinds 供应链攻击活动复杂、隐蔽、精巧，美国的政府和关键企业在遭受攻击长达一年左右的时间中都未能发觉。该事件说明来自外部的网络安全威胁依然十分巨大。

目录
CONTENTS

02 整体情况

在 2020 年，微步在线威胁追踪团队持续跟踪境内外的 APT 攻击活动，捕获了绿斑、海莲花、蔓灵花、白象、孔夫子、拉撒路、响尾蛇等 APT 组织发起的大量攻击活动，撰写相关报告、通报 50 余篇，积极协助国内有关部门抵御来自境外的网络威胁。

基于微步在线黑客画像系统数据统计发现，在 2020 年，被曝光的 APT 攻击事件近百起，40 余个国家和地区遭受了不同程度的 APT 攻击，中国、美国、韩国、印度、巴基斯坦、乌克兰和中东、欧洲等地区是 APT 攻击最大的受害者，政府、军事、外交、科技、金融、医疗、能源和教育等行业是攻击者瞄准的主要目标，而发起者主要来自南亚、东南亚、朝鲜半岛和中东地区。

此外，随着信息技术的发展，跨平台的 APT 攻击已成为主流，而不再单一聚焦于 Windows 平台。据统计，成熟度较高的 APT 组织如海莲花、Lazarus、Turla、APT28 等均实施过跨平台的攻击活动，主要集中于 Windows、Linux 和 Android 平台，少量出现在 macOS/iOS 平台。

下表是对本报告中涉及的主流 APT 组织跨平台攻击情况的统计情况：

APT组织 / OS平台	Windows	Linux	Android	macOS
孔夫子 (Confucius)	有		有	
蔓灵花 (Bitter)	有		有	
响尾蛇 (SideWinder)	有		有	
肚脑虫 (Donot)	有		有	
假旗部落 (FalseFlager)	有		有	
海莲花 (OceanLotus/APT32)	有		有	有
Lazarus	有	有	有	有
危险密码	有			
DarkHotel	有			
Kimsuky	有		有	
Konni	有		有	
绿斑	有			
Gamaredon	有			
APT28	有	有		
Turla	有	有		
WellMess	有	有		
APT35	有			
MuddyWater	有			
APT-C-23	有		有	
StrongPity	有			

典型攻击手法

供应链攻击

2020 年 12 月 13 日，国外网络安全公司 FireEye 发布安全分析报告称，2020 年 3 月至 6 月期间，有攻击者通过将美国基础网络管理软件供应商 SolarWinds 的商业软件更新程序木马化，以污染供应链方式入侵了北美、欧洲等地区的政府、科技、电信等重要机构，最终实现信息窃取的目的。该报告一石激起千层浪，随着各大安全公司分析的逐渐深入，更多受害者也开始浮出水面，包括美国国防部、国务院、商务部、财政部和国土安全局等政府机构，火眼、微软等科技公司也都涉及其中，媒体报道称“美国正遭遇史上最严重黑客袭击”。

通常来说，供应链攻击极难防御检测，而作为拥有大批美国政府部门客户的 SolarWinds，是一个绝佳入口点，携带有后门的网络产品完美绕过了相关部门的安全防御体系，加之后门通信技术以及域名选择方面更是提高了被检测难度。此次攻击活动从开始实施到被披露至少经过半年，攻击者拥有充足的时间对核心目标单位进行进一步攻击，是供应链攻击又一个经典案例，影响范围远超近年来的 Xcode、CCleaner、Xshell、phpStudy、驱动人生等软件供应链攻击事件。

隔离网渗透

2020 年 5 月，国内外两家安全公司分别曝光了 DarkHotel 组织一款名为 Ramsay 的攻击工具，该工具可在物理隔离网络中收集信息，且无网络行为，属于定制性木马。

借助物理层面的网络隔离，在理想情况下可以有效地阻断传统的基于网络路由可达的网络攻击、确保隔离内网的生产环境的安全稳定。然而隔离网络系统的建设注定要牺牲网络数据交换的便捷性，为了解决实际生产环境中的数据交换需求，经常会出现一些“不得已”的违规操作，譬如搭建内网跳板机映射共享目录、使用可移动存储设备进行数据摆渡等，这些操作相当于间接打通一条与外网通信的隧道、破坏了物理隔离的完整性。

Ramsay 可通过被感染的软件安装包进行传播，该程序在隔离网络的主机上被运行后，会执行 exe 文件感染、内网扫描、文档收集等行为，并将收集到数据加密压缩并附加在正常文档中，待这些文档被带出隔离网络并接入在其他被控的设备后，攻击者就能够成功提取窃取的数据，实现对隔离网络攻击。Ramsay 是继 Stuxnet（震网）攻击事件、Flame 蠕虫、CIA 网络武器库 Vault7、NSA 秘密武器 COTTON-MOUTH 等隔离网突破组件后的又一经典案例。

挖矿伪装

2020 年 11 月，微软发布分析报告称，越南背景的黑客组织海莲花在今年的攻击活动中通过在受害者主机部署门罗币挖矿程序，以此隐藏其高级攻击的行为。

研究发现，海莲花至少在针对越南本国、法国和我国的攻击中均使用了该手法，攻击活动通常由定向钓鱼邮件开始，通过诱导目标用户执行恶意文档植入白利用木马，然后以该主机为据点对目标企业内部进行横向渗透，海莲花会在这个阶段部署门罗币挖矿木马，即使用户发现网络中的异常，也会判定为挖矿活动选择忽视或低优先级处理，从而隐藏了攻击的真实目的。据悉，海莲花已通过此类挖矿活动获利上千美元，且越来越多的政府支持黑客开始从借助常规网络犯罪活动掩盖定向攻击，为应急响应定级带来新的挑战。

雇佣 APT

2020 年 8 月 24 日，国外安全厂商曝光了一个在全球范围内开展 APT 活动的黑客组织 DeathStalker，该组织主要针对金融科技公司、律师事务所和财务顾问，他们并不实施安装勒索软件、窃取支付信息等常见黑产的活动，而是专注收集商业机密，因此安全分析师判断该组织具有雇佣兵性质，攻击活动主要是为雇主服务。

DeathStalker 主要使用一种称为 Powersing 的攻击武器实现远程控制，该工具主要使用诸如 Google+、Twitter、YouTube、Imgur、Reddit、Reddit 等公共平台存放加密密钥及真正的 C2 地址，然后不断将受害者的屏幕截图发送至 C2 服务器，同时可以执行从 C2 下发的其他脚本，以便攻击者实施更多后续操作。此类黑客团伙并非具备国家背景的 APT 组织，但其对大多数商业公司具备更大威胁。

勒索病毒

勒索病毒一般用于追求收取利益，这种攻击手法在 APT 组织攻击活动中并不常见，但在今年的观察中发现，多个 APT 组织开始采取使用勒索病毒作为攻击流程的一部分，例如熟知的 Lazarus 组织在今年上半年攻击活动中通过 VPN 网关漏洞进行入侵并使用其后门 Dacls，在接管 AD 服务器后使用 VHD 勒索软件感染网络中所有计算机，根据 Lazarus 历史活动来看，极有可能以敛财为目的投递勒索病毒。

而使用勒索病毒并非来自半岛 APT 组织专有手段，在下半年的活动中，来自中东的两个 APT 组织同样使用勒索病毒作为他们的攻击手段之一。在针对中东与北非的“流沙行动”中，MuddyWater 组织在受害者机器上部署 PorwGoop 木马后，继续下载 Thanos 勒索病毒。而另外一个 Fox Kitten 组织在其活动中则使用 Pay2Key 勒索病毒。结合今年中东发生一系列矛盾冲突事件，不排除以破坏报复以及隐藏痕迹等目的。

结合今年多个 APT 活动使用勒索病毒的情况来看，我们猜测勒索病毒可能作为 APT 组织武器库中另外一件利器将越来越普遍。

04 团伙详情

南亚

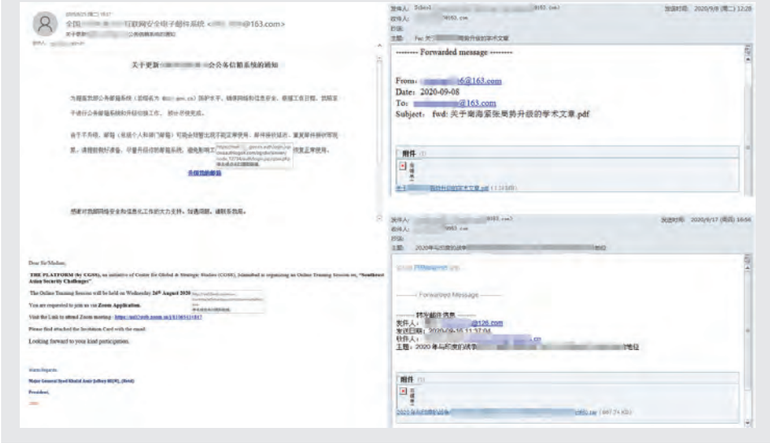
鉴于中国西南方向的地缘政治局势，涉印方向 APT 组织一直是对华网络攻击的主力军。在 2020 年新冠肺炎爆发和中印关系恶化的特定背景下，涉印方向 APT 组织对中国的网络攻击愈是变本加厉，其攻击目标涵盖中国境内政府、军队、军工、核电、航空航天、科研机构、高等院校、经济贸易、通信运营商、藏区政府等各个方向。根据涉印 APT 组织对中国的网络攻击活跃程度，孔夫子（Confucius）组织应是充当其主力网军队伍，其次为蔓灵花（Bitter）组织和白象（Patchwork）组织，肚脑虫（Donot）组织和响尾蛇（Sidewinder）组织攻击频次相对较低。

1. 孔夫子

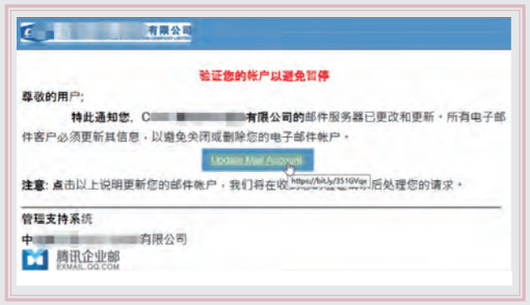
孔夫子（Confucius）组织是一个印度背景的 APT 组织，主要针对南亚各国的政府、军事等行业目标进行攻击。该组织在早期攻击活动中使用的恶意代码和基础设施与白象（Patchwork）APT 组织早期所使用的存在较大重合，但是目标侧重有所不同，早期的孔夫子组织一度被认为是白象 APT 组织的某个分支机构。

自 2019 年至今，孔夫子 APT 组织持续使用钓鱼邮件进行定向攻击，尤其是在 2020 年第三季度活动频率显著增加。监测发现，孔夫子 APT 组织的定向网络攻击活动可以大致分为两类：（1）以窃取目标人员的邮箱账号密码为目标的钓鱼攻击；（2）通过植入恶意间谍木马进行窃密活动的钓鱼攻击。在以窃取目标人员邮箱账号密码为目标的钓鱼攻击中，攻击者通常伪造“邮件系统升级”、“账户安全验证”、“账户扩容”等有时间紧迫性的主题内容，然后内嵌恶意的 Web 邮箱登录 URL 外链对象，诱使用户点击，来骗取目标人员的邮箱账密信息、从而为后续攻击做准备。在通过植入恶意间谍木马进行窃密活动的钓鱼攻击中，攻击者多以“中印政治关系”、“南海局势”、“台湾问题”等敏感政治话题为诱饵，向目标人员发送携带恶意攻击载荷附件的钓鱼邮件。

部分代表性钓鱼邮件如下：



年度代表性攻击事件如下：



在 2020 年，孔夫子 APT 组织对中国的攻击目标较 2019 年相比有显著增多，涵盖国内政府、军工、航空航天、科研机构、经贸、高等院校等多个重点行业目标。与孔夫子 APT 组织在历史攻击活动中所投入的特马武器（Confucius_CPP_Stealer 自研窃密木马）不同的是，该组织在 2020 年的攻击活动中还大量投入使用了商业木马和开源木马，如 AveMaria、AsyncRAT、Morphine 等商业远控木马以及针对移动端的 SpyNote 开源安卓远控木马，来对目标人员或组织进行窃密和监听。

简而言之，孔夫子 APT 组织是 2020 年下半年中印关系紧张的局势背景下印方对华攻击的主要网军队伍。

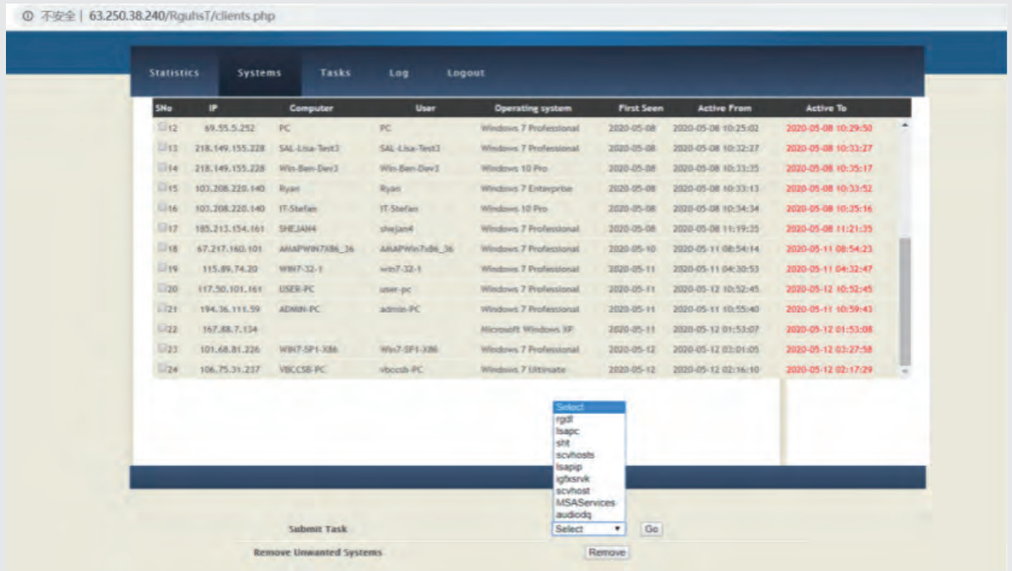
2. 蔓灵花

蔓灵花（Bitter）是一个长期针对中国、巴基斯坦等国家的政府、军工、电力、核等部门发动网络攻击的 APT 团伙，其主要攻击目的为窃取敏感资料，具有较强的政治背景，该组织最早在 2016 年由美国安全公司 Forcepoint 进行了披露，其后，国内各大安全厂商持续对其网络攻击活动进行追踪曝光。

在对中国攻击的涉印 APT 组织中，Bitter 组织是被公开披露的攻击频次最高的一支网军队伍。自披露至今，其不曾间断地对华发起定向攻击，包括频繁的以窃取目标人员的邮箱账号密码为目标的钓鱼攻击和通过植入恶意间谍木马进行窃密活动的钓鱼攻击。2020 年 Bitter 组织对中国攻击目标依然集中在政府、军工、电力、核等单位，除此之外还包括少部分高等院校、军队、运营商等行业目标。

2020 年，Bitter 组织的特马武器的控制端后台因 SQL 注入漏洞曾遭到多次曝光披露。在 2020 年的攻击活动中，Bitter 组织使用的攻击框架以及武器库插件并无明显变化。追踪该组织发现，2020 年 Bitter 组织投递的钓鱼邮件中的攻击载荷主要为自解压 PE 和 MSI 安装包程序两类，其中以 MSI 安装包为主。其使用的网络资产偏向于免费的动态域名，如 netlify.app、000webhostapp.com、herokuapp.com、esy.es 等。在 Bitter 组织的恶意插件托管站点上首次出现了 Mimikatz 局域网密码爬取工具，可见 Bitter 组织亦会进行内网的横向移动来扩大战果。

Bitter 组织的木马主控后台如下：



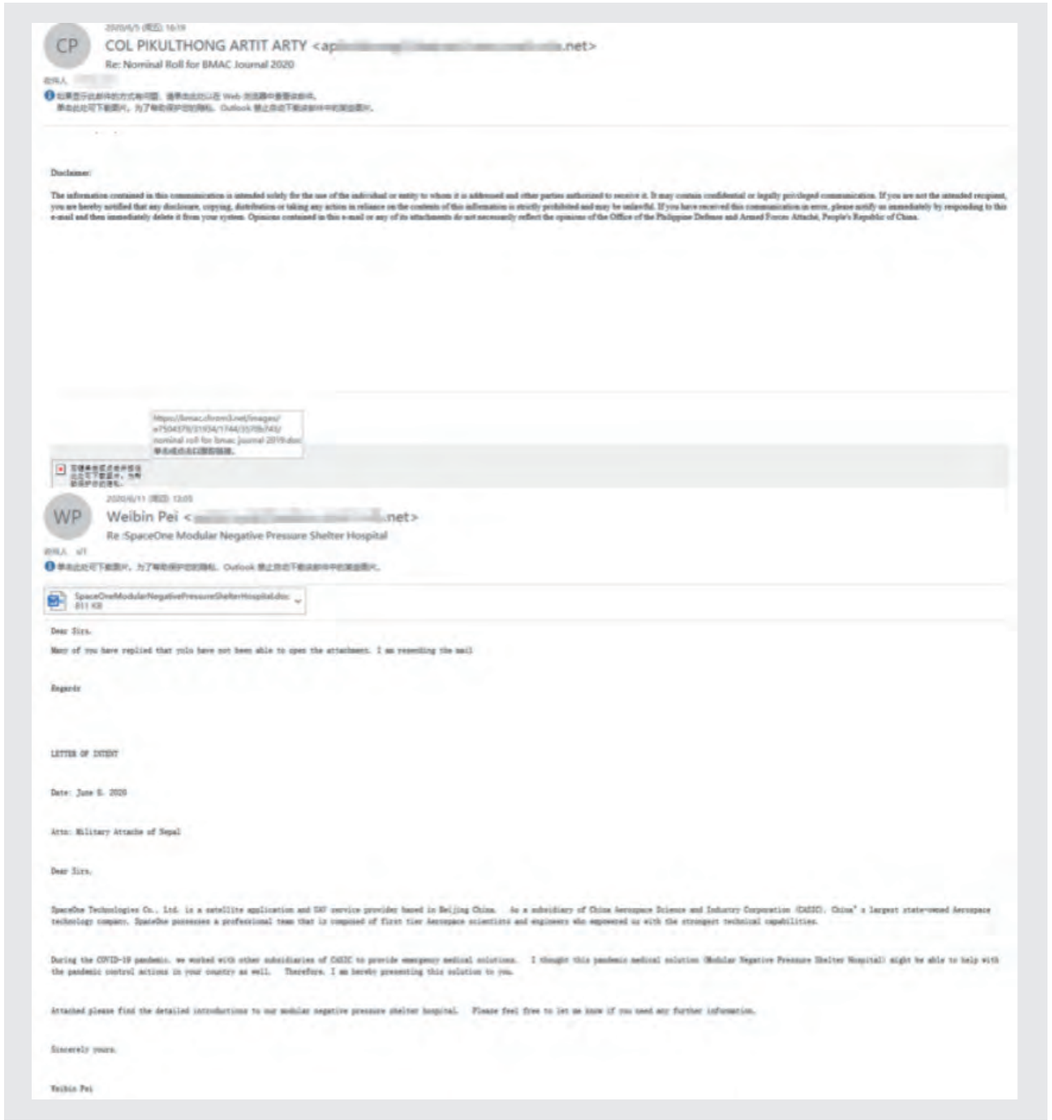
年度代表性攻击事件如下：

3. 响尾蛇

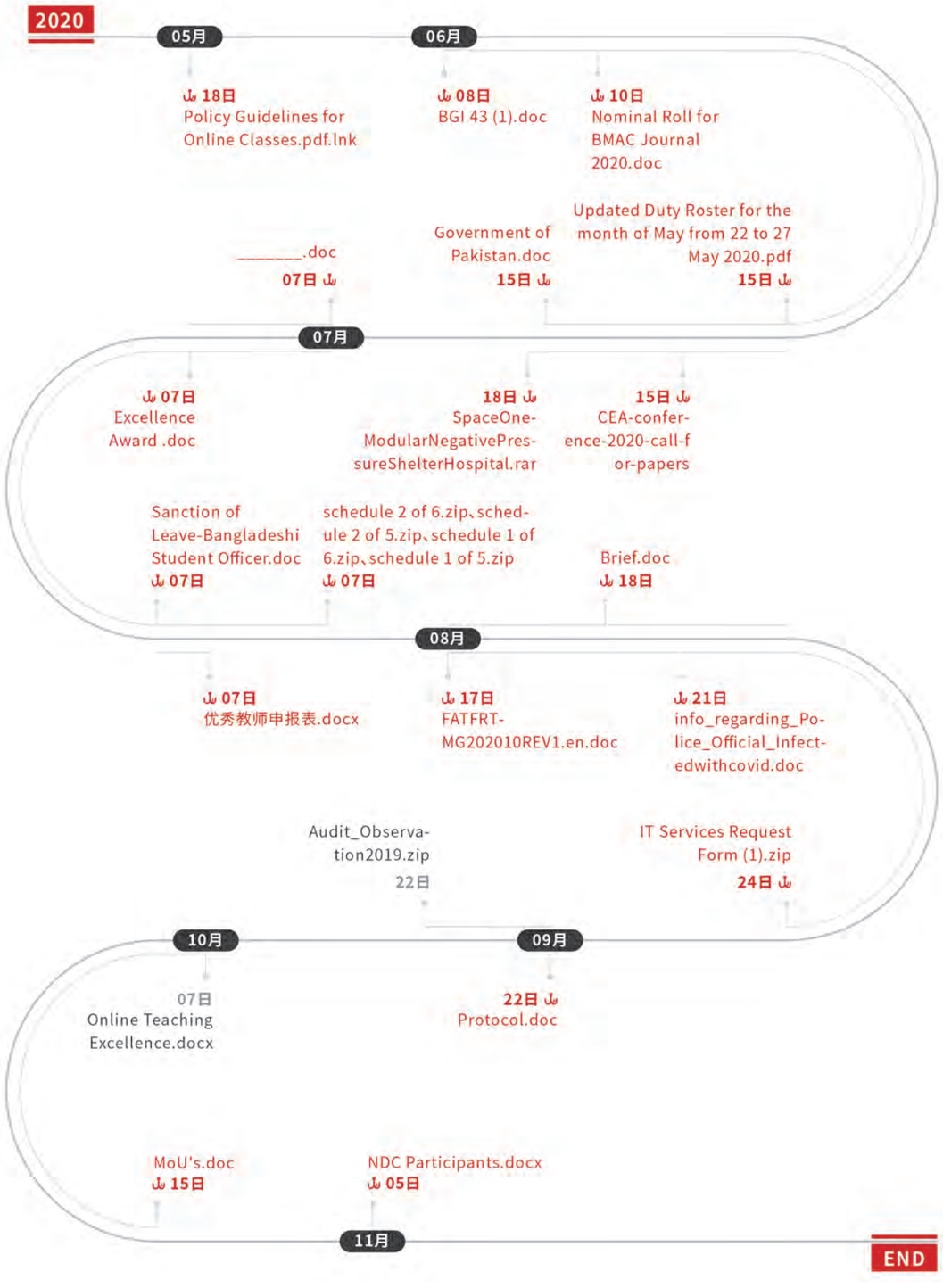
响尾蛇 APT 组织（SideWinder）是一支疑似具有印度政府背景的黑客团伙，最早活跃时间可追溯到 2012 年。其攻击目标主要为中国、巴基斯坦、孟加拉国等国家的军工、外交、科研等相关敏感单位。

响尾蛇 APT 组织自披露以来长期保持活跃状态，其攻击目标以军工单位为主，在过去的 2019 年更是对中国发起了高频次的网络攻击活动。2020 年，微步在线追踪该组织发现，响尾蛇组织投入使用的攻击框架、攻击战术以及特马武器几乎没有变化，除了前期落地的攻击载荷经过一系列新的包装之外，最终均释放相应的白利用组件、通过无文件加载技术内存执行 .Net 框架窃密木马达到情报刺探的攻击目的。值得注意的是，2020 年响尾蛇组织主要攻击目标存在较大变化。除了对巴基斯坦进行频繁攻击之外，该组织还借助新冠肺炎热点事件对中国境内的南亚地区国家驻华使馆发起定向攻击，对华攻击目标主要涉及学术协会、高等院校方向。

部分钓鱼邮件如下：



本年度代表性攻击事件如下：

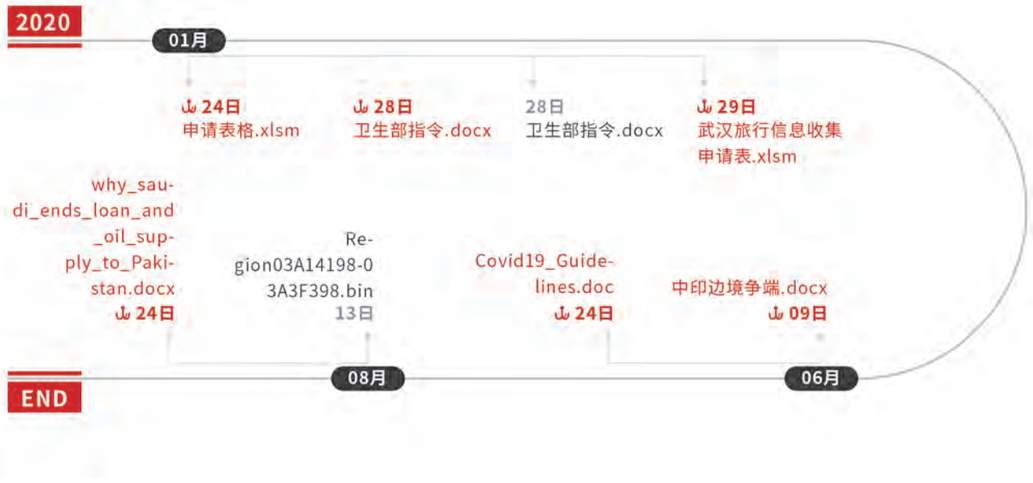


4. 白象

白象 APT 组织，又名“Patchwork”、“摩诃草”、“The Dropping Elephant”，是一个具有印度国家背景的 APT 组织，该组织最早由 Norman 安全公司于 2013 年曝光，主要针对中国、巴基斯坦等亚洲地区国家进行网络间谍活动，以窃取敏感信息为目的，相关攻击活动最早可以追溯到 2009 年 11 月。自 2009 年至今，“白象”组织已经活跃十年有余，从最初的小黑客团伙到如今成为一支极具代表性的国家级网军队伍，其经历了漫长的网络武器资源整合、组织规模扩充、武器库研发投入等过程。当前该组织已经具备多平台攻击能力（覆盖 Windows 和 Android 平台），但是其攻击活动数量明显下降、每次攻击活动都是在特定时政事件背景下发起的精准化网络攻击，体现了出于政治目的的网军攻击特性。

2020 年，白象 APT 组织对中国的攻击活动较少，主要集中在两个特殊的时间节点：第一季度国内疫情紧张时期，6 月至 8 月中印政治关系开始恶化时期。与印度方向的其他 APT 组织相比，白象组织虽然攻击频次较低，但是 nday 漏洞利用能力较强。

年度代表性攻击事件如下：



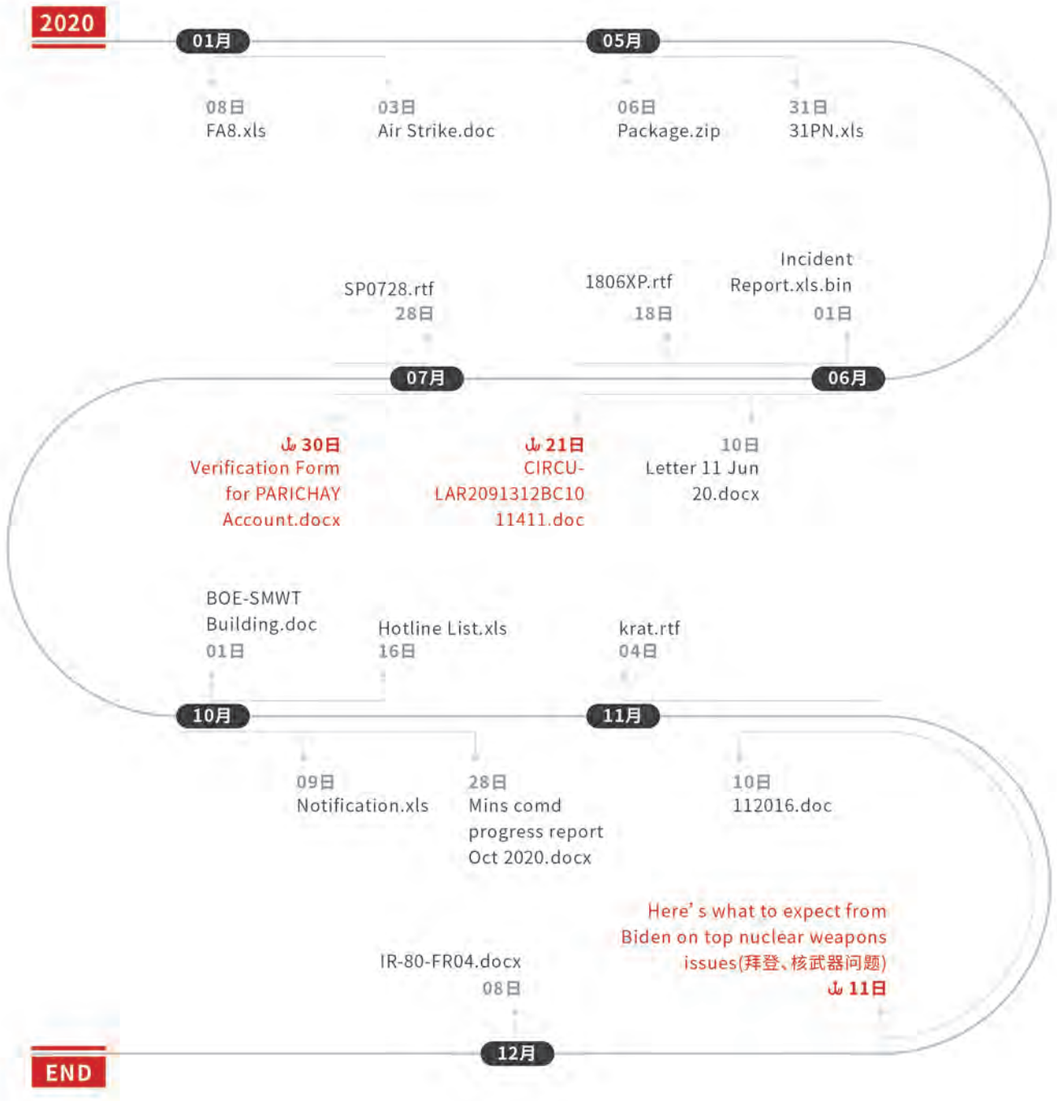
5. 肚脑虫

肚脑虫（Donot）是一个印度背景的 APT 组织，主要针对巴基斯坦等南亚地区国家的政府机构、重点企业等领域进行网络间谍活动，以窃取敏感信息为目的。该组织最早的攻击活动可以追溯到 2016 年上半年，目前该组织的攻击活动依然十分活跃。

肚脑虫 APT 组织具备 PC 端和移动端的攻击能力，移动端攻击频率相对较高，其攻击目标主要为巴基斯坦的政府和军队。

追踪肚脑虫 APT 组织的攻击活动发现，该组织投入使用的攻击框架、最终攻击插件并无明显变化，投入使用的攻击诱饵制作粗糙，并且存在较多疑似测试的攻击样本。根据 2020 年所捕获的攻击样本，肚脑虫组织在攻击活动中使用的下载器存在较大调整，之前简单明了的下载器程序替换成较为复杂的多文件模块。其通过诱饵文档 OLE 技术实现无文件加载组件释放，然后经过内存解密装载运行核心的下载器模块，最终通过与 C2 端交互实现攻击插件下发。

年度代表性攻击事件如下：



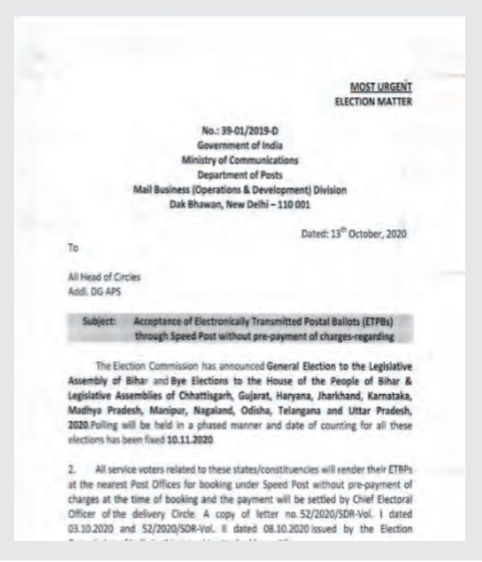
6. 假旗部落

在印巴冲突方面，巴基斯坦地域的 APT 组织活动同样值得我们注意。除了熟知的 Project-M APT 组织外，微步情报局发现一个至少自 2019 年以来针对印度、阿富汗等地区的新 APT 组织，内部将其命名为 FalseFlager，中文名称“假旗部落”。该组织疑似具备巴基斯坦背景，主要针对南亚地区印度、阿富汗等国的军事、政府、金融、教育、科研等行业和机构开展网络间谍活动。

该组织至少具备 Windows 以及 Android 双平台攻击能力。Windows 平台上，该组织长期模仿印度方向的相关 APT 组织攻击手法，木马的使用则结合了开源木马和特马，但相关特马开发程度仍属于初期阶段。使用的插件也多为 goLazagn、SharapLogger 这样的开源工具。

部分攻击流程如下：

某次以 2020 比哈尔立法议会选举活动相关主题，针对印度陆军邮政局（APS）相关政府机构的攻击诱饵如右图：



MOST URGENT
ELECTION MATTER

No.: 39-01/2019-D
Government of India
Ministry of Communications
Department of Posts
Mail Business (Operations & Development) Division
Dak Bhawan, New Delhi – 110 001

Dated: 13th October, 2020

To

All Head of Circles
Addl. DG APS

Subject: Acceptance of Electronically Transmitted Postal Ballots (ETPBs) through Speed Post without pre-payment of charges-regarding

The Election Commission has announced **General Election to the Legislative Assembly of Bihar** and **Bye Elections to the House of the People of Bihar & Legislative Assemblies of Chhattisgarh, Gujarat, Haryana, Jharkhand, Karnataka, Madhya Pradesh, Manipur, Nagaland, Odisha, Telangana and Uttar Pradesh, 2020**.Polling will be held in a phased manner and date of counting for all these elections has been fixed **10.11.2020**.

2. All service voters related to these states/constituencies will render their ETBPs at the nearest Post Offices for booking under Speed Post without pre-payment of charges at the time of booking and the payment will be settled by Chief Electoral Officer of the delivery Circle. A copy of letter no.52/2020/SDR-Vol. I dated 03.10.2020 and 52/2020/SDR-Vol. II dated 08.10.2020 issued by the Election

而在 Android 平台上，攻击者将恶意木马伪装成社交软件进行攻击，该木马具备录音、录屏、SMS、获取图片、获取文档、读取联系人列表以及命令执行等功能。

某次伪装社交软件截图如右图：

东南亚

海莲花，又名 APT32 和 OceanLotus，是具备越南背景、目前东南亚最为活跃的 APT 组织。APT32 至少自 2012 年开始活跃，长期针对中国能源相关行业、海事机构、海域建设部门、科研院所和航运企业等进行网络攻击。此外，“海莲花”的目标还包含全球的政府、军事机构和大型企业，以及本国的媒体、人权和公民社会等相关的组织和个人。

在今年上半年新冠肺炎疫情爆发形势下，“海莲花”借用疫情热点话题内容，频繁攻击中国企业和单位，涉及海事、能源等机构。在下半年，APT32 利用伪造的新闻、论坛等网站，诱导目标受害者下载伪造的“Adobe 插件”后门程序，活动瞄准了越南的人权活动家、老挝和柬埔寨的政府机构、新闻社和其他攻击者感兴趣的企业。

APT32 一直在不断完善和更新攻击手法和攻击工具，在攻击链的“交付”阶段中，攻击者擅长使用水坑攻击、鱼叉式网络钓鱼攻击手法，结合社会工程学诱导受害者进行一系列的后续操作。攻击链“命令和控制”阶段中包含 Denis 特有后门、PhantomLance 特有后门、Cobalt Strike 商业工具等，涉及 Windows、macOS 和 Android 等多个平台。

在涉及 Android 用户受害者的活动中，攻击者创建了 Facebook 账号。冒充成活动家或企业用户来说服受害者从谷歌商店下载 Android 应用程序，而实际上这些应用程序是 APT32 组织所特有的 PhantomLance 木马，具备：收集信息（通讯录、文本信息、通话历史、设备位置和所安装应用）、下载执行文件、上传问题、执行 Shell 命令等功能。

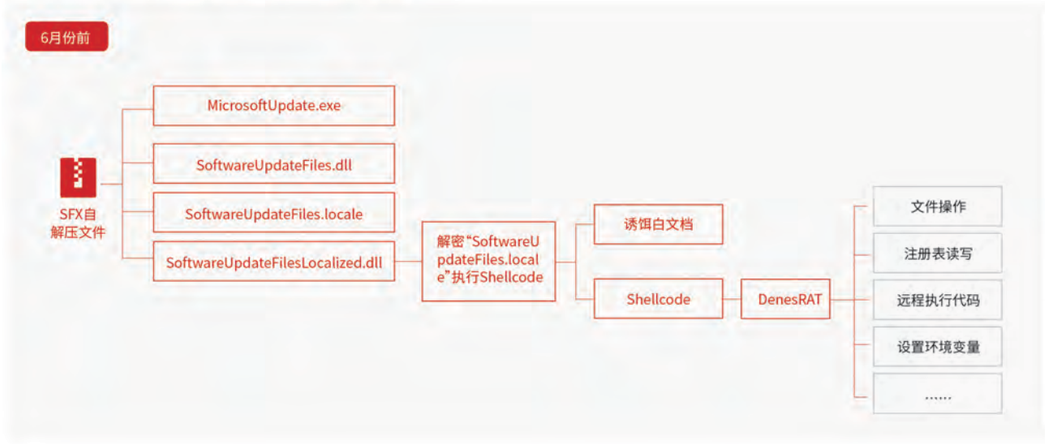
在 macOS 平台上，攻击者会使用伪装为 Microsoft Word 文档的恶意 macOS 应用进行攻击。恶意 macOS 应用在受害者运行后会经过 Shell 脚本执行、后门释放程序执行、后门运行三个阶段，最终释放的后门具备获取配置信息、下载文件、上传文件、执行 Shell 命令等功能。

在 Windows 平台的攻击活动中，攻击者擅长利用白加黑、DLL 体积膨胀、Shellcode 多层加密、花指令等方法躲避杀软检测和对抗沙箱分析。投递的诱饵主要涉及三种，包括：白利用结合压缩包、（SFX）RAR 自解压文件和携带宏代码的 MIME 格式文档。

部分代表性的攻击流程图如下：

诱饵1: Thu moi gap mat bao chi.rar

诱饵2: 36 ASEAN Summit 26 -06 -2020 Conference.doc~ .exe



诱饵3: Report _tiecuoi.doc

综合研究发现，APT32 网络工具武器库储备充分，特有木马外，Mimikatz、Phant0m 等公开工具也在 APT32 的武器库中。APT32 一些常见的攻击特点包含：特马“一机一码”，该特马运行后利用目标计算机的用户名、IP 地址等作为密钥多层解密 Shellcode 后回连 C2 服务器；通常会劫持某些正常程序的 DLL 文件（如：搜狗输入法、360 系列软件的更新程序）用于攻击的持久化。

东亚

1. Lazarus

Lazarus 组织是具有朝鲜背景的大型黑客组织，其攻击活动足迹遍布于世界各地，至少自 2007 年开始活跃，该组织的武器库强大，经常攻击全球范围内政府、媒体、金融、医疗、航空、研究中心等机构，攻击动机以窃取敏感信息和获取经济利益为主。

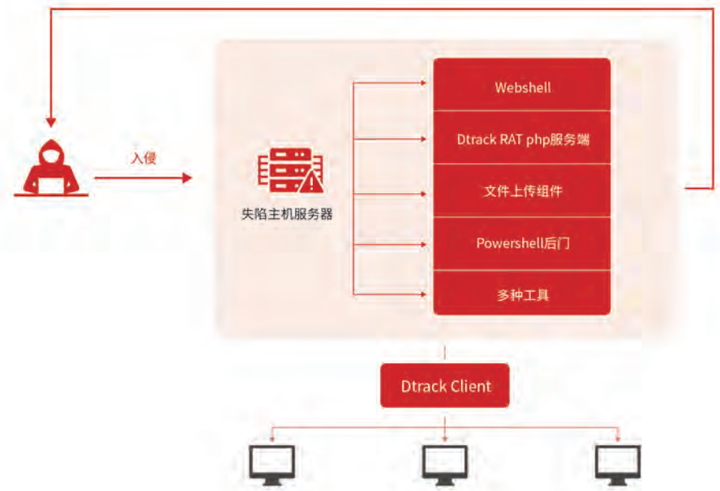
在今年上半年，COVID-19 疫情席卷全球，以此为主题的网络攻击事件骤然增长，其中中国、韩国、意大利等国家成为网络攻击的高风险地区。Lazarus 组织亦将疫情相关主题作为诱饵对韩国进行了定向攻击活动，伪造韩国仁川疾控中心的邮件进行钓鱼攻击，邮件的附件使用了韩国特有的 HWP 文档格式，具有很强的针对性。HWP 文档中包含的恶意 PostScript 脚本会在运行后加载恶意后门模块来进行情报收集活动。

此外，加密货币公司也一直是 Lazarus 组织的目标之一，其攻击的主要目的是获取经济利益，该组织在针对加密货币方面使用的样本包含多平台版本，经常以推广交易软件为名推广带有后门的交易软件，攻击样本在运行后会检查运行环境再释放恶意代码文件，恶意代码运行后会修改配置实现自启动，之后连接 Lazarus 组织控制的失陷主机，接受攻击者的命令并进行下一阶段的攻击活动，对加密货币的用户有针对性，而且比较隐蔽，不易被发现。

在针对航空公司的攻击活动中，Lazarus 冒充波音、麦道和 BAE 等航空公司，先以竞争公司挖角的方式引诱员工，然后在所谓的职位详细信息文档中植入恶意木马，利用社会工程学以 Job Description 为名义向目标发送包含恶意载荷的诱饵文档进行攻击，此外，攻击者还会建立虚假的 LinkedIn 账户，以进一步降低目标警惕性。

在今年下半年，Lazarus 入侵了一批暴露在公网上的服务器，将入侵的服务器作为 C2 服务端，使用名为“Dtrack”的 RAT 工具对数十个国家地区进行了攻击，在攻击活动中，微步在线监测到攻击者窃取了大量医药相关资料，结合该组织以往攻击目标以及当前全球疫情局势，推测 Lazarus 正在全球范围内谋求并窃取 COVID-19 疫苗相关资料。

Lazarus 使用“Dtrack”RAT 工具的攻击流程图如下：



Lazarus 早期主要针对美国、韩国发起带有政治目的的网络攻击，而近几年其攻击目标不断扩大，Lazarus 早已演变成了全球性的 APT 组织。该组织擅长使用钓鱼邮件及社会工程学方案进行攻击，经常批量扫描暴露在公网上的服务器，借助漏洞利用、爆破等方式入侵主机，将失陷站点作为攻击活动中的 C2 服务器，在以往的攻击活动中，Lazarus 为了避免被发现会及时清除活动证据，包括通过删除工具和日志数据来清除其在目标主机上的活动证据。

2. 危险密码

“危险密码”是由微步在线命名的一个至少自 2018 年 3 月起开始活跃的 APT 组织，主要针对中国、美国、日本、欧洲、俄罗斯等地区的加密货币公司发起攻击。

“危险密码”组织在 2020 年初被安全厂商披露后停止活跃了一段时间，7 月份微步情报局监测发现一批针对国内外企业金融交易相关业务的定向攻击活动，经过深度分析后，确认这批攻击活动的幕后攻击者为“危险密码”组织。

“危险密码”组织早期攻击手法主要通过钓鱼邮件投递恶意文件下载链接，诱导收件者从仿冒的谷歌、微软、亚马逊云服务器下载木马压缩文件。解压后的文件包括经过加密的合法 Office 文档以及伪装成密码文本（包括英语、俄语、日语等）的恶意快捷方式文件。

在追踪“危险密码”组织的过程中，发现该组织投递的诱饵在不断迭代更新中。最早的诱饵文件伪装成“PassWord.txt.lnk”，而在最新的一些攻击中通常伪装成 PDF 或者 DOCX 等文档的格式，部分诱饵将白文档存放在谷歌云等云端，部分诱饵则存放在 LNK 文件尾部。

同期，芬兰安全公司 F-Secure 对“危险密码”组织追踪发现，JavaScript 后门在后续会通过一段 C2 下发的 PowerShell 下载最终的二进制木马，木马与卡巴斯基曾披露的 Bluenoroff（Lazarus 组织分支）组织所使用的特马高度相似。这意味着“危险密码”组织与 Bluenoroff 组织存在一定关联，结合其特定的攻击目标和攻击目的，研究人员认为“危险密码”组织疑似为“Lazarus”组织的一个分支。

3. DarkHotel

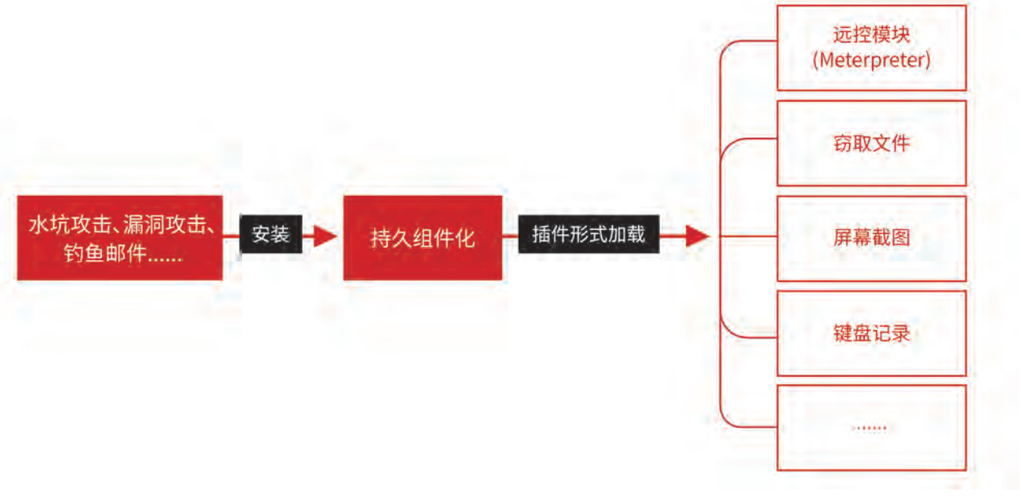
DarkHotel（又名 Dubnium、Nemim、Tapaoux、黑暗酒店等）是一个被认为来自韩国的 APT 组织，具有 0day 攻击的能力，不排除有政府背景，该组织最早在 2014 年被卡巴斯基曝光，最早活动可以追溯到 2007 年，是近年来活跃的 APT 组织之一，其主要目标是入住高端酒店的电子行业、通信行业的企业高管以及有关国家政要人物，攻击入口是酒店 WiFi 网络，当目标接入酒店 WiFi 时便会遭遇攻击，因此得名 DarkHotel，攻击范围遍布中国、朝鲜、印度、日本、俄罗斯等多个国家。

该组织技术实力深厚，在以往的攻击活动中使用劫持 WiFi 投递诱饵、鱼叉式钓鱼邮件、滥用数字签名、白利用，以及感染 U 盘文件达到突破物理隔离等技术手段，另外还会使用多种漏洞进行攻击，比如 CVE-2012-0158、CVE-2017-11882、CVE-2018-8174、CVE-2018-8373 等，其中带有 CVE-2018-8174 和 CVE-2018-8373 的攻击样本被捕捉时还处于 0day 状态，其进一步使用的恶意代码非常复杂，相关功能模块达到数十种，涉及恶意代码模块超过 200 余个，该组织主要针对 Windows 系统进行攻击，非常善于对组件进行伪装，同时释放恶意组件与正常文件，这让目标往往难以察觉背后的猫腻，该组织善于发掘现实中的水坑场所，不管是入侵酒店网络进行恶意软件投送，还是通过钓鱼邮件投送，都展现出 DarkHotel 有着极强的对潜在网络脆弱性的获取和利用能力，无论是整体实力还是威胁等级在现有的 APT 组织中都是属于很高的级别。

在今年 1 月份，DarkHotel 同时利用 IE 浏览器和火狐浏览器两个 0day 漏洞进行复合攻击，漏洞编号为 CVE-2019-17026（火狐浏览器）和 CVE-2020-0674（IE 浏览器），主要攻击目标为我国商贸相关的政府机构，意图长期监控及窃取机密文件。漏洞利用是该组织常用的攻击方式之一，该组织长期关注 PC 漏洞，具有深厚的技术实力。

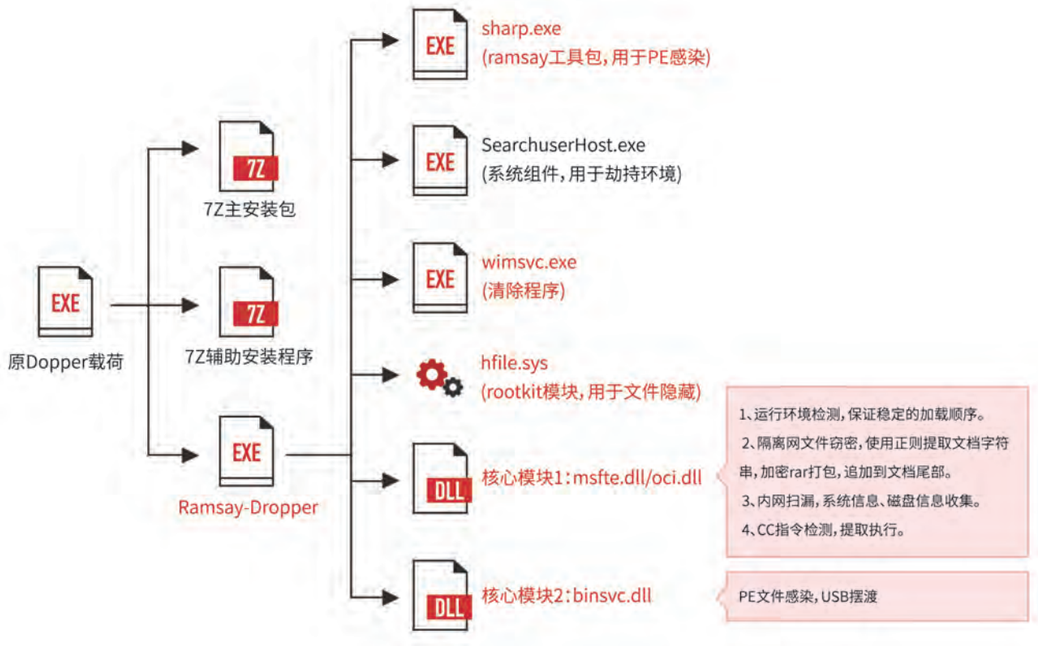
从 2020 年 3 月起，DarkHotel 使用了一个名为“Thinmon”的全新后门框架，该后门可能已经被 DarkHotel 秘密使用了三年之久，包括屏幕截图、文件窃取、键盘记录、远程监控等功能，其插件在计算机中皆以二进制加密的形式存放在临时目录，只有在需要被加载启动时，调度模块才会对其解密并加载，主要用途为对目标进行长期监控和窃取机密文件。

Thinmon 后门框架攻击流程示意图如下：



2020 年 5 月，国外安全机构发现了一款名为 Ramsay 的攻击组件，该组件具备隔离网络攻击能力，经关联分析，该组件为 Darkhotel 组织所有，至今已存在多个迭代版本。Ramsay 组件为携带蠕虫模块的打包器程序，通过 USB 移动存储设备进行互联网主机与隔离网络主机之间的信息摆渡，最终实现内网渗透、文件窃密、恶意模块执行、Shell 执行等功能。

Ramsay 组件攻击流程示意图如下：



在今年 3 月份的疫情期间，该组织利用深信服 VPN 服务器 0day 漏洞入侵了 200 多台 VPN 服务器，其中一百多台位于政府机构的网络中，攻击者入侵服务器之后，将客户端升级组件替换为后门程序，并且使用了伪装成深信服数字签名的木马进行攻击。

DarkHotel APT 组织是近年来最活跃的 APT 组织之一，经常使用 0day 漏洞对目标进行攻击，技术积累深厚，该组织对企业所使用的内网安全软件和办公软件进行了深入的研究，是目前针对中国境内进行攻击的 APT 组织之一，攻击者惯用精心伪造的电子邮件，通过附件投递攻击文档，攻击文档大多利用较新的系统高危漏洞定制。最终受害电脑会被安装特种木马，通过木马插件实现键盘记录、敏感数据文件上传、收集主机进程信息操作系统信息，以及实现远程控制，其攻击目标不仅包括相关企业的高层，还针对特定的行业进行攻击，以窃取机密资料，因此尤其要引起相关企业和相关企业的高层管理人员的注意。

4. Kimsuky

Kimsuky 组织是具有朝鲜背景的 APT 组织，至少从 2012 年开始活跃，据悉其背后由朝鲜政府提供支持，该组织长期针对韩国政府、新闻等机构进行攻击活动，在近几年，其目标已经扩大到包括美国、俄罗斯和欧洲各国在内的多个国家。

Kimsuky 经常向目标发送包含恶意载荷的诱饵文档进行钓鱼邮件攻击，例如伪装成简历、更新程序、图片等，在今年该组织保持高度活跃，进行了以“新型冠状病毒”为主题的攻击活动、冒充韩国青瓦台以“邮箱安全检查”的名义进行钓鱼邮件攻击以及各种伪装简历的攻击活动等等，攻击目标通常涵盖政府、新闻、医疗、金融等机构，此外，Kimsuky 对热点事件特别是政府相关事件保持很高的关注度，在今年 11 月美国大选期间，该组织就曾以“美国大选预测”为主题进行攻击活动以收集情报。

Kimsuky 以其复杂的基础设施架构而广为人知，这些基础设施包括使用动态域名、自由注册域名、被攻陷的域名主机以及由该组织注册的私有域名等。该组织经常使用的一款名为“BabyShark”的恶意组件是基于可视化基本脚本（VBS）的恶意软件，该组件可从攻击者控制的服务器上远程下载和执行 HTML 应用程序 (HTA) 文件，然后下载、解码和执行“BabyShark”的 VBS 脚本文件，该脚本通常通过创建注册表启动项或任务计划来维持持久化，之后收集主机系统信息将其发送到 C2 服务器等待进一步的命令。

多年来，Kimsuky 一直在其攻击活动中使用一系列恶意软件，其中包括一个今年启用的称为 "KGH_SPY" 的新恶意软件套件，包含多个用作间谍软件的模块。"KGH_SPY" 是一套模块化间谍工具，为威胁参与者提供侦察、键盘记录、信息窃取和后门功能，其通常伪装成合法的 Mocrisoft Windows 工具，包括但不局限于以下功能：

- 将收集到的主机信息发送到 C2 服务器
- 使用 Windows 开机启动机制实现持久化
- 键盘记录器
- 查看目录及文件列表
- 从 C2 服务器下载分发恶意模块
- 通过 cmd 或 Powershell 执行任意命令
- 从浏览器、Windows 凭据管理器、WINSCP 和邮件客户端窃取隐私数据

此外，Kimsuky 所使用的名为 "CSPY" 的下载器是一种旨在逃避分析和下载分发恶意模块的工具，"CSPY" 包含强大的规避技术，并且恶意软件在继续下载恶意载荷之前不会在虚拟机或分析工具的环境中运行。"CSPY" 通过搜索特定的虚拟机相关加载模块、进程 PEB 结构、各种文件路径、注册表项和内存等，进行一些列检查，以确定它是否在虚拟机中运行或是被调试，这突出了攻击者为逃避监测而付出的努力，完成反分析检查后，加载程序开始准备受感染的环境以下载分发其他恶意组件，为了避免引起受害者的怀疑，"CSPY" 下载器利用一种已知的 UAC 旁路技术，该技术使用 SilentCleanup 任务来执行具有提升权限的二进制文件，最终，"CSPY" 会进行自我删除。

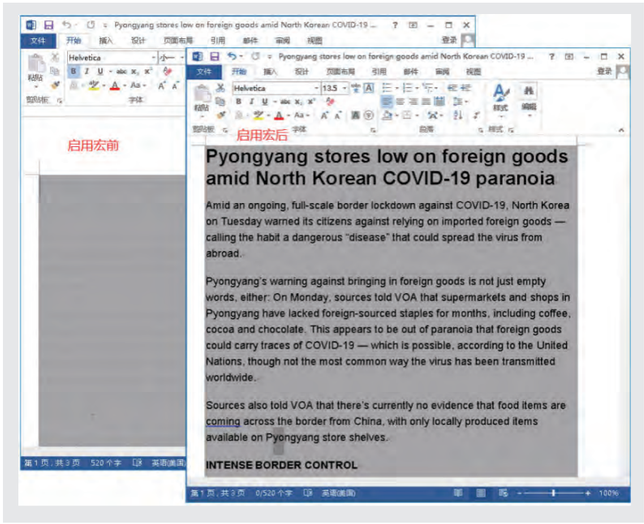
Kimsuky 善于使用各种反取证和反分析技术，包括将恶意软件样本的编译时间修改到过去年份、代码模糊化处理、反虚拟机和反调试技术等等，该组织在攻击过程中体现出轻量化、多阶段脚本载荷的特点，近些年，Kimsuky 不断开发新的工具以及旧工具的变种，积极参与全球情报收集活动，经常通过批量扫描入侵韩国以及其他国家地区站点服务器作为其 C2 服务器，这与具有相同半岛背景的 Lazarus 组织有一定的相似度。

5. Konni

Konni 组织是朝鲜半岛地区最具代表性的 APT 组织之一，自 2014 年以来一直持续活动，据悉其背后同样由朝鲜政府提供支持，该组织经常利用鱼叉式网络钓鱼的攻击手法，使用与朝鲜相关的内容或当前社会热点事件来进行攻击活动，其主要目标为韩国政治组织，以及俄罗斯、日本、越南、中国等地区。

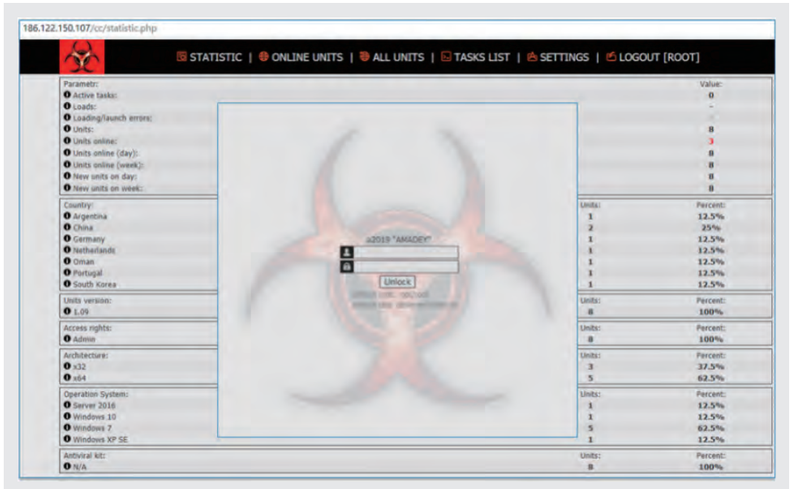
Konni 组织经常向目标发送带有恶意宏的诱饵文档，并且将文字颜色设置为难以阅读的颜色以诱导用户启用宏，该组织善于使用朝鲜相关热点话题进行攻击活动，且极具针对性。

某次以朝鲜疫情物资为主题的诱饵文档如下：



在文档携带的恶意宏中，通常从攻击者事先入侵的失陷服务器中下载名为“Amadey”的家族木马，该木马通过 Web 方式管理，攻击者可利用该木马模块从服务器获取下载链接，进行下一步恶意模块的分发，Konni 组织经常使用此家族木马进行攻击活动。

Amadey 家族木马服务端截图：



使用诱饵文档搭配“Amadey”家族木马进行攻击是 Konni 组织惯用的攻击手法之一，在今年的多起攻击活动中，均发现了类似的“Amadey”木马家族组件，从其攻击目标以及攻击手法来看，与相同背景的半岛地区 APT 组织 Kimsuky 组织或有关联。

Konni 组织通常以对朝鲜事务感兴趣的机构或个人作为目标进行间谍活动，在以往的攻击活动中，该组织主要使用鱼叉钓鱼邮件进行攻击，之后使用包含恶意宏的诱饵文档部署恶意组件用于高度针对性的攻击，其使用的木马可以记录键盘、窃取文件、屏幕截图、收集目标主机信息、窃取浏览器隐私信息以及执行任意代码等。Konni 组织的攻击样本由于不断演变而能够逃避部分监测，可以预见的是，在未来的时间里 Konni 会继续开发其新的工具及变种，以更好的逃避检测。

6. 绿斑

“绿斑”组织是具备台湾地区政治背景且长期针对大陆境内目标的 APT 组织。根据微步在线监测情况发现，其网络攻击活动涉及的行业包括政府、国防军工、航空航天、国家智库、医疗疫苗、高新科研、能源、贸易等领域。在涉及到的攻击目标中基本事关国家安全、稳健发展的职能或研究单位 / 部门，具备极高的国家战略价值。

2020 年 2 月，" 绿斑 " 以新型肺炎相关的 " 疫情防控日报表 "、" 社会维稳 " 和 " 献药方 " 等主题为诱饵，利用仿冒 QQ 和 163 邮箱的域名针对中国大陆政府部门和医疗机构等目标进行攻击，旨在窃取邮箱账密和进行情报收集；2020 年 3 月至 10 月，" 绿斑 " 持续通过相似的手法对大陆的航天航空、军民融合、军工装备企业、军转干部、高端产业、高新科研院校等关联单位和个人发起钓鱼攻击；2020 年 11 月，" 绿斑 " 使用“军工、国防装备配套需求信息发布平台 .rar”、“2021 年度省列高技术产业园项目重大项目申请”、“组织开展退役军人思想教育活动”等主题诱饵文档针对境内军工科研单位、政府发展规划部门展开攻击。

在相关的攻击中，" 绿斑 " 会根据攻击目标定位的精准度、对象需求和切合度等评估投放钓鱼内容以及采集情报类型。如果目标属于高精准度的高价值攻击目标，" 绿斑 " 会在钓鱼邮件里面直接投放附带情报窃取类型的木马附件，诱使攻击目标触发下载后门木马，通过后门木马采集并窃取攻击目标设备的指定文件类型的情报数据。

“绿斑”经过长期的工具优化，其使用的攻击工具已经具备适合不同环境的 PE 窃密木马和 lnk&vbs&ps1 结合窃密脚本套件。

某次攻击流程如下：

1.反向回连文件服务器：https://*.*.81.176/；
2.调用systeminfo.exe获取系统配置信息、系统进程名称、桌面文档列表、用户临时目录列表等信息；
3.将采集到的系统配置信息压缩回传到文件服务器：https://*.*.81.176/upload/%yyyyMMddhhmmss%_-threeswordsmen/start.log；
4.枚举特定目录下的特定格式文件，并压缩回传至FTP服务器，目录包含Windows、Users、Program Files、Program-Data、MSOCache、PerfLogs、System Volume、Documents and Settings、Recovery、Boot等，文件格式包含.doc、.docx、.pdf、.ppt、.pptx、.xls、.xlsx、.ps1、.cpp、.eml、.js、.html、.cs等；
5.循环获取appdata\Microsoft\Windows\Recent\目录数据，并使用RSA算法加密回传FTP服务器。

东欧

1. Gamaredon

隶属于俄罗斯安全情报部门的 APT 组织 Gamaredon 近年来一直针对乌克兰政府高层、外交、国土安全、法务、军事武装、东部克里米亚地区等部门发起定向攻击，其存在明显的军事和政治攻击意图。

微步情报局根据对该团伙已有的网络资产监测发现，Gamaredon 今年持续通过各种诱饵主题攻击乌克兰司法、国土安全、军事武装、政府、外交、医疗等部门。该组织在 6 月份，还延伸恶意 lnk 方式替换模板注入诱饵文档方式进行植入后门木马。目前已经发现该组织利用该手法以“根据《乌克兰刑法》第 368 条第 3 款涉嫌犯罪的通知”、“关于经济安全局副局长勒索贿赂的事实”、“关于勒索事实”、“请求访问公共信息的问题列表”、“在打击国际恐怖主义的斗争中识别和防止威胁的实际措施”等议题疑似向乌克兰的军事、法务、外交等部门展开攻击。经过关联资产信息分析判断，该团伙在 2020 年 2 月前后测试 lnk 类型诱饵，并于 6 月开始投递此类诱饵展开攻击。在此之前，该组织主要以投递模板注入类的诱饵展开攻击。

Gamaredon 与 APT28、Turla、Sandworm 等组织 / 团伙相比攻击手法相对简单，但该组织背后的攻击者极为勤劳，投递的诱饵数量较为庞大。钓鱼邮件中的诱饵从一开始的自解压释放 VBS 后门木马，到模板注入文档释放 VBS 后门木马，再到近期投递的 LNK 木马。从攻击过程使用的手法木马等来看，Gamaredon 一直在原有的技术基础上为攻击的隐蔽性做优化，以及为攻击目的需求做工具完善。

2. APT28

“奇幻熊”，又名 APT-28，是俄罗斯背景的高级攻击黑客组织。长期针对欧洲外交部，美国研究机构、金融机构、乌克兰政府、哈萨克斯坦政府、能源机构、荷兰政府、国际奥林匹克委员会、波兰军事武装、阿塞拜疆政治领袖、中国研究机构等国家政府 / 组织 / 行业进行攻击。

2020 年 5 月，APT28 组织使用了波兰的弗罗茨瓦夫市所属军事预防医学中心近期公开发布的一条军事公告做诱饵文件，公告内容涉及波兰军队卫生官员就新冠疫情对波兰边境军队活动的指示，诱饵文件下载附带释放 APT28 的 Zebrocy 后门木马的组件。因此，初步判断本次攻击是 APT28 组织利用新冠疫情议题对波兰的军事目标展开攻击。在此后的 6 月和 7 月都监测发现有 APT28 组织利用 Zebrocy 木马进行攻击的活动痕迹。

2020 年 8 月上旬，在有关国际情报平台上关联采集到疑似攻击阿塞拜疆的样本，原始名称为 "Course 5 - 16 October 2020（译：（某领导人）2020 年 10 月 5 日至 16 日行程）"。从使用木马功能、手法角度上分析，与 5 月份疑似攻击波兰目标使用的木马相似度极大。结合 2020 年 7 月 15 日阿塞拜疆将军在亚美尼亚和阿塞拜疆之间的边境冲突中丧生，中亚局势骤然升温。而后，俄罗斯 7 月 17 日表示，准备对亚美尼亚与阿塞拜疆之间升级的边境争端进行调解判断。猜测本次 APT28 攻击对象可能是军事、政府高层或党派领袖。当然，从提交样本关联线索分析，被攻击者可能是一名主持人、党派领袖或者政治家。因此，也可以将此次的攻击活动定性为疑似针对阿塞拜疆国内知名人士、党派领袖以及政治家进行定向攻击的 APT 事件。

3. Turla

Turla，也称为 Snake 或 Uroburos，是一个使用俄语的网络间谍组织，该组织至少在 2007 年成立，直到 2014 年被卡巴斯基所发现，被怀疑拥有俄罗斯政府背景。攻击目标主要为政府、使馆、军事、研究和教育组织等单位。主要受害者在西方各大国，但在其他地区例如亚洲、中东等地也有发现该组织的攻击痕迹。今年 Turla 组织攻击集中在欧洲国家的政府、外交部和军事等单位。

2020 年 3 月，发现亚美尼亚政府相关网站被侵入用于水坑攻击，其中包括：亚美尼亚驻俄罗斯大使馆领事处、Artsakh 共和国自然保护和自然资源部、亚美尼亚国际

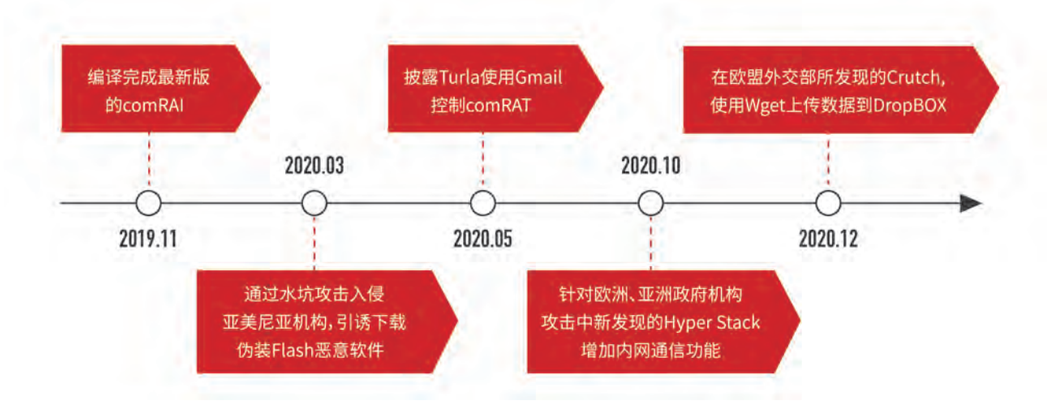
和安全事务研究所、亚美尼亚存款担保基金。有迹象表明这些网站在 19 年初就已经遭到了入侵。Turla 通过向网页中嵌入混淆后的恶意 JavaScript 代码，引诱用户下载恶意的 Flash 安装程序，在这次活动中没有任何的浏览器漏洞等利用技术出现，仅依赖于社会工程学。

5 月，ESET 安全研究员发现 Turla 组织通过 Gmail 来控制 ComRAT 后门，最新的 ComRAT 在 2019 年 11 月编译完成，有证据表明该恶意软件直到 2020 年也依然被使用。通过 Powershell 或者其他 Turla 后门程序安装在受害主机中，整个恶意软件包括注入到 explorer.exe 的核心代码、一个通信 DLL 模块、一个虚拟的 FAT16 文件系统，其中包含了配置和日志文件。

10 月，在最近一次针对欧洲、亚洲政府的攻击活动中，Turla 使用了具有重大更新后的工具包，其中包括 HyperStack，Carbon 和 Kazur 后门三者。其中更新的内容包括：通过创建用于远程通信的管道等可以对旧版本恶意软件进行更新，使用合法的公开页面来接受加密的指令及 HTTP 基础结构，使用 ComRAT 和 Zebrocy 后门来执行各种恶意操作。

Turla 组织擅长使用一些新颖的方式来隐藏自己的 C2 地址。15 年，Turla 组织使用卫星来隐藏自己的 C2 地址。17 年使用了布兰妮·斯皮尔斯（Britney Spears）官方 Instagram 帐户上一张照片的评论来下发指令。20 年新发现的 ComRAT 后门继续使用 Gmail 来与受害主机进行通信。在最新捕获的样本中，Turla 组织的 Hyper Stack 后门更新添加了与内网通信的功能，将一样本作为代理，与内网中没有互联网连接的计算机建立通信。后门使用命名管道和 IPC 会话进行横向传播。12 月新发现 Crutch 后门 v4 版本，依然使用 DropBox 接受窃取到的数据，v3 版本中所使用的为 DropBox API 进行上传，更新后的 v4 版本则使用 Windows 版本的 Wget 将数据上传到 Dropbox。

Turla 组织仍在积极开发自定义和更加复杂的网络军火武器，通过各种方式提高隐蔽性，以便在目标受害者网络中长期保持持久性。



4. WellMess

WellMess 组织至少从 2017 年 12 月开始网络间谍活动，最早由日本安全研究机构披露。7 月 16 日，美国网络安全和基础设施安全局（CISA）、英国国家网络安全中心（NCSC）、加拿大通信安全机构（CSE）和美国国家安全局（NSA）发布了一份联合报告，称 APT29 组织使用 WellMess 系列工具针对美国、英国和加拿大的新冠病毒研究和疫苗研发相关机构发动攻击。

除针对国外的一些攻击外，微步在线在 4 月份曾观察到该组织使用深信服的 SangFo VPN 漏洞针对国内涉及新冠病毒的研究所、疫苗研发企业发起攻击活动，关联到的 C2 服务器涉及国内多个 IP。

WellMess 组织使用的后门包括“WellMess”和“WellMail”，由 Go 语言和 .Net 所开发，具备跨平台的能力。WellMess 系列工具使用 HTTP 和 HTTPS 的方式回传数据，其中数据部分会存放在 Cookie 和 Post 包中，采用非标准 Base64、RC6、RSA 等方式加密。

根据微步在线分析人员的研究，WellMess 恶意软件直接回连的 C2 服务器提供的是加密数据中转服务，具备下发数据（命令数据）和回传数据的功能，这种 C2 服务器部署方式可以隐藏真正的主控服务器，增加分析人员取证分析的困难。

中东

中东地区局势复杂，造成复杂局势原因众多，例如历史遗留、宗教信仰、地域政治以及与西方国家干涉等因素。受今年美国启动伊朗核协议回弹机制恢复对伊朗制裁，以及伊拉克准军事组织指挥官阿布·马赫迪·穆罕迪斯和伊朗伊斯兰革命卫队特种部队“圣城旅”高级军官卡西姆·索莱马尼少将被害等重大事件影响，该地域政治军事冲突愈演愈烈。

回归到网络空间战争中，该地区 APT 组织同样错综复杂且活跃度高。受局势影响，该地域的攻击活动也充满政治目的。其中典型 APT 组织包括 MuddyWater、APT34、APT35、APT-C-23、COBALT DICKENS、APT39、Rampant Kitten、MoleRats 等，部分相关 APT 组织在今年更新了他们的 TTPS，例如 Oilrig(APT34) 在今年针对中东电信组织攻击活动中使用了其武器库中更新后的 RDAT，使用基于电子邮件的 C2 通信管道。MoleRats 使用新后门 SharpStage 和 DropBook，新后门使用合法云服务进行通信和威胁活动。双尾蝎 (APT-C-23) 在其双平台攻击武器库中做了进一步更新。并且中东地区部分 APT 组织朝鲜化，将勒索软件加入了其武器库中，例如 MuddyWater 组织使用 Thanos 勒索软件进行破坏性攻击，Fox Kitten 则使用 Pay2Key 勒索软件攻击。

从受害者范围来看，中东地域大部分 APT 组织在目标选取上依旧保持着以往的习惯，例如 COBALT DICKENS 攻击目标依旧为教育行业，比较值得注意的是，该组织今年使用的部分基础设施则在伊朗，这项举动可能是为了躲避相关执法机构调查。部分 APT 组织在攻击方向同样存在重合部分，例如今年 9 月，美国财政部外国资产控制办公室（OFAC）对伊朗网络威胁组织 Chafer（APT39）实施了制裁，认为其长期监视持有不同政见者以及伊朗邻国学术和电信行业。这与 Rampant Kitten APT 组织攻击目标一致，Rampant Kitten 同样长期针对伊朗侨民和不同政见者。同月被美国政府起诉的三名疑似 APT33 的伊朗成员攻击航空航天行业，窃取商业信息和个人数据。而今年 5 月份 MuddyWater 同样被披露利用 LinkedIn 社交媒体平台伪装 HR 人员对航空航天行业进行攻击，诱导受害者下载恶意诱饵文件。

在众多中东 APT 组织活动中，其中 APT35、MuddyWater 和双尾蝎 APT 组织的攻击活动在攻击目标、攻击手法以及活跃度等方面较为突出。

1. APT35

Phosphorus(又名 APT35，Charming Kitten，Ajax Security) APT 组织疑似来自伊朗地区，与伊朗国家和情报部门疑似关系密切，于 2014 年首次被披露，该组织擅长利用社交媒体进行网络间谍活动，主要针对在美国，英国、中东和欧洲国家的私人或者政府机构、智囊团、学术界研究人员和不同政见者。

该组织在今年活动也异常频繁，同时攻击目标进一步扩大，增加了他们目标清单，包括了 COVID-19 相关的组织，例如 WHO。和以往一样，该组织的活动有较强的政治目的，在去年的活动中，该组织曾经试图对美国大选相关政府官员进行攻击，同样在今年攻击活动中，该组织并未放弃针对大选的攻击，一直试图获取美国总统大选有关的个人工作账户。除此以外，在今年举行的慕尼黑安全会议和沙特阿拉伯的 Think20(T20) 峰会，也发现该组织攻击活动，攻击人员通过以缓解 COVID-19 感染途径为诱饵发送远程会议邀请钓鱼邮件给可能参会人员，受害者包括前政府官员，政策专家，学者和非政府组织的领导者。

在今年的活动中，该组织的 TTPs 也发生了改变。在七月的活动中，攻击人员通过伪装德国记者以电子邮件或者 WhatsApp 消息诱使受害者打开恶意链接，为了获取受害者信任，攻击者还伪造了 LinkedIn 个人资料，并且使用了合法的德国电话号码。这是首次发现该组织使用 WhatsApp 和 LinkedIn 加入到攻击活动中，同时还攻击人员试图像受害者发送恶意 ZIP 文件。

除攻击活动外，今年 5 月 IRIS(IBM 威胁情报部门) 发现一台属于该组织的 VPS 服务器上存放者多达 40G 的视频证据，该服务器托管着 2020 年初活动中使用的多个恶意域名，在相关视频中演示了该组织利用盗取的凭证数据进行相关平台登录，进一步收集各种数据，以及修改账户安全设置。其中的一些视频显示该组织已经成功袭击美国海军和希腊海军相关受害者，并从两个目标处收集了大量信息。

部分窃取数据快照如下图：

Name	Size	Type	Modified
[redacted]@gmail.com	88.1 MB	Folder	10 May 2020
[redacted]ages.plusgoogle.com	1.5 MB	Folder	12 May 2020
[redacted]gmail.com	89.8 MB	Folder	12 May 2020
Dropbox [redacted]@gmail.com)	31.7 MB	Folder	10 May 2020
[redacted]tax Douments	127.5 kB	Folder	10 May 2020
[redacted]ppages.plusgoogle.com	7.7 MB	Folder	10 May 2020
[redacted]gmail.com	40.9 GB	Folder	10 May 2020

2. MuddyWater

MuddyWater APT 组织又名 Static Kitten、Seedworm，自 2017 年开始活跃，主要针对中东、中亚地区的政府、军事、电信、教育及能源企业进行攻击，同时也会对周边地区和其他国家的目标进行攻击，如印度和美国等，被认为服务于伊朗伊斯兰革命卫队 (IRGC)。该组织通常使用带有宏代码的 office 文档进行鱼叉式钓鱼攻击，恶意文档往往采用模糊处理，引诱受害者启动恶意宏释放后续多阶段恶意样本执行。

该组织在去年被曝光使用的 MuddyC3 后门工具，而在今年活动中更新其 TTPS。从年初被披露的 ForeLord 后门到年中活动中被发现的 MoriAgent 后门以及最新活动中使用的 PowGoop，该组织正在积极的更新其武器库。

受疫情影响，在今年的很多 APT 活动中都发现使用 Covid-19 相关话题进行攻击，MuddyWater 在今年年中的活动中同样发现使用 Covid-19 话题诱饵进行攻击，将诱饵文件和恶意后门通过 NSIS 打包成带有文档图标的可执行程序进行投递，且在此次活动中使用的后门是被命名为 MoriAgent，MoriAgent 被认为是其第三代攻击武器 (第一代 PowerStats，第二代 DNS 隧道木马)。

而在针对中东与北非的国有组织攻击活动的“流沙行动”中，投递恶意诱饵文档或者利用 CVE-2020-0688 Exchange 服务器远程执行漏洞部署 PowGoop 有效负载，并在以色列受害者机器发现后续行为会释放 Thanos 勒索病毒。基于 PowGoop 与 MoriAgent 的代码相似性，“流沙行动”被归因于 Muddywater。将勒索病毒纳入武器库也是今年中东相关 APT 组织一个较大的变化。

某次攻击中的诱饵文件如下：

3. APT-C-23

双尾蝎 (APT-C-23) 又名 Desert Falcons、Arid Viper，是一个针对巴勒斯坦和以色列两个中东国家教育、军事、政府等领域进行有组织、有计划、有针对性的长时间不间断攻击的 APT 组织，于 2017 年首次被披露，疑似来自中东地区。该组织具有针对 Windows 和 Android 双平台攻击能力，武器库包含定制的 Windows 恶意软件 (Kasperagent，Micropsia) 和 Android 恶意软件 (Vamp，GnatSpy)，使用鱼叉、水坑、社工等手段针对特定目标人群进行攻击。

该组织在今年的活动也较为频繁，同时也在不断改进武器库。针对移动端的活动和以往大致一致，主要通过钓鱼网站或者社工的手法诱导受害者下载恶意 APK，而这些 APK 大多伪装成社交媒体 app 软件。例如年初就被色列国防军 (IDF) 官方社交媒体披露伪装成社交媒体软件利用社会工程学引诱以色列国防士兵下载安装恶意 APK。

而在观察到后续的攻击活动中，该组织 Android 端后门虽然继续伪装成社交媒体软件但也对后门做了部分更新，例如对功能指令进行加密修改，增加读取通话记录、屏幕录像、读取来自社交媒体软件的通知文本 (WhatsApp、Facebook、TeleGram 等) 和关闭不同 Android 设备上内置安全性应用程序通知（Samsung、小米、华为等）等间谍功能。

在 Windows 平台上，该组织通过投递伪装成文档文件、视频文件以及图片文件等 EXE 可执行样本，点击 EXE 执行后则会释放出对应的诱饵文件，从而迷惑受害者。后门使用则以 VC 后门和 Delphi 后门居多。微步情报局也披露该组织今年部分活动，并且在后续跟踪过程中发现相同资产下存在 Pacal 后门，这也是观察到该组织首次使用 Pacal 编写木马后门。

05 总结

本报告以微步在线的视角展示了 2020 年期间活跃 APT 组织攻击活动对网络安全、信息安全和国家安全带来影响，我国作为 APT 攻击的主要受害者，在发现、防御、响应安全体系建设方面仍有很长的路要走，微步在线也将继续关注对 APT 组织和事件的跟进研究，为共筑网络安全防线贡献绵薄之力。

06

附录

团队简介
微步情报局
Team Introduction

微步情报局，即微步在线研究响应团队，负责微步在线安全分析与安全服务业务，主要研究内容包括威胁情报自动化研发、高级 APT 组织 & 黑产研究与追踪、恶意代码与自动化分析技术、重大事件应急响应等。

微步情报局由精通木马分析与取证技术、Web 攻击技术、溯源技术、大数据、AI 等安全技术的资深专家组成，并通过自动化情报生产系统、云沙箱、黑客画像系统、威胁狩猎系统、追踪溯源系统、威胁感知系统、大数据关联知识图谱等自主研发的系统，对微步在线每天新增的百万级样本文件、千万级 URL、PDNS、Whois 数据进行实时的自动化分析、同源分析及大数据关联分析。微步情报局自设立以来，累计率先发现了包括数十个境外高级 APT 组织针对我国关键基础设施和金融、能源、政府、高科技等行业的定向攻击行动，协助数百家各个行业头部客户处置了肆虐全球的 WannaCry 勒索事件、BlackTech 定向攻击我国证券和高科技事件、海莲花长期定向攻击我国海事 / 高科技 / 金融的攻击活动、OldFox 定向攻击全国上百家手机行业相关企业的事件。

威胁感知平台

Threat Detection Platform - TDP ®

产品概览：

微步在线威胁感知平台 (以下简称 TDP®) 通过情报驱动的威胁感知内核与紧贴甲方视角的风险分析模块，支持对双向全流量进行深度分析，能够全面发现网络威胁，实时判定成功攻击，精准定位失陷主机，并提供基于终端和流量的处置闭环能力；同时，通过非侵入方式梳理资产与服务，识别潜在风险暴露面。对安全团队掌控全网态势，发掘隐藏风险，聚焦真实威胁，加强联动能力，提升运营效率等方面提供有力支撑。

核心功能：

精准威胁检测，识别外部成功攻击、梳理内网渗透态势、定位内部失陷主机。

TDP ®通过对全流量日志以及告警原始流量包记录，采用分级存储策略，为企业提供攻击行为丰富的上下文信息；通过双向流量检测，精准识别外部成功攻击；利用可视化技术，多维度多视角地呈现威胁态势；依赖微步在线全球最新的威胁情报数据能力和专业的威胁分析，精确定位内网中的失陷主机。

全面梳理资产，识别风险暴露面

TDP ®通过流量监听来对企业业务资产进行识别，了解企业自身开放的服务、端口、应用，帮助企业了解自身资产的暴露情况，并能够针对性做出合理管控；通过实时检测模块，监测企业对外开放登录后台的访问，企业内外部的弱口令，API 的异常使用情况以及企业内外部的文件传输行为，帮助企业了解风险点。

网络 + 端点的联动处置，消除威胁

安全团队可通过网络告警中丰富的威胁情报上下文，辅助处置决策。平台支持对外部威胁进行阻断；并提供和平台联动的终端工具，以便于定位恶意进程，阻断网络访问，自动化清理流行恶意软件。

产品特性：

01

分钟级同步微步在线专业威胁情报库

02

威胁事件科学归类，并提供丰富的威胁事件上下文信息

03

支持以旁路的方式灵活部署在任意网络节点

04

完整还原攻击路径，多维度多视角呈现安全态势

05

提供联动终端处置工具，定位恶意进程和阻断威胁

06

支持双向流量监听，快速检测攻击成功以及针对性告警

“聚焦真实威胁”

互联网安全接入服务 OneDNS

OneDNS Cloud

产品概述：

OneDNS 互联网安全接入服务是微步在线提供的具备安全防护能力的 DNS 递归解析服务，该服务可以保护任何一台终端、任何一个办公职场均可安全地接入到互联网，有效防护：恶意软件、勒索病毒、APT 攻击、钓鱼链接、非法站点。

产品特性：

无需任何硬件

分钟级配置即可完成上线

全面威胁防护

全面防护恶意软件、勒索病毒、APT 攻击、钓鱼链接、非法站点等

多职场统一管控

一个账号管控多个职场安全，让分支机构借力专业威胁情报能力实现高级威胁防护

覆盖漫游终端

保证员工设备在任何时间任何地点都能安全地接入互联网

灵活定义策略

轻松为多设备、多分支快速应用安全管控规则

稳定、高效的 DNS 解析

覆盖全国的加速网络、长达 7 年的 100% 稳定运行，无感知故障切换技术

亮点功能：

威胁拦截功能

基于微步在线专业威胁情报数据，可识别全球恶意软件远控地址、钓鱼地址和矿池地址，并识别关联的恶意软件、攻击团伙、严重级别等信息。OneDNS 实时从微步在线云端同步威胁情报数据，来对威胁提供实时拦截能力。企业内一旦有对应的恶意软件运行，则 OneDNS 将会阻断这些恶意软件与远控端的通信，有效降低恶意软件的风险，包括阻止恶意软件进一步运行、阻止下载其他恶意模块如内网渗透模块、挖矿模块等。

上网行为分类拦截

基于微步在线安全云的大数据捕获能力与域名分类能力，可准确捕获全球任意一个新增域名，并准确识别其对应网站分类，目前识别超过 80 种分类，包括非常多的敏感类别如：色情暴力、违法内容、赌博、文件共享、游戏、广告等。用户可自主选择是否拦截这些类别的站点。

内部威胁主机定位

通过 OneDNS 拦截恶意软件的通信之后，安全团队如果需要进一步定位内部机器并进行分析、溯源和清理工作，可使用内部威胁主机定位工具 - 虚拟转发器（简称 VA）来实现内网机器的定位。该工具可作为 DNS 服务器插件的方式安装，或者独立安装并接入 DNS 日志或者旁路流量。

职场与策略管理

为管理多职场，OneDNS 提供职场管理能力，可为职场配置出口、管理员、用户、漫游终端，并为各职场灵活配置防护策略。一键配置，毫秒级生效。

动态 IP 接入

对于出口为动态 IP 的机构或者分支单位，可使用动态 IP 接入功能，保证这部分机构可稳定、持续使用 OneDNS 的拦截能力。

漫游终端接入

为远程办公的设备提供一键安装的轻量工具，无论切换到什么网络，均可自动调整系统 DNS 配置保证可接入 OneDNS 防护体系。该工具支持 Windows、Mac 等多种操作系统。

本地态势感知平台对接 API

提供 API 能力与本地的日志平台、态感平台进行对接，输出 OneDNS 全量防护数据。

微步在线云API

ThreatBook SaaS API

产品概览：

云 API 依赖云端强大的、基础数据收集系统，结合自主研发的多款、累计数十种提取方法的核心情报提取系统，快速且自动化的生产高覆盖度、高准确度、上下文丰富的情报数据。为各种不同类型的业务提供独特的价值。

数据积淀

日均数百万新增域名，累计数百亿的域名基础数据

8年PassiveDNS数据

18年的域名历史Whois数据

日均100万新增恶意样本、累计数十亿恶意样本

40 万 高精度 IOC 失陷情报数据

42 亿 全球 IP 信誉与标签

180余个全球范围内大型黑客组织，小时级全球事件跟进

分钟级情报更新

业务价值

办公网终端/生产网及DMZ区服务器的威胁发现和失陷检测

Web/邮件/SSH等公网开放的应用或者服务的外放访问IP的风险识别

终端/服务器的可疑文件/进程的是否属于恶意程序的分析识别

内部SOC/SIEM大数据平台或者WAF/IPS/NGFW等安全设备日志的威胁检测

内外部安全事件的关联拓线及溯源追踪

接口能力

	IP 检测能力	域名检测能力	文件分析能力	URL分析能力
基础分析接口	IP分析 IP信誉 失陷检测	域名分析 失陷检测	Hash查询 文件信誉报告 反病毒引擎检测	URL分析 URL信誉报告
高级查询接口	IP高级查询	域名高级查询 子域名查询 域名上下文		

情报驱动的恶意软件分析平台

ThreatBook Cloud Sandbox

产品概览：

与传统的反恶意软件检测不同，微步云沙箱提供完整的多维检测服务，通过模拟文件执行环境来分析和收集文件的静态和动态行为数据，结合微步威胁情报云，分钟级发现未知威胁。

产品功能：

基于多款反病毒引擎检测，快速检测已知威胁

利用虚拟化沙箱深度分析技术，实现恶意文件自动化、可定制化的行为分析，检测未知威胁

集成微步多个核心的高级情报分析系统，对文件运行过程中的网络、主机行为进行智能化的威胁判定，产出可直接用于失陷检测和应急分析的 IOC

支持识别和检测反沙箱恶意软件，防止恶意软件逃避虚拟机检查

产品优势：

1 汇集 25 款源于不同国家的顶级反病毒引擎，帮助提高对已知威胁的检测能力。

2 持续通过遍布全球范围的蜜罐网络等多个渠道实时捕获全球上百万最新新增恶意样本，实现全球范围内威胁的全覆盖。

3 结合 700 多个高质量行为签名，提升识别和分类恶意软件的能力。

TIP-本地威胁情报管理平台

Threat Intelligence Platform - TIP

产品介绍

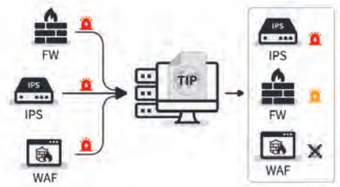
微步本地威胁情报管理平台(Threat Intelligence Platform，以下简称TIP)是一款部署在用户本地环境的多源威胁情报管理平台。

主要用于整合多源情报，实现统一管理与共享；与现有安全系统或态感系统对接，降低告警噪音、提升威胁感知与响应能力；帮助企业进行本地私有化情报生产，实现情报关联分析与深度挖掘。

产品特性

产品价值

1 解决现有安全运营人员“告警疲劳”问题



“安全设备每天告警太多了，看不过来……”

为现有告警信息附加更多威胁情报字段，帮助企业对海量告警进行筛选、过滤、优先级排列，提高告警信息丰富度，提高安全设备和人员的检测分析能力，通过威胁情报可以通过零星的告警线索快速关联安全事件攻击者所属团伙、意图、手段、特征，进一步清晰还原攻击者画像，帮助应急响应人员进行威胁隔离和消除，并对未来黑客可能采取的攻击手段进行预防。

2 解决情报生产能力问题

“授人以鱼不如授人以渔”

通过TIP内置的生产模块，真正赋予用户情报生产能力，准确、透明、可调节的生产过程让每个用户都拥有自己的情报生产基地。

3 解决自动化联动防御问题

“自动化攻击大行其道，防守者如何进入防御快车道？”

TIP内置SOAR模块，支持自定义联动策略充分利用原有安全设备建立联合防御阵地，快速实现单点失陷全面防御策略。

4 解决匿名共享威胁情报问题

“我们被攻击了，想匿名提供攻击者信息，看看谁能提供有价值的线索”

“HW期间，如何匿名自动化的获取高价值威胁情报？”

用户许可前提下，TIP可加入微步情报网匿名发布攻击者信息或狩猎相关线索，HW期间不同行业的TIP用户匿名自动交换高价值威胁来源地址，高效进行提前防御。

5 解决云环境安全能力萎缩问题

“我们公司业务都已经上云了……”

TIP支持硬件、软件交付行态，支持在本地和各类云环境部署。

微步在线X情报社区

Threat Intelligence Analysis Community - X

产品概览：

X 情报社区是国内首个综合性的威胁分析平台和情报分享社区。以威胁数据查询、分析及情报数据共享为基础，为全球安全从业人员和企业提供便利的一站式分析工具，旨在帮助社区用户通过实时返回的分析检测结果及已分享的情报样本、黑客资源、攻击手法、线索、事件等，提高安全事件的快速分析与响应处置能力；同时，为企业用户提供安全运营工具、外部资产监控、行业情报等企业级服务，辅助个人及企业快速定位及排除安全隐患。

产品特性：

开放的社区用户情报及诱人的奖励计划

除公开的用户分享情报外，X 情报社区首创发布价值千万的情报奖励计划，促进安全行业情报共享，重视优质情报发掘，诚意回馈社区成员与商业客户。

丰富的威胁类型查询与分析结果

深耕威胁数据精度与宽度，提供丰富数据源及可视化关联分析结果，辅助用户快速、及时排除网络安全隐患。支持资产监控、域名 /IP/Hash/URL 等的安全分析、可视化分析，用以进行事件鉴别、威胁程度分析、威胁影响分析、关联及溯源分析等。

强大的企业级工具和服务

提供企业级批量情报查询工具及外部资产监控等服务，助力企业快速发现资产威胁，密码泄露、敏感文件泄露、邮箱泄漏等数据泄露风险，及对外开放后台、服务、端口等服务暴露风险。

精准的场景化威胁情报API功能

为企业应用场景打造的 Private API，可获取微步在线威胁分析平台的所有数据，支持与您的产品或服务做深度整合。辅助您现有的安全设备开启“上帝视角”。

适用场景

- 办公网/生产网的失陷检测
- 入站风险识别
- 内部SOC/SIEM系统的威胁检测能力提升
- 企业资产发现
- 文件威胁检测
- URL威胁检测

产品功能：

基础情报查询

支持全球恶意 IP、恶意域名、白名单域名、恶意 URL、远控 C&C、恶意钓鱼 URL、黑白文件 Hash、SSL 数字证书等的快速检索。检索结果包括：威胁评估结果、情报类型、相关安全事件信息背景信息（家族、行业等）、相关恶意样本等。

高级数据查询

支持 IP 的 PDNS 数据、域名历史 WHOIS、子域名数据等高级查询，为用户对攻击事件中域名、IP 的关联资产进行拓线分析提供助力，获得更多背后攻击团伙的攻击资产信息。同时结合 whois 等数据溯源，得到背后攻击者的个人身份或者虚拟身份。

重保护航

支持企业外部资产监控，及时掌握资产暴露面、数据泄漏、服务暴露等风险情况。同时提供批量情报查询工具，一键提交快速获取关键情报结果，协助用户特殊时期快速发现威胁，辅助提升处置效率。

可视化关联分析

一键自动关联查询。能够基于域名、IP 等初始线索，自动关联相关信息，对攻击事件相关 IP、域名、样本信息进行自动威胁评估。

资源监控

对于敏感 IP、域名进行监控，以便及时掌握其关联样本、报告、相关 URL、关联信息变化，便于追踪黑客攻击事件等。

情报分享

同社区用户分享情报样本、黑客资源、攻击手法、线索、事件等，共建安全行业社区。

详情请登录 x.threatbook.cn

检测及响应服务

Managed Detection and Response -MDR

服务概览：

基于微步在线全球领先的威胁情报、专业安全分析团队及先进的产品 / 工具，为企业提供威胁巡检、应急响应、重保驻场、专家咨询、高级情报订阅、外部资产监控等安全相关服务。由资深安全专家提供支持，对企业内外部威胁及时发现、告警、处置、响应，并对攻击者进行画像分析与溯源分析。针对主流威胁、重大安全事件、高危 APT 等事件进行深度分析。提供预警、防范、处置及修复建议。针对金融、能源、政府等重点行业威胁情报及安全事件提炼分析，提供处置及应对的最佳实践，帮助提升企业安全水平。

服务内容

外部资产梳理服务

基于领先的威胁情报基础数据支撑和强大的数据采集能力，对客户数据泄露、服务暴露、资产漏洞、网站挂马篡改、资产恶意情报标记等进行监控。

威胁巡检服务

配合专业检测设备，定期（如每月 / 季度）提供专业巡检、分析及专家咨询服务。

应急响应服务

当客户突发重大安全事件，如数据窃取、APT 攻击、勒索加密、漏洞攻击等，提供专业的应急取证、威胁定位、溯源分析、安全加固等服务。

暗网监控服务

通过暗网搜索引擎实时获取多个暗网论坛最新交易信息，覆盖金融、能源、政府等重点行业的数据泄露、黑客工具交易、色情、涉政涉恐等违法犯罪活动。

高级情报订阅服务

针对重点行业典型安全事件以及全球最新流行性威胁、外部资产及风险的深度分析报告，输出高价值的安全防护情报、措施及建议。

重保驻场服务

针对重要活动、攻防演练等活动提供全流程的服务，覆盖前期的准备阶段、实战阶段和总结阶段。

安全服务能力

微步专业安全分析 / 服务团队

1	2	3	4	5	6
资深的漏洞分析专家、逆向工程师、恶意软件分析师等信息安全专家。	熟悉常见 APT 组织 / 黑产团伙的攻击手法及特点。	熟悉金融行业特点及其面临的主要威胁。	具备丰富的甲方工作经验，对于企业安全建设具有多年的经验。	平均安全从业经验达 8 年以上。	国内领先的威胁情报专家，云端威胁情报系统和狩猎系统支持。不仅在主流威胁的快速定位和处置上具有丰富经验，更有深度挖掘威胁事件、内部溯源的专业能力。

海量的情报基础数据

- 8 年 PDNS 数据
- 18 年历史 Whois 数据
- 累计数十亿的恶意样本

全面的服务 / 产品 / 系统

- 便携式内网威胁检测设备
- 国内最大的威胁分析社区 X
- 自动化样本分析沙箱 S
- 自动化的追踪溯源系统 Z

丰富的安全服务经验

- WannaCry/Petya/BadRabbit 等重大安全事件响应经验
- 数百起 APT/ 挖矿 / 勒索 / 资金窃取等应急响应案例
- 参与重大会议安保、重保
- 累计服务金融、能源、政府、互联网数百家政企客户