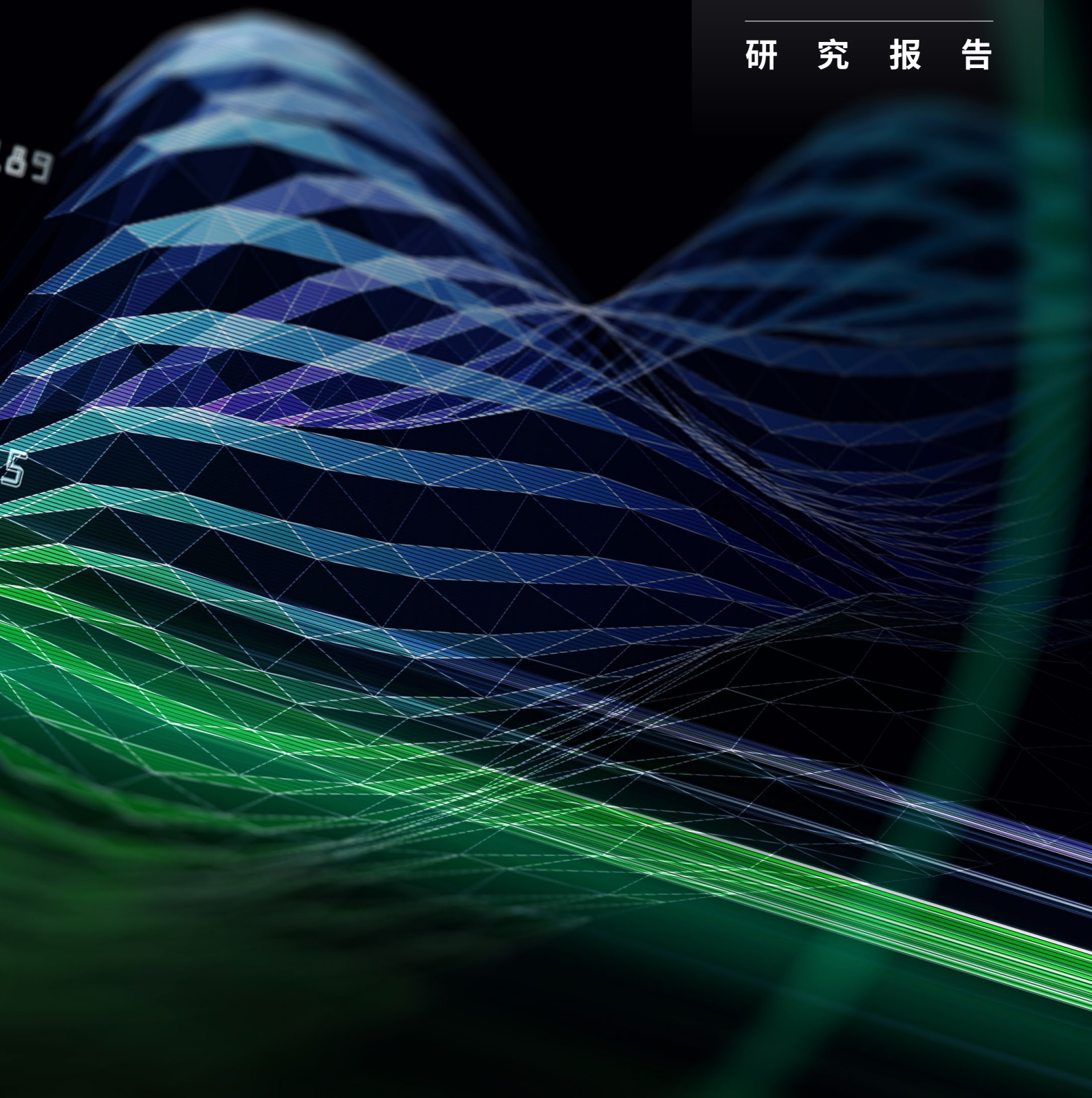
360数字安全
数字安全的领导者

360
高级威胁研究院

二零二二年全球高级持续性威胁研究报告



CONTENTS 目录

01

02

03

04

05

全球高级持续性威胁
研究报告
RESEARCH REPORT

2022 /
PART.01

2022年高级可持续性威胁概览

PART.01

2022年高级可持续性威胁概览

Advanced Persistent Threat

在经历了新冠肺炎疫情肆虐，当今世界正处在大发展大变革时期。2022年俄乌冲突爆发、全球经济衰退加之国际间各种力量的较量，使得国际局势日益错综复杂。2022年全球高级持续性威胁（APT）形势依然严峻。全年全球网络安全厂商公开发布的APT报告累计742篇，报告中披露的攻击活动涉及APT组织141个，其中首次披露的APT组织54个，均比2021年明显增加。全球范围内APT攻击活动依然紧跟政治、经济等时事热点，攻击目标集中分布于政府、国防军工、教育、金融等行业领域。

依托自身“看见”的能力，360已累计发现了51个境外APT组织，监测到5800多起针对中国的网络渗透攻击。2022年，360高级威胁研究院捕获到境外新组织：APT-C-63（沙鹰），另外在全球范围内率先监测到APT-C-06（DarkHotel）组织利用Firefox浏览器的2个在野0day漏洞（CVE-2022-26485、CVE-2022-26486）[1]针对特定目标进行水坑攻击。这也是2022年国内唯一一家捕获APT攻击活动中利用0day漏洞的安全厂商。2022年全球APT组织利用0day漏洞展开攻击活动的增长趋势放缓，但仍处高位。

2022年2月24日俄乌冲突爆发，成为全球关注的焦点。俄乌冲突期间，与俄乌冲突相关的APT攻击、大规模DDoS攻击、黑客组织网络攻击、网络信息舆论对抗等一系列网络攻击和对抗活动，将网络空间战争形态展现在了世人面前。网络空间已经成为俄乌间冲突对抗的重要战场，在军事冲突之外产生着愈发深刻的影响。

2022年是我国“十四五”规划的第二年，在全面建设社会主义现代化国家新征程中，一批5G、工业互联网等新基建项目扎实推进，为数字经济发展开拓新空间、增添新动能。新基建的背后是产业、经济、政府、社会的全面数字化，而数字化安全将成为发展数字经济、建设数字中国的底座，成为新基建的安全基建。

通过2022年全球高级持续性威胁态势分析看，我国数字化转型和自主可控领域的发展面临更加严峻和复杂的网络威胁形势。需要网络安全从业者保持网络空间常态实战化的状态应对网络空间的攻防对抗，不断提升我国网络安全和数据安全保护能力，保障国家网络空间安全。

全球高级持续性威胁研究报告
RESEARCH REPORT

2022 /
PART.02

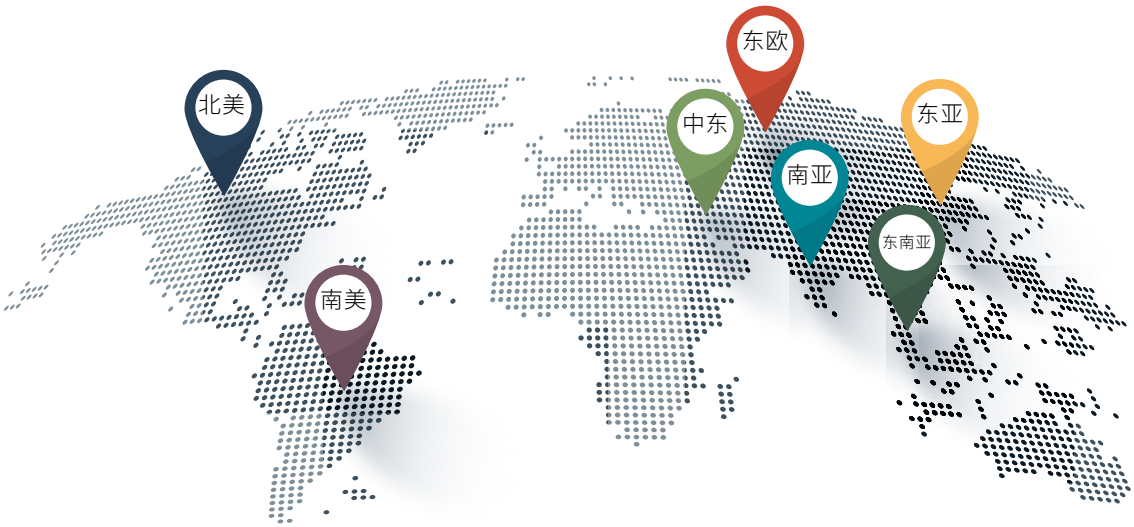
2022年活跃APT组织

PART.02

2022年活跃APT组织

Advanced Persistent Threat

2022年，俄乌冲突爆发和全球经济衰退对地缘政治乃至世界格局的演变产生了深远影响，使得国际局势日益错综复杂。与此同时，全球APT组织的攻击活动在地缘政治冲突热点事件的影响下，保持着高活跃度。2022年，全球网络安全厂商公开发布的APT报告累计742篇，报告中披露的攻击活动涉及APT组织141个，其中首次披露的APT组织54个，攻击活动涉及APT组织数量和首次披露的APT组织数量，均比2021年大幅增加。



东欧	热度
APT-C-53(Gamaredon)	★★★
APT-C-13(SandWorm)	★★★
APT-C-25(APT29)	★★½
APT-C-20(APT28)	★★
APT-C-29(Turla)	★½

东亚	热度
APT-C-01 (毒云藤)	★★★½
APT-C-28 (ScarCruft)	★★★½
APT-C-26 (Lazarus)	★★★
APT-C-55 (Kimsuky)	★★★
APT-C-06 (DarkHotel)	★★★

中东	热度
APT-C-23 (双尾蝎)	★★
APT-C-49 (OilRig)	★

北美	热度
APT-C-40 (NSA)	★★★
APT-C-39 (CIA)	★

南亚	热度
APT-C-08 (蔓灵花)	★★★
APT-C-48 (CNC)	★★½
APT-C-24 (响尾蛇)	★★½
APT-C-09(摩诃草)	★★½
APT-C-56(透明部落)	★★½
APT-C-35(肚脑虫)	★★
APT-C-61(腾云蛇)	★½

东南亚	热度
APT-C-00 (海莲花)	★★★½

南美	热度
APT-C-36 (盲眼鹰)	★

2022年全球典型APT组织分布

360高级威胁研究院对360全网数字安全大脑中APT威胁监测数据进行统计：2022年对中国发起的APT攻击活动，涉及14个APT组织，主要的攻击活动分布于政府、教育、信息技术、科研和国防军工等15个行业领域。

基于APT组织攻击频次、被攻击单位数量、受影响设备数量、技战术迭代频次等多个指标，我们对2022年对中国发起攻击活动的APT组织活跃程度进行评估，得出下表。

排名	组织名称	主要影响行业领域
TOP1	APT-C-01 (毒云藤)	政府、教育、科研等
TOP2	APT-C-00 (海莲花)	政府、信息技术、国防军工等
TOP3	APT-C-08 (蔓灵花)	政府、教育、国防军工等
TOP4	APT-C-12 (蓝宝菇)	交通运输、政府、国防军工等
TOP5	APT-C-48 (CNC)	教育、科研等
TOP6	APT-C-06 (DarkHotel)	贸易、教育等
TOP7	APT-C-60 (伪猎者)	贸易、教育等
TOP8	APT-C-09 (摩诃草)	教育、科研等
TOP9	APT-C-24 (响尾蛇)	医疗卫生、政府等
TOP10	APT-C-28 (ScarCruft)	政府、媒体等

北美 | Advanced Persistent Threat

APT-C-40 (NSA)

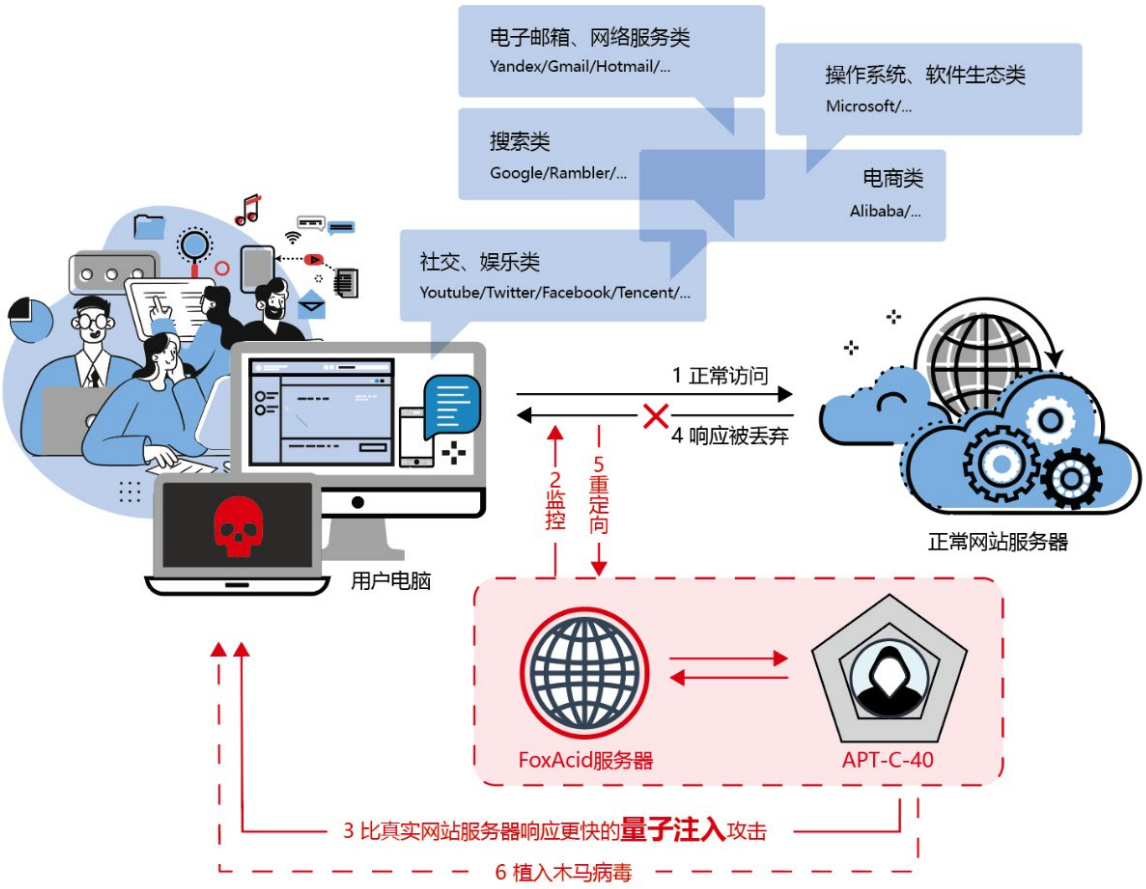
2022年，360高级威胁研究院陆续公开披露了《 网络战序幕：美国国安局NSA (APT-C-40) 对全球发起长达十余年无差别攻击》、《Quantum (量子) 攻击系统-美国国家安全局 “APT-C-40” 黑客组织高端网络攻击武器技术分析报告 (一) 》、《关于西北工业大学发现美国NSA网络攻击调查报告 (之一) 》、《西北工业大学发现美国NSA网络攻击调查报告 (之二) 》等多篇有关NSA组织攻击活动及技术细节报告。

发布时间	发布机构	披露内容
2022年2月23日	奇安盘古实验室	Bvp47-美国NSA方程式组织的顶级后门[2]
2022年3月2日	360高级威胁研究院	网络战序幕：美国国安局NSA (APT-C-40) 对全球发起长达十余年无差别攻击[3]
2022年3月14日	国家计算机病毒应急处理中心	“NOPEN” 远控木马分析报告[4]
2022年3月15日	安天CERT	从 “NOPEN” 远控木马浮出水面看美方网络攻击装备体系[5]
2022年3月22日	360高级威胁研究院	Quantum (量子) 攻击系统-美国国家安全局 “APT-C-40” 黑客组织高端网络攻击武器技术分析报告 (一) [6]
2022年6月29日	国家计算机病毒应急处理中心	美国国家安全局 (NSA) “酸狐狸” 漏洞攻击武器平台技术分析报告[7]
2022年6月29日	360高级威胁研究院	“验证器” (Validator) —美国国家安全局NSA (APT—C—40) 的木马尖兵[8]
2022年9月05日	360高级威胁研究院	关于西北工业大学发现美国NSA网络攻击调查报告 (之一) [9]
2022年9月27日	360高级威胁研究院	西北工业大学遭受美国NSA网络攻击调查报告 (之二) [10]

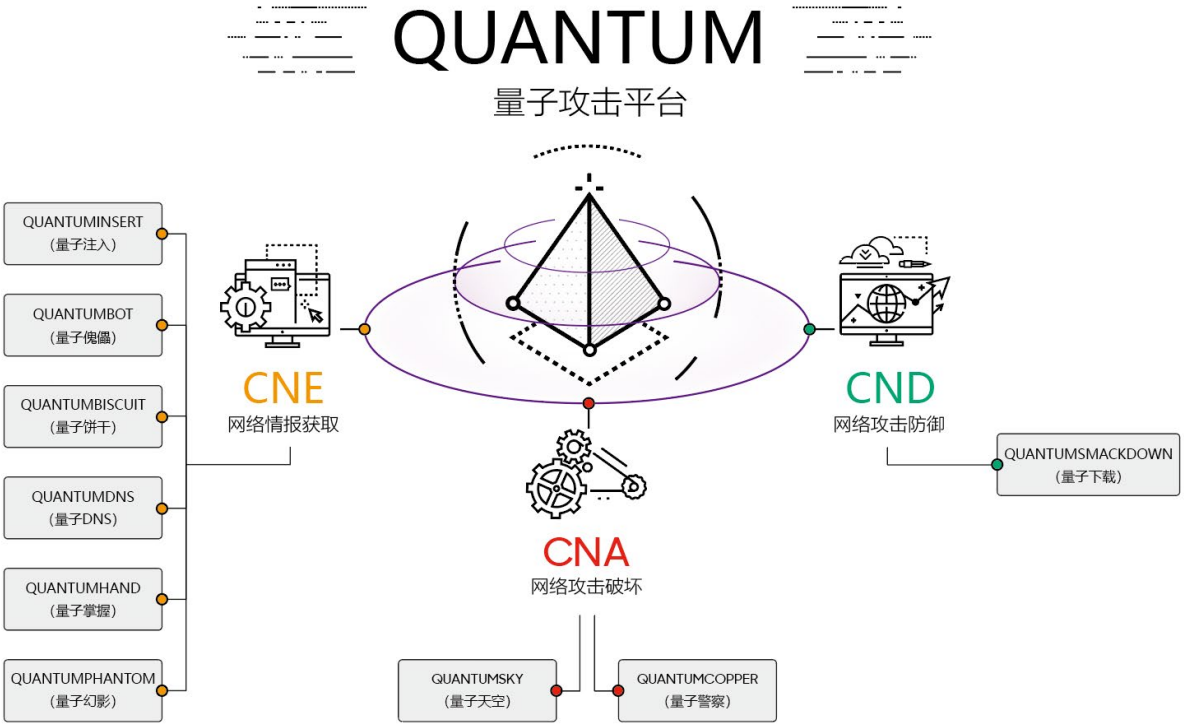
APT-C-40 (NSA) 组织持续对中国和全球多个国家地区展开网络攻击活动，给全球互联网安全带来了严峻的风险和挑战。在披露的NSA组织对西北工业大学的一系列网络攻击活动中，美国国家安全局 (NSA) “特定入侵行动办公室” (TAO) 使用了40余种不同的NSA专属网络攻击武器，持续对西北工业大学开发起多轮持续性的网络攻击和窃密行动。

一直以来，美国国家安全局 (NSA) 针对我国各行业龙头企业、政府、科研机构甚至关乎国计民生的核心基础设施运维单位长期进行黑客攻击活动，对我国的国防安全、关键基础设施安全、社会安全、生产安全以及公民个人信息安全造成严重危害。

APT-C-40组织针对中国境内目标攻击中使用了其最具代表性的Quantum (量子) 攻击系统。该系统针对国家级网络通信进行中间劫持，以实施漏洞利用、通信操控、情报窃取等一系列复杂网络攻击。360全网数字安全大脑对Quantum (量子) 系统进行了长期的跟踪研究，并对Quantum (量子) 系统的九种先进网络攻击能力模块进行了总结。



Quantum (量子) 攻击系统示意



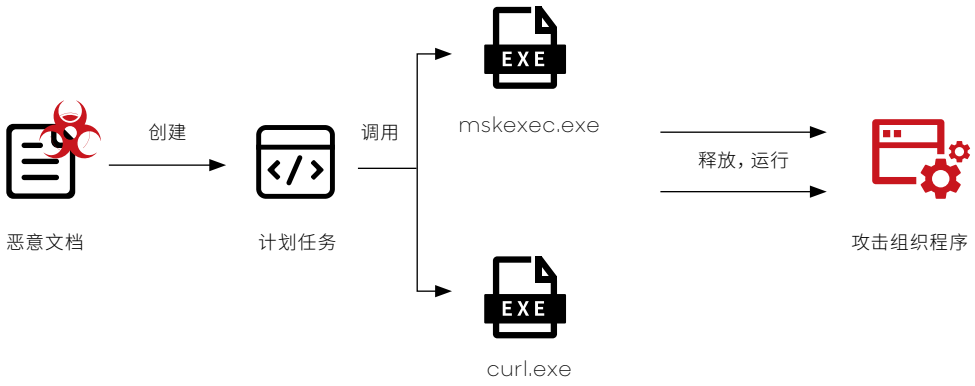
当前全球不稳定因素增多，国际势力间的对抗增加，在此大背景下，大国间的网络对抗势必将会持续进行，面对国家级背景的强大对手，我们需要长期的关注和防范以APT-C-40 (NSA) 为代表的北美APT组织通过网络空间，对我国重点行业领域的攻击活动。

南亚 | Advanced Persistent Threat

2022年，南亚地区APT组织相关攻击活动依然针对南亚、东南亚等地区，围绕国防军工、政府、能源、科研等关键行业领域。在2022年，南亚地区的部分APT组织，如摩诃草、CNC、蔓灵花等，被发现选择医疗行业作为攻击目标，推断这可能与2022年爆发的多起大规模传染病传播事件（如猴痘、不明病因儿童肝炎、新冠病毒变异株Deltacron变种等）存在一定相关性。

• APT-C-08（蔓灵花）

2022年APT-C-08（蔓灵花）组织依旧延续使用之前的攻击技战术，主要使用恶意文档作为与目标人群接触的切入点，通过文档中携带的宏代码、公式编辑器漏洞、chm包含的内嵌脚本等方式来完成代码的执行，通过执行的代码在设备中留下计划任务，用以周期性的与服务器进行连接，通过计划任务调用curl.exe或msiexec.exe向服务器请求文件数据，最终完成落地。



较以往有所不同的是，在msi文件中，部分文件中包含VBS文件。VBS文件的功能多为重命名并执行一同被释放的组件程序，在这些VBS文件中，会以"explorer.exe"代理启动指定应用程序。

攻击流程简要示意图

在2022年上半年，360高级威胁研究院捕获到了蔓灵花组织使用的最新远控程序，根据其路径名“wmservice.exe”，将其命名为“wmRAT”，该远控程序使用的指令功能列表如下:

指令	功能
0	包含打开文件流、上传设备信息、删除指定路径下文件等功能的7个子指令
1	向服务器提供远程shell
2、3、4、7、9、10、13、14	无功能
5	关闭指令“F@ngS”中打开的文件流
6	接收文件数据，写入指令“F@ngS”打开的文件路径中。
8	打开文件，并向服务器上传数据，单次上传字节0x2000
11	上传文件数据（单次上传0x2000字节及以下）
12	搜索指定路径的文件/文件夹，将文件信息发送至服务器
15	搜索指定路径的文件/文件夹，将文件名发送到服务器

由于“wmRAT”当前已有的功能以文件搜索和上传下载等功能为主，且在通讯中存在较多无实际功能的指令，推断该远控程序还处于研发阶段，后续可能增加其他多种功能在更多维度完成对失陷设备的控制。

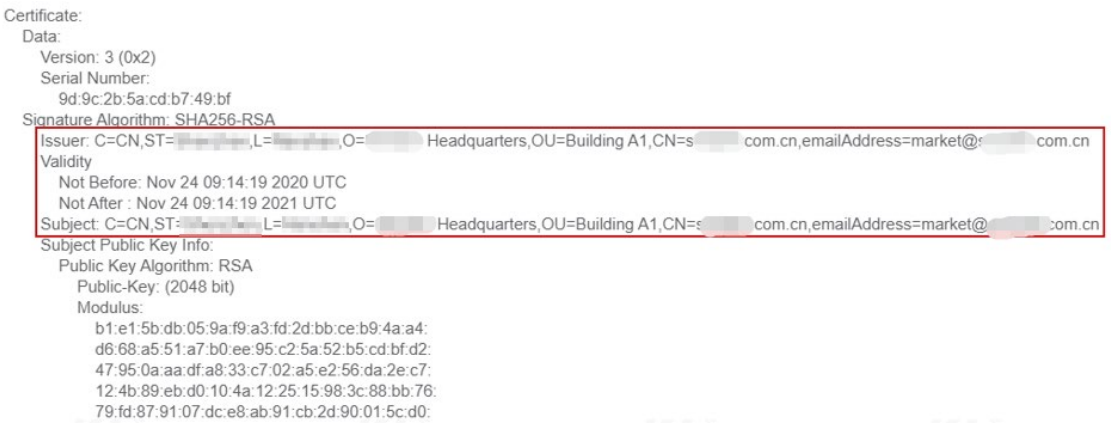
• APT-C-48 (CNC)

APT-C-48 (CNC) 组织在2022年的攻击活动继续重点针对教育、科研领域相关单位。该组织攻击技战术也沿用2021年360高级威胁研究院对外发布的《猎天行动CNC (APT-C-48) 组织最新攻击活动披露》[11]一文中披露的两种攻击流程，在原攻击流程不变的基础上进行了拓展优化，增加多种功能组件程序的下发，试图增强对设备的控制。

360高级威胁研究院对捕获到的APT-C-48 (CNC) 组织威胁样本文件进行分析，威胁样本文件名和对应功能如下表：

文件名	相关功能
lsass.exe	窃取最近打开的文件，并通过FTP上传到服务器
zdwm.exe	向docx文件中注入恶意宏代码
AdobeIPCBrokr	向GitHub上传目标设备相关信息
MSUsoCoreWorker.exe	记录键盘按键消息
Chrome/Edge	窃取chrome/edge浏览器中保存的用户名密码
sharpscanner	探测端口/网段信息
Screenshooter	截图/录屏工具
Plink	Plink网络集成工具
socketServe	Socket_server,代理服务端

CNC组织凭借对攻击目标以及失陷设备的情报收集，将攻击过程中的部分步骤完成了定制化的改变，如基础设施的SSL证书源自国内某安全厂商。



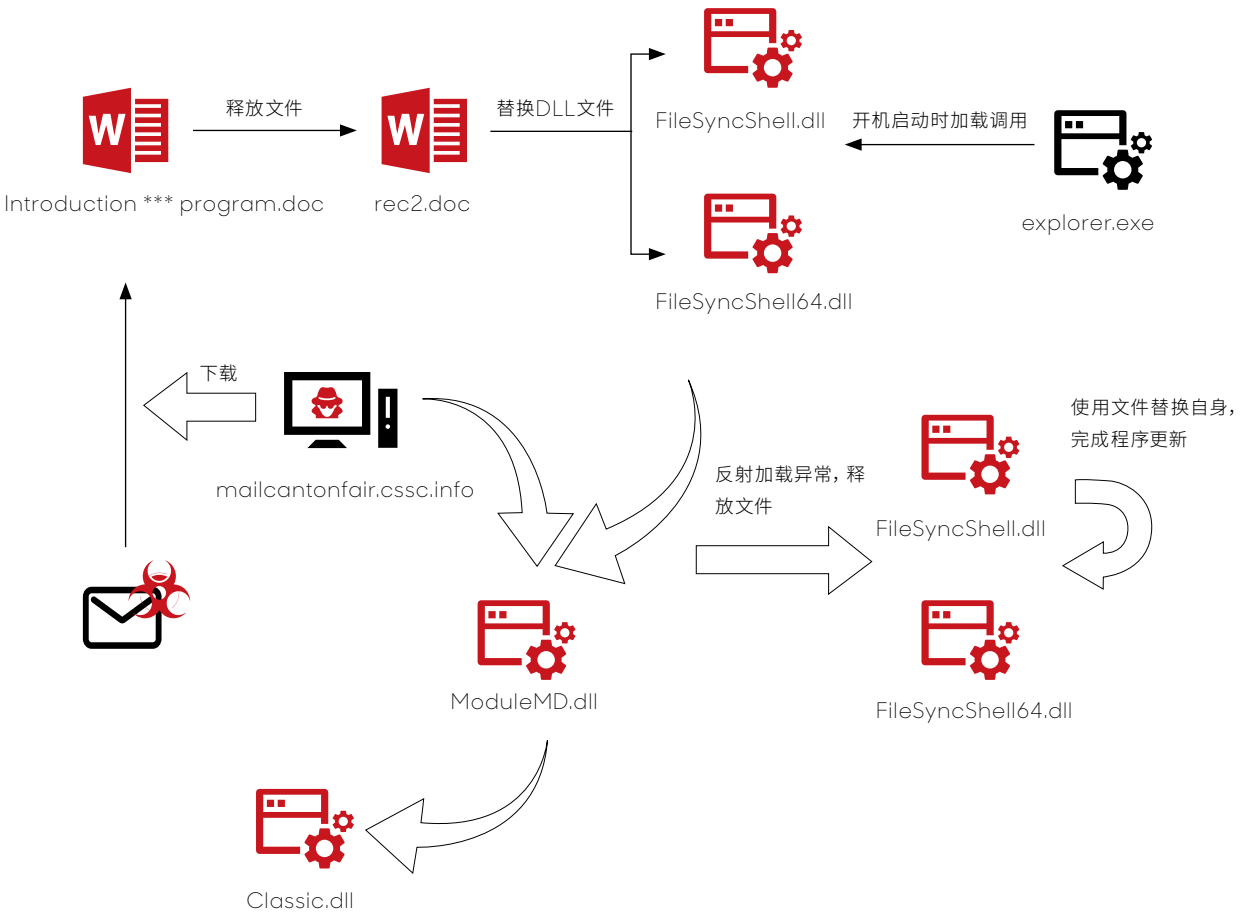
CNC组织的威胁样本在部署时会通过劫持设备上常用软件程序或功能组件作为驻留路径，360高级威胁研究院捕获到的CNC组织曾替换的软件名称如下:

SGTool.exe
YoudaoDict.exe
wpsupdate.exe
sogouupdate.exe
360zipupdate.exe
...

• APT-C-24 (响尾蛇)

2022年，响尾蛇组织依旧以南亚周边国家地区的外交事务相关人员为重心展开攻击活动，此外360高级威胁研究院也捕获到部分该组织针对医疗行业人员的攻击事件。

2022年2月，360高级威胁研究院首次捕获到响尾蛇基于“FileSyncShell.dll”实施的攻击活动：《filesyncshell.dll劫持？APT-C-24响尾蛇最新攻击活动简报》[12]。在攻击流程中利用了windows中FileSyncShell.dll会开机自启以及多个应用程序调用的特点，将恶意程序与设备上的白文件进行替换，完成劫持行为。



上述攻击流程与响尾蛇组织在2020年对国内某高校使用漏洞“CVE-2017-0199”+“CVE-2020-0674”的情况相类似，此攻击流程后续并未被发现在攻击活动中广泛投入使用。

响尾蛇攻击活动流程

除上面提到的个别攻击活动外，响尾蛇2022年整体的攻击流程以及代码框架并未发生较大的变化，主要变化集中在对“DotNetToJScript”生成的脚本代码的混淆上。

```
    try {
        var hKLWM = ActiveXObject, ct_transiti = window["eval"]("String.fromCharCode");

function SupportImagga_cropDefaultView(str) {
    var chars = str.split('');
    chars = chars.reverse();
    return chars.join('');
}

function AAAThingReturn(str, l) {
    var chars = str.split('');
    for (var i = 0; i < chars.length - (chars.length % l); i += l) {
        var temp = chars.slice(i, i + l);
        temp = temp.reverse();
        for (var j = 0; j < l; j++) {
            chars[i + j] = temp[j];
        }
    }
    return chars.join('');
}
```

图1

• APT-C-09 (摩诃草)

2022年下半年开始，APT-C-09 (摩诃草) 组织针对国内的攻击活动突增，主要针对科研教育领域，相关集中攻击持续几个月后又处于蛰伏阶段。

摩诃草组织在攻击活动初期入侵阶段，使用漏洞文档文件完成代码执行，下发BADNEWS RAT到目标设备上，攻击过程与该组织历史攻击活动相似。在2022年的捕获的攻击活动中，摩诃草组织修改了开源工具” SharpInjector “代码，用以对Quasar进行封装，试图减少威胁样本文件落地时被查杀的概率。摩诃草组织攻击活动使用的攻击流程如下:

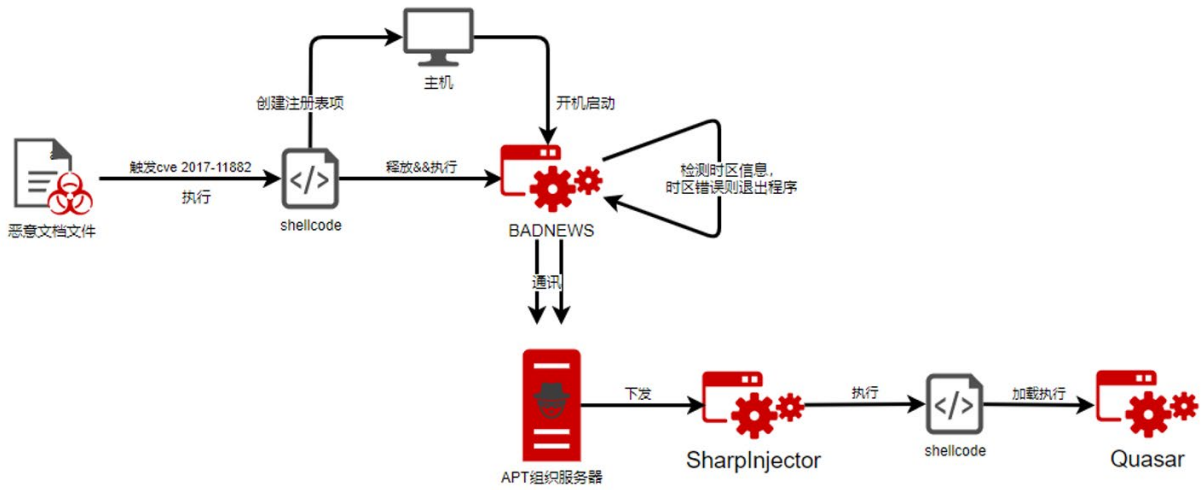


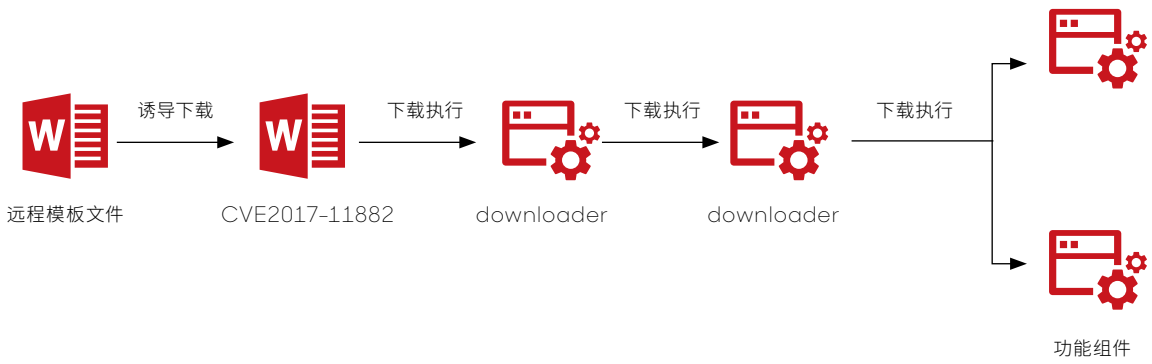
图2

图1 响尾蛇组织-变化后的混淆代码　　图2 摩诃草攻击活动流程图

● 其他组织

APT-C-35（肚脑虫）

APT-C-35（肚脑虫）组织又称Donot，是一个针对目标地区政府机构展开网络间谍攻击活动，以窃取敏感信息为主要目的的APT组织。该组织在2022年被披露的攻击活动中使用的攻击流程未发生变化，360高级威胁研究院对该组织惯用的攻击流程总结如下:



肚脑虫攻击活动流程

APT-C-61 (腾云蛇)

APT-C-61 (腾云蛇) 是由360高级威胁研究院在2021年首次披露的全新APT组织。该组织在基础设施的选择上，主要使用各类云服务平台，如：谷歌云硬盘、dropbox、herokuapp、pythonanywhere等。2022年腾云蛇组织被披露的攻击活动显示，该组织在载荷投递和代码执行进行了如下更新：

01.载荷投递

除了在邮件中携带附件的攻击方式外，腾云蛇增加使用链接的方式诱导用户下载文件到本地执行。

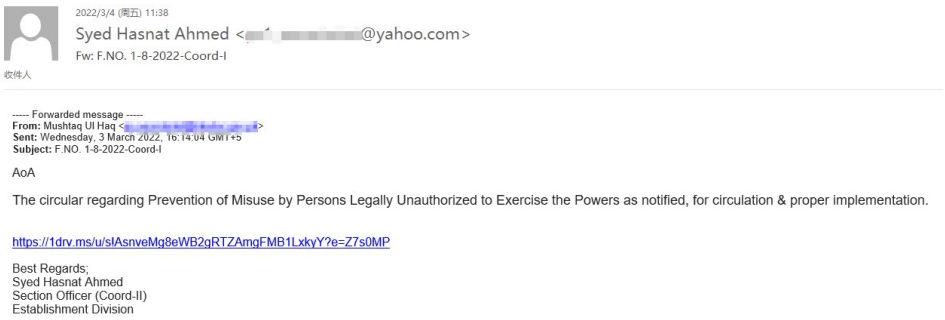


图1

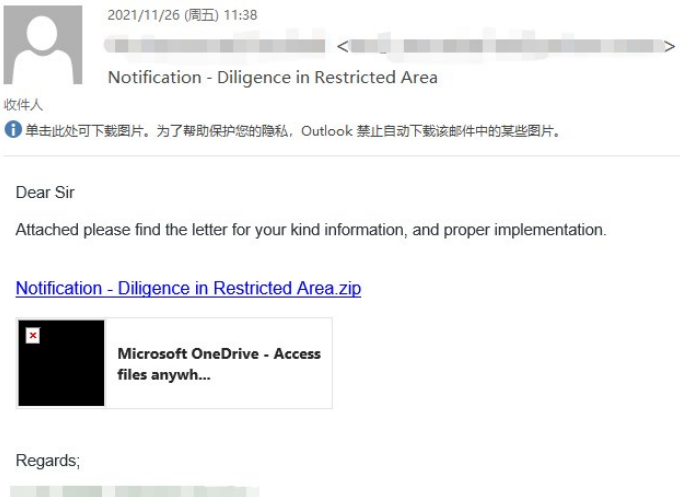
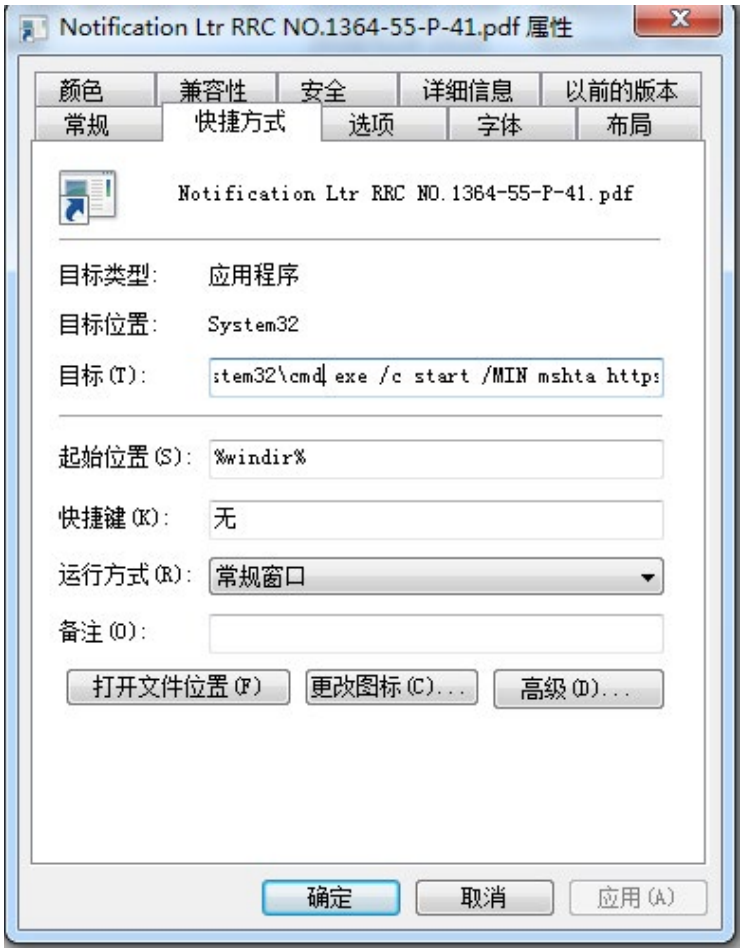


图2

图1 腾云蛇使用OneDrive共享链接实施钓鱼攻击　　图2 腾云蛇投递钓鱼攻击邮件

02.代码执行

我们捕获到腾云蛇开始效仿响尾蛇使用lnk文件调用mshta的方式来加载执行后续代码。相比响尾蛇，腾云蛇在快捷方式的使用上，存在多处细节差异。



腾云蛇使用的快捷方式文件

APT-C-56 (透明部落)

APT-C-56 (透明部落) 又名APT36、ProjectM、C-Major，是一个具有南亚背景的APT组织。在2022年，360高级威胁研究院持续监测和捕获到伪装成印度国防部邮件进行投递的恶意文档，文档内部包含宏代码，一旦用户疏忽点击了启动宏功能，内部隐藏的恶意宏代码自动运行。

2022年12月，360高级威胁研究院捕获到透明部落组织疑似围绕恐怖主义发起攻击的恶意样本。攻击者分别使用了Android和Windows平台的远控工具，其中Android平台攻击样本使用了商业间谍软件SpyNote和SonicSpy，以及开源间谍软件AhMyth和Metasploit。Android平台攻击样本主要伪装成与恐怖主义相关的内容和工具，如Explosive_course (爆炸物课程)、Abdul Rasheed (巴基斯坦伊斯兰原教旨主义者和圣战活动家)、Bolan Attack Video (俾路支解放军攻击视频) 等。

图1

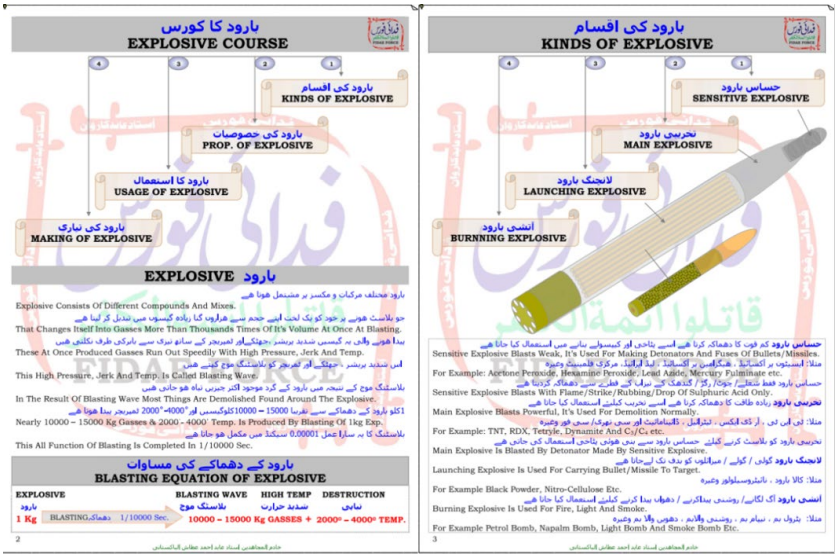


图2

图1 透明部落使用的Android平台恶意样本图标　　图2 伪装成爆炸物课程的恶意文档

东亚-朝鲜半岛 | Advanced Persistent Threat

2022年，东亚-朝鲜半岛地区的APT组织攻击活动尤为活跃，如：APT-C-26 (Lazarus)、APT-C-28 (ScarCruft)、APT-C-55 (Kimsuky) 等。

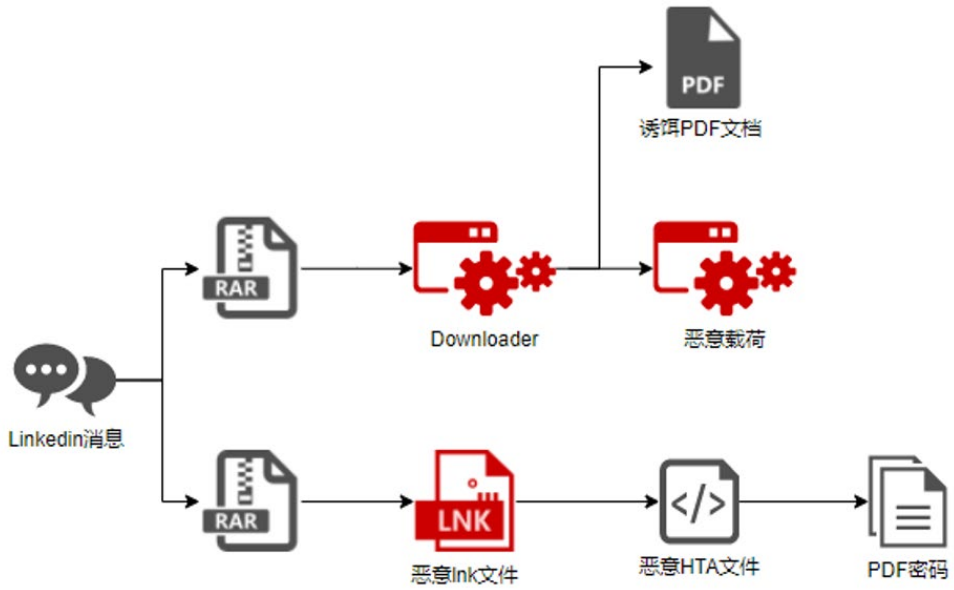
APT-C-26 (Lazarus) 组织作为东亚地区较活跃的APT组织，其攻击目标分布广泛，近年存在向加密货币行业领域发展的趋势。APT-C-28 (ScarCruft) 是一个技术精湛且非常活跃的APT组织，主要关注朝鲜半岛事务，攻击的也大多是与朝鲜半岛有关的商业组织和外交机构。APT-C-55 （Kimsuky) 组织是东亚地区最活跃的APT组织之一，该组织以专注网络间谍活动而闻名，偶尔会展开以经济利益为目的的网络攻击活动。

• APT-C-26 (Lazarus)

APT-C-26 (Lazarus) 历来是朝鲜半岛非常活跃的APT组织之一，长期针对东亚、南亚、东南亚等地区国家进行攻击渗透，攻击目标范围逐渐扩大。Lazarus组织以加密货币、金融、航空航天、军工、制造等为主要攻击目标行业。由于其针对全球金融机构的屡次攻击活动，已经逐渐成为全球金融机构的一大威胁。2022年Lazarus组织被披露的攻击活动显示，该组织持续重点针对加密货币行业领域进行钓鱼攻击，Lazarus组织2022年被披露的典型攻击活动如下表。

时间	披露厂商	事件
2022年1月13日	卡巴斯基	BlueNoroff小组发起SnatchCrypto攻击活动窃取加密货币[13]
2022年3月24日	Google	Lazarus组织利用Chrome中的远程代码执行漏洞CVE-2022-0609针对新闻媒体、IT、加 密货币和金融科技行业[14]
2022年4月18日	CISA	Lazarus组织攻击区块链和加密货币行业的各种公司、实体和交易所[15]
2022年4月26日	Zscaler	Lazarus组织针对东亚多个信息技术机构发起攻击[16]
2022年5月12日	ASEC	Lazarus组织利用Log4Shell漏洞投递NukeSped恶意软件[17]
2022年6月29日	Malwarebytes	Lazarus组织利用洛克希德马丁工作机会为诱饵，使用Windows Update客户端执行恶意代码，利用GitHub进行C2通信[18]
2022年7月5日	卡巴斯基	Lazarus组织投递DTRACK恶意软件和MAUI勒索软件[19]
2022年9月30日	ESET	Lazarus组织利用亚马逊主题针对欧洲目标发起攻击活动[20]
2022年10月24日	ASEC	Lazarus组织利用Dream Security公司的MagicLine4NX产品及BYOVD手法发起攻击[21]
2022年11月15日	卡巴斯基	Lazarus组织利用恶意软件DTrack对欧洲和拉丁美洲发起攻击[22]
2022年12月1日	volexity	Lazarus组织将AppleJeus恶意软件伪装成虚假加密货币应用程序发起攻击[23]

2022年8月，360高级威胁研究院监测到Lazarus组织以LinkedIn为媒介，向国内某机构发起“DreamJob”攻击活动。在该攻击活动中，攻击者通过LinkedIn平台向用户发送了与工作机会相关的恶意压缩文件，在恶意Downloader样本执行后，从远程C2下载下一阶段载荷和密码保护的诱饵PDF文档。之后又向受害用户发送包含恶意LNK文件的压缩包。执行恶意LNK文件后，加载远程HTA文件，显示PDF密码。



在2022年的攻击活动中，Lazarus组织不断开发新的恶意软件和探索新的攻击手法来对抗安全产品的检测。2022年9月，组织被披露利用新类型恶意软件MAGICRAT发起攻击，由于MagicRAT借助Qt框架构建，加大了人工分析和自动检测的难度；在2022年9月到10月，Lazarus组织被披露利用BYOVD技术手法发起攻击，BYOVD是“自带脆弱驱动程序”攻击方法，攻击过程中，通过修改与内核相关区域中的数据，禁用系统内包含反病毒程序内的所有监控程序。

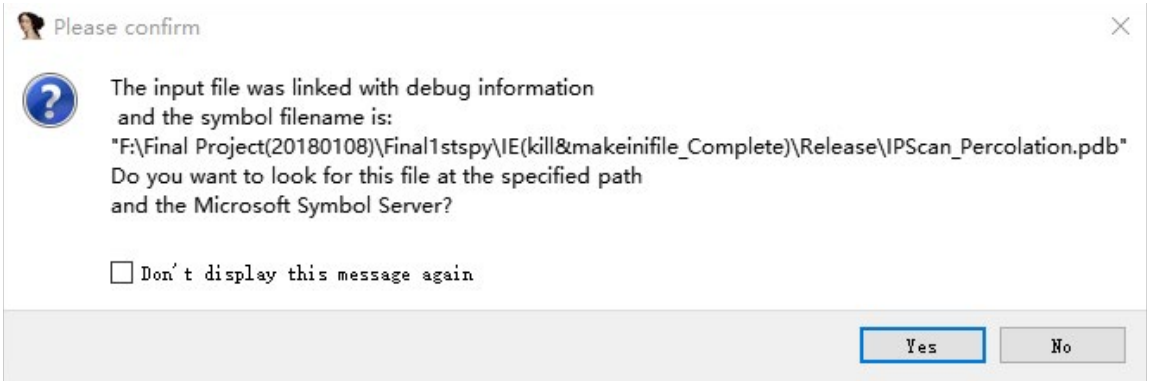
Lazarus组织“DreamJob”攻击活动流程图

• APT-C-28 (ScarCruft)

APT-C-28 (ScarCruft) 是具有朝鲜半岛背景的APT组织，善于利用热点事件发起攻击，主要以核问题、网络安全、朝韩关系、政治时事等话题为诱饵。2022年主要针对东欧、东亚相关重点目标发起攻击。

2022年3月，360高级威胁研究院监测到ScarCruft组织针对某驻外机构发起一系列攻击活动，例如向目标机构投递Final1stspy和DOGCALL恶意软件。Final1stspy恶意软件是ScarCruft组织使用的Dropper，用来投递DOGCALL恶意软件；DOGCALL是ScarCruft组织使用的后门，具有截屏键盘记录、捕获麦克风数据、收集受害者信息、收集感兴趣的文件以及下载并执行额外的有效载荷等功能，该恶意软件曾在2017年被用于攻击韩国政府和军事组织。

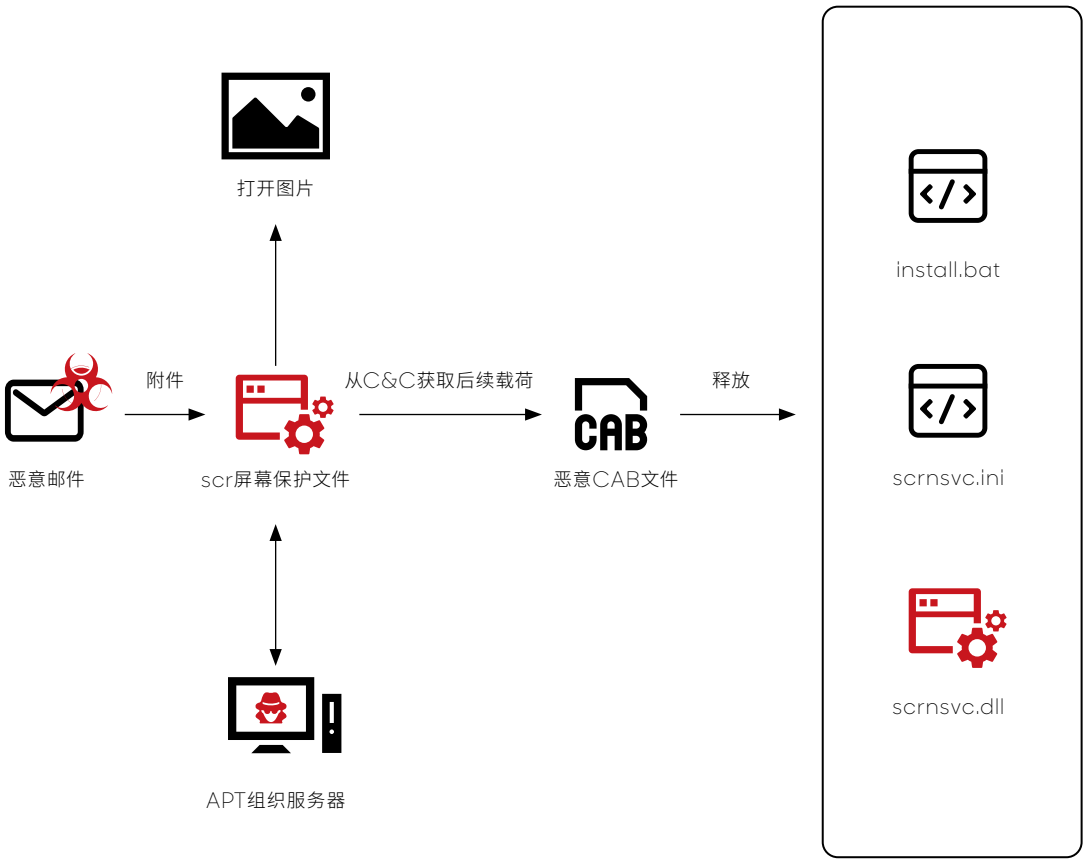
攻击者将Final1stspy伪装成微软补丁文件，例如KB330331.exe等，通过cmd指令调用PowerShell从失陷服务器投递到目标主机充当Dropper。样本在system路径下创建文件NWCWorkstation.dll。其中解密后的NWCWorkstation.dll为后续阶段载荷，并利用服务启动后续载荷。



Final1stspy载荷PDB信息

ScarCruft组织在2022年上半年，持续利用恶意软件植入等方式，针对东欧政府机构展开攻击活动。据安全厂商披露情报显示，该组织相关攻击活动至少从至少从2021年8月已经开始。2022年初，ScarCruft组织通过使用新年前夜庆祝活动相关主题的邮件作为诱饵，发起钓鱼攻击。一旦恶意电子邮件附件被打开和执行，会触发多个阶段的任务链，最终在受影响终端植入一个属于Konni RAT家族的恶意软件作为最终有效载荷。

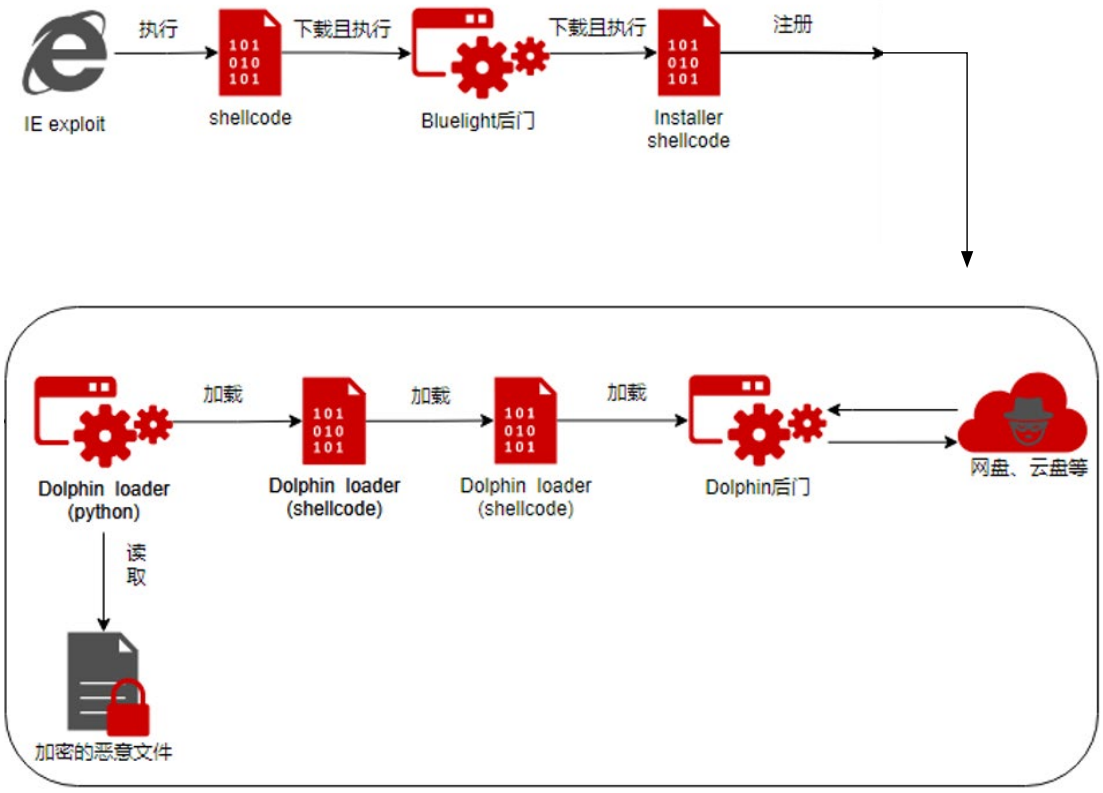
下图显示了在受影响终端，从包含恶意压缩文件的电子邮件附件解压开始，到执行恶意下载程序、下载程序激活复杂的操作链、完成命名为scrnsvc.dll的Konni RAT恶意软件植入，并将其作为Windows服务的攻击过程。



ScarCruft组织攻击流程图

2022年下半年，360高级威胁研究院捕获了ScarCruft组织针对某驻外机构的攻击活动。在攻击活动中，攻击者将初始可执行程序样本的图标伪装成文件夹以迷惑用户。用户执行后将恶意shellcode注入到系统程序进程中，通过后续多个阶段最终释放RokRat恶意程序。RokRat是基于云的远程访问工具，从2016年开始一直被ScarCruft组织在多个攻击活动中使用。

2022年11月，ScarCruft组织的新后门Dolphin被公开披露。该后门曾经被作为2021年初多阶段攻击的最终有效载荷。Dolphin后门仅针对选定的受害者手动部署，并且主动搜索驱动器并窃取攻击者认定高价值扩展名的文件。自2021年4月Dolphin后门首次被发现以来，现已经捕获到该后门的多个版本，攻击者在此期间不断尝试改进后门的功能，并试图逃避检测。



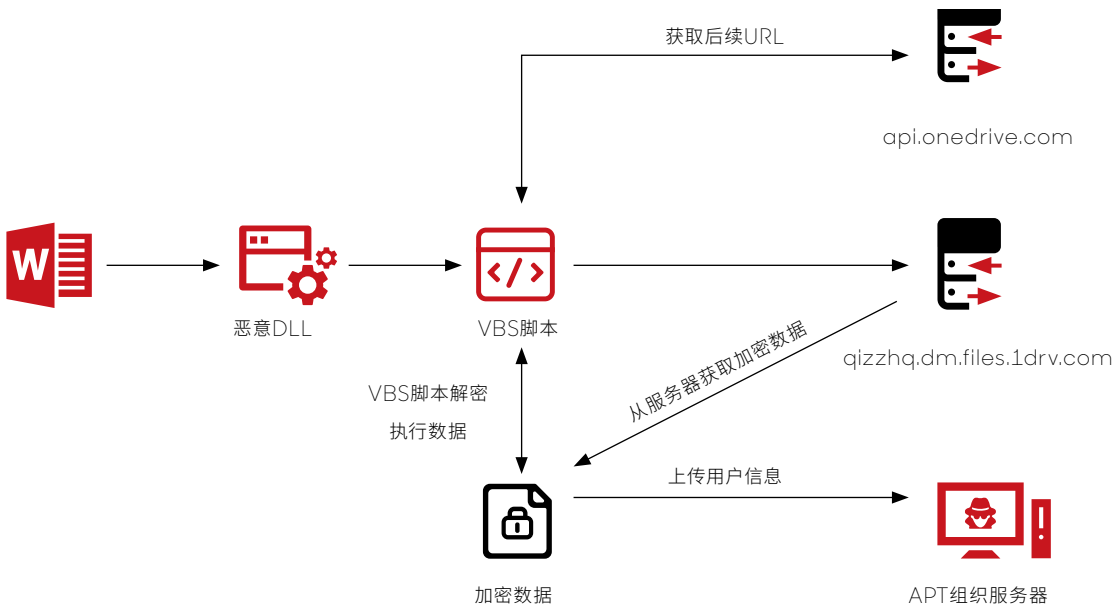
Dolphin恶意软件攻击流程图

• APT-C-55 (Kimsuky)

APT-C-55 (Kimsuky) 是东亚地区最活跃的APT组织之一，该组织以专注网络间谍活动而闻名，偶尔会展开以经济利益为目的的网络攻击活动。Kimsuky组织的攻击目标范围主要集中在东欧和东亚地区。2022年，Kimsuky组织被披露的主要攻击活动主要是针对智库、军事、工业、研究所等机构展开，同时其攻击目标涉及加密货币行业，攻击方式以钓鱼攻击为主。

2022年，360高级威胁研究院捕获到了Kimsuky组织使用BabyShark组件的多起攻击活动。Kimsuky组织使用该组件针对特定用户进行定向攻击，并通过对多个地址访问请求增强其溯源难度，提升自身攻击活动的隐蔽性。

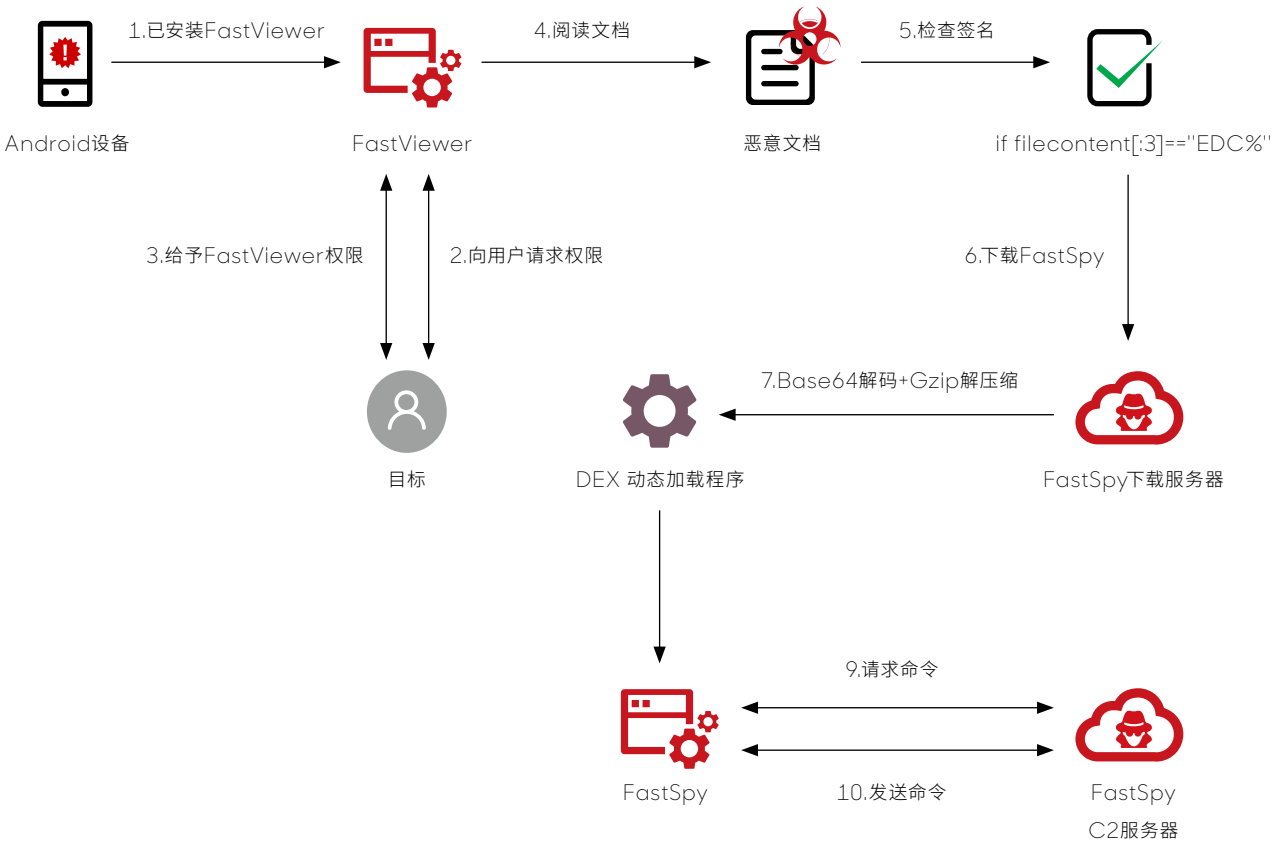
BabyShark组件于2019年2月被发现应用于针对目标国家安全智库和学术机构的攻击活动，后续也被发现用于从事核安全和朝鲜半岛国家安全问题的间谍活动，BabyShark组件主要用于收集目标的敏感信息。



利用BabyShark组件攻击流程图

2022年10月，Kimsuky组织被披露在攻击中使用了三种针对Android设备的恶意软件，分别命名为FastFire、FastViewer和FastSpy。FastFire恶意软件伪装成谷歌安全插件，从谷歌支持的应用开发平台Firebase接收命令；FastViewer恶意软件伪装成“Hancom Office Viewer”，从受感染终端窃取信息后下载其他恶意软件；FastSpy是基于开源AndroSpy的远程访问工具，由FastViewer下载释放，通过TCP/IP协议从攻击者的服务器接收命令。

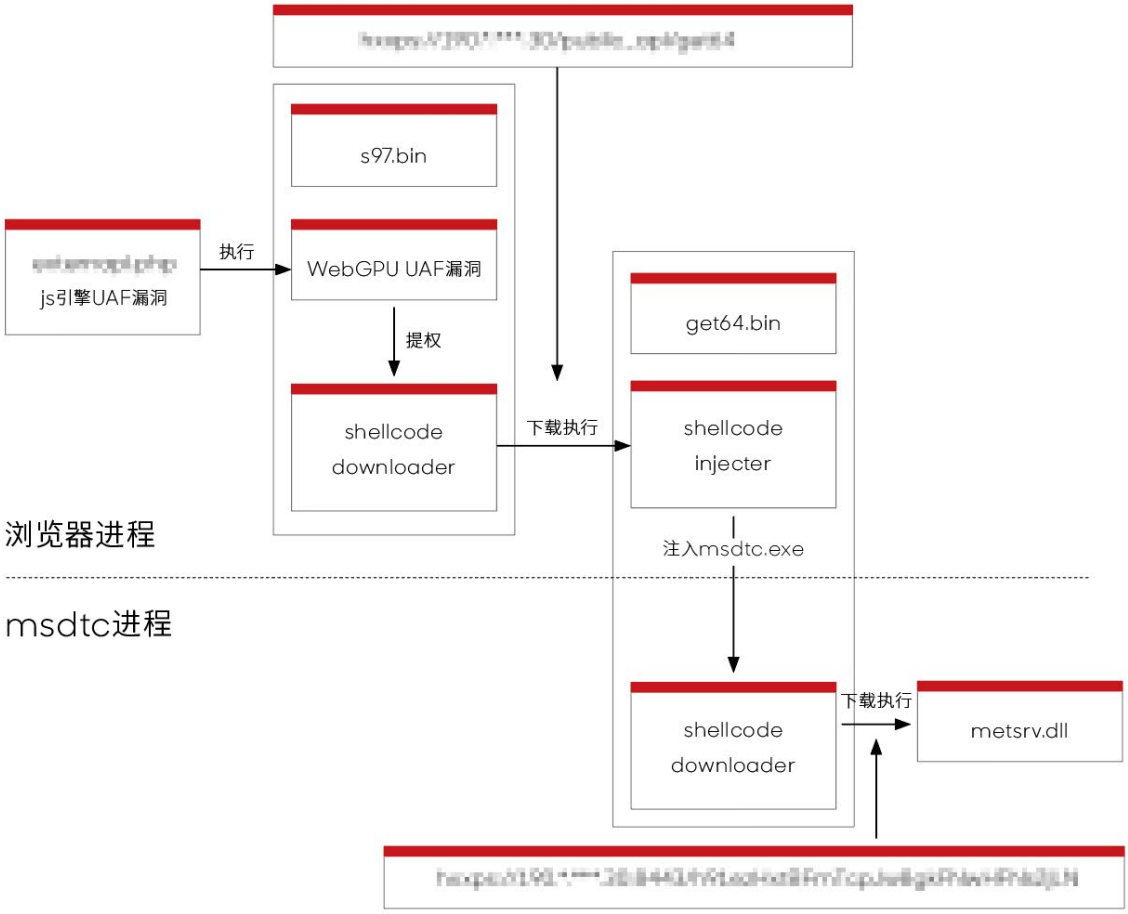
Kimsuky组织正不断面向移动终端展开攻击，Kimsuky组织针对移动终端的攻击战术和策略会越来越先进，未来需要注意防范Kimsuky组织可能向Android移动终端展开的复杂攻击。



FastViewer和FastSpy整体流程

APT-C-06 (DarkHotel)

APT-C-06 (Darkhotel) 组织在2022年，依旧保持高频率的漏洞使用。继2021年Darkhotel组织在UMK攻击行动中利用IE浏览器0day漏洞发起水坑攻击后，2022年上半年该组织又一次使用最新Firefox 0day漏洞发起水坑攻击。360高级威胁研究院率先捕获到这两个Firefox 0day浏览器漏洞：CVE-2022-26485、CVE-2022-26486。shellcode的执行路径如下图所示：



攻击者通过向目标网站嵌入恶意代码，投递浏览器漏洞发起水坑攻击。恶意js代码通过执行一系列请求，最终执行漏洞代码。

shellcode的执行路径

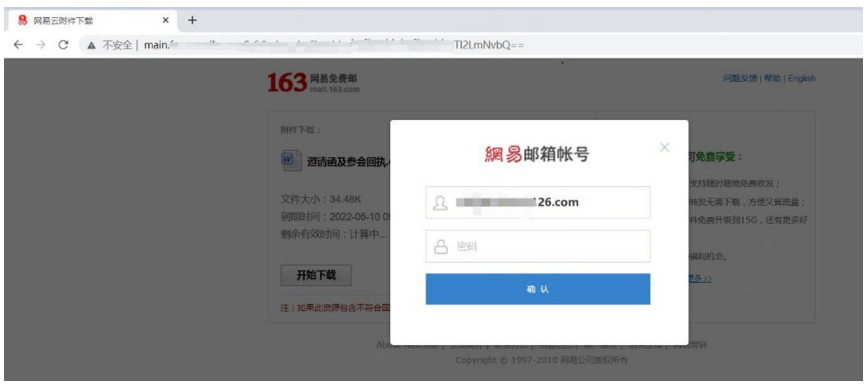
东亚-其他地区 | Advanced Persistent Threat

2022年东亚其他地区活跃APT组织，主要为APT-C-01（毒云藤）、APT-C-12（蓝宝菇）。毒云藤组织在2022年攻击活动频次和受其攻击影响的单位较2021年明显增多，被攻击目标单位集中于科研单位和教育机构。蓝宝菇组织2021年下半年针对我国重点领域单位开始的定向攻击活动持续至今，仍不断有新增受影响用户。其他如APT-C-59（芜琼洞）、APT-C-62（三色堇）等2021年较为活跃的APT组织，在2022年整体活跃度有所降低，这符合APT组织以往针对特定领域展开短期集中攻击活动后蛰伏的特点。

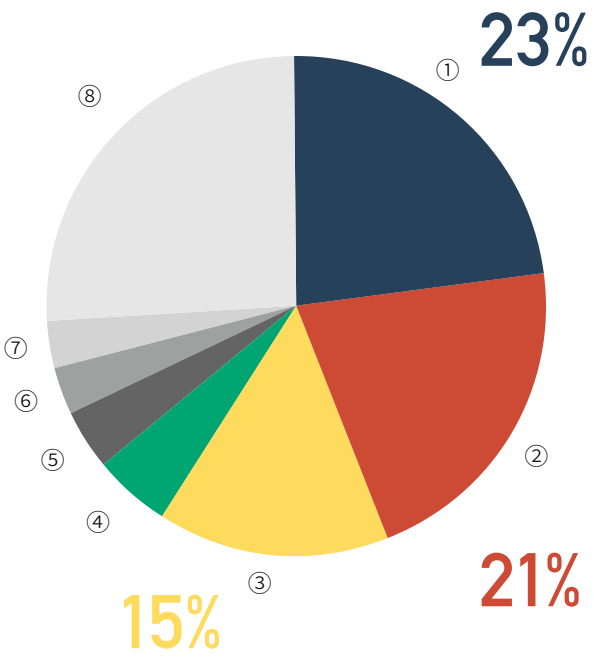
• APT-C-01（毒云藤）

APT-C-01（毒云藤）组织一直以来擅长紧跟时事热点，针对政府、国防军工、科研等多个领域的重点单位发起伪装性很强的大规模钓鱼攻击，以窃取受害者的邮箱账号密码以及其他敏感信息为目的。该组织在2022年针对我国的攻击活动持续活跃，相较于去年攻击频次和受影响单位都明显增多，更加关注科研单位和教育机构。

APT-C-01（毒云藤）组织使用的钓鱼网页一部分仿冒网易、搜狐、新浪邮箱等国内知名邮箱服务网站，通过域名包含163、mail、126等带有迷惑性的关键词，进行大规模集中钓鱼攻击活动；另一部分网页仿冒受害目标单位邮箱系统网站，域名大多包含受害单位的官方域名用以迷惑用户，在钓鱼链接中多数硬编码受害单位人员的邮箱用户名，实现定向钓鱼。并且毒云藤组织使用的诱饵文件也紧跟时事热点，如2月-3月俄乌冲突爆发后，使用“俄乌”相关话题作为诱饵文件关键词，在3月份，随着国内个人所得税申报开始，使用“个人所得税汇算清缴事项”为诱饵文件关键词进行钓鱼活动。4月份，各地推行场所码的时候，出现以 “场所码代扫”作为关键词的诱饵文档。9月份，该组织开始使用“综合防灾减灾”作为关键词的诱饵文档。



毒云藤组织仿冒的邮箱服务网站



①政策通知	23%
②项目类	21%
③报告类	15%
④科研	5%
⑤会议	4%
⑥国防军工	3%
⑦疫情防控	3%
⑧其他	26%

图1

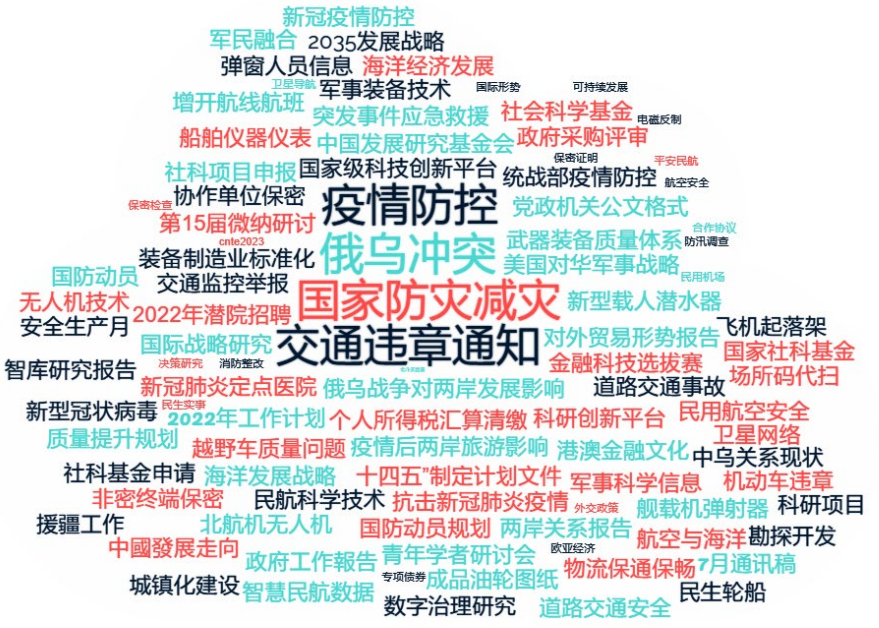


图2

图1 毒云藤组织诱饵文档类型分布统计　　图2 毒云藤组织使用的部分诱饵文档关键词

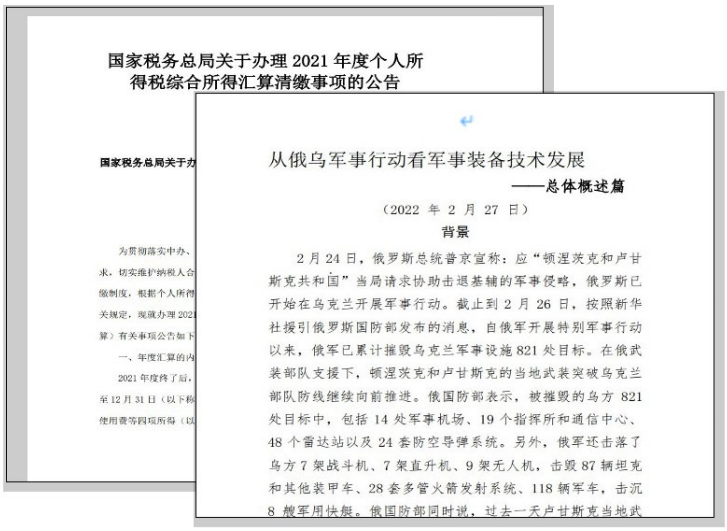


图1

360高级威胁研究院监测到APT-C-01（毒云藤）组织在2022年的钓鱼攻击活动中，更加注重自身的隐蔽性。比如降低通过钓鱼网站投递恶意附件的攻击倾向，受影响用户输入邮箱账户密码后，网站跳转下载附件或访问文章，多为正常文件；另外将文件名、邮箱名硬编码到钓鱼链接中，并且链接携带校验码，在钓鱼页面对链接加以判断，如果链接格式或者校验码错误，跳转至404页面，并且在同一个钓鱼域名下存放不同的文件，根据链接携带的文件名和文件ID可以下载不同的文件，以此来对抗安全技术人员的探测和发现。

```
var getUrlString = location.href;
var url = new URL(getUrlString);
var prodId = url.searchParams.get('id');
var fileId = url.searchParams.get('filename');
var ckId = url.searchParams.get('ck');
var dkId = url.searchParams.get('dk');
var email = url.searchParams.get('mail');

if(!prodId || 0 === prodId.length || prodId.length<31) {
   window.location.href='https://mail.163.com/404';
}

if(!email || email.indexOf("@") == -1 || !(email.includes("126.com") || email.includes("163.com") || email.includes("beidou.org"))) {
   window.location.href='https://mail.163.com/404';
}

if(!fileId) {
   window.location.href='https://mail.163.com/404';
}

if(!ckId && !dkId) {
   window.location.href='https://mail.163.com/404';
}

document.getElementById("login_btn").addEventListener("click", function( event ) {
    var href = "login.html?"+"id="+prodId+"&filename="+fileId+"&mail="+email+"&ck="+ckId;
    window.location.href = href;
}, false);
```

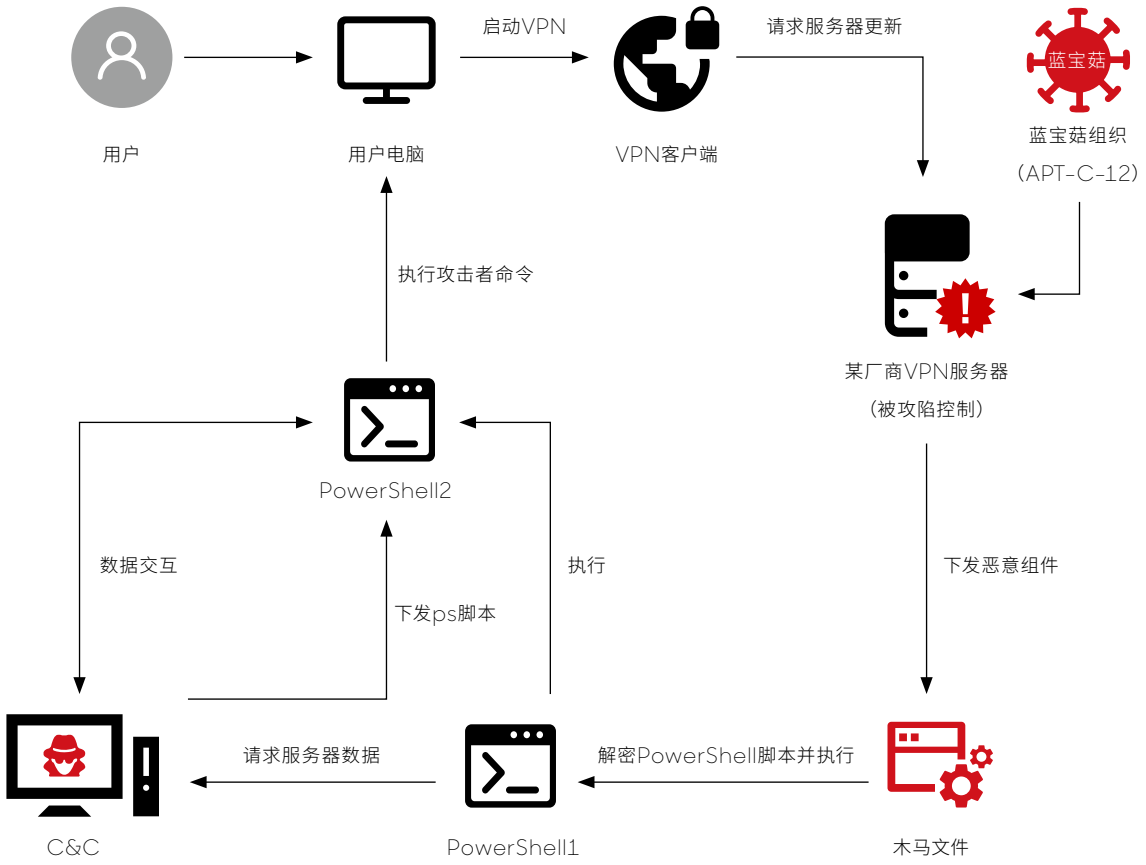
图2

图1 捕获毒云藤组织部分诱饵文件示例　　图2 钓鱼网页部分源码

• APT-C-12 (蓝宝菇)

APT-C-12 (蓝宝菇) 组织自被披露以来，长期对我国国防、政府、科研、金融等重点单位和部门进行持续网络间谍活动。该组织从2020年活跃度逐渐减弱，蛰伏近一年，在2021年10月展开了一系列针对我国通信、国防军工等多个领域重点单位的攻击活动。一直到2022年，仍有受其恶意文件影响的用户，相较2021年已明显减少。相关攻击活动主要采用控制基础网络设施来进行突破渗透，主要是针对国内某安全厂商VPN产品，攻击手法与2020年4月APT-C-06 (DarkHotel) 对某厂商VPN产品漏洞的利用非常相似。

相关恶意组件与之前攻击活动中的Winsta_Dropper属于同一家族，主要在攻击手法、解密算法密钥和C2服务器方面进行了更新，并且增加了对360安全防护产品的对抗策略。



APT-C-12 (蓝宝菇) 利用某厂商VPN攻击流程

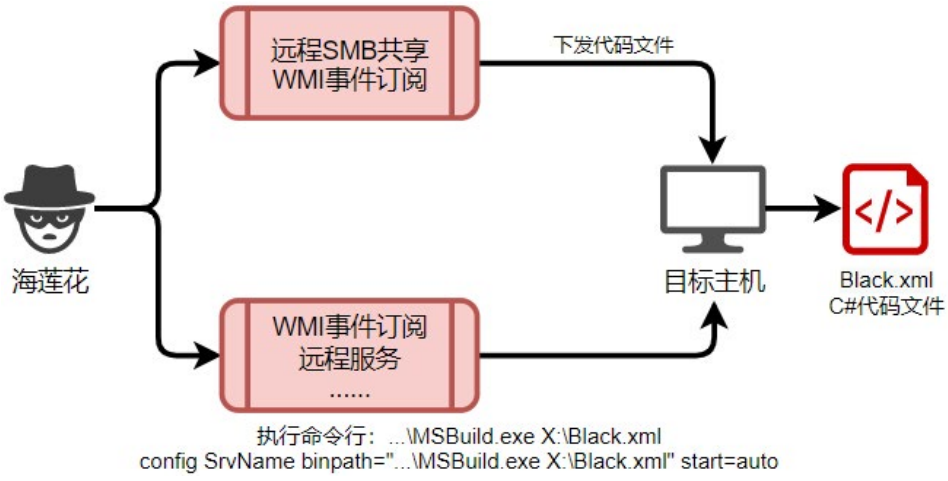
东南亚 | Advanced Persistent Threat

2022年，东南亚地区活跃APT组织主要为APT-C-00（海莲花）。海莲花组织延续对我国各重点行业领域活跃攻击的势头，受其攻击影响较为严重的是政府机构、ICT供应商等领域。

• APT-C-00（海莲花）

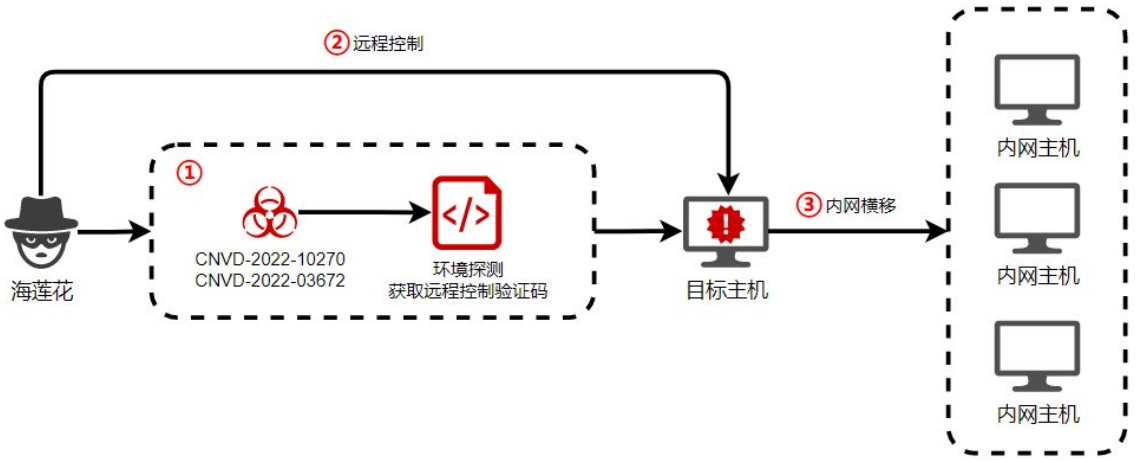
海莲花组织在2022年的攻击活动中依旧延续了白利用方式，除了其惯用的利用有效数字签名文件加载恶意DLL文件外，更加注重同安全软件和安全技术人员的对抗，以提高自身的隐蔽性。

海莲花在2022年初的攻击活动中主要以MSBuild实时编译XML格式的C#代码文件为主，首先MSBuild程序自带有效数字签名，其次是将载荷以代码文本文件的形式进行实时编译执行，以此来对抗安全软件。



海莲花组织使用的实时编译恶意载荷文件

2022年2月底，海莲花在攻击活动中利用了在2022年2月披露的向日葵软件RCE漏洞（CNVD-2022-10270，CNVD-2022-03672），进行大面积渗透攻击，主要利用RCE漏洞进行攻击环境探测，获取并解密远程控制验证码，最终通过向日葵远程控制完成初期攻击部署，随后进行内网横向移动并实现对受影响主机的持续控制。而在2022年下半年，360高级威胁研究院监测到海莲花组织利用下半年披露的商业渗透测试框架CobaltStrike的RCE漏洞CVE-2022-39197，对使用低版本CobaltStrike的相关人员展开攻击活动。



海莲花组织在利用远程控制功能实施攻击时，首先通过关闭终端安全软件的自启动，确保攻击活动隐蔽性的同时也保证了攻击载荷能够顺利运行；其次将攻击载荷所在目录加入终端安全软件的信任区，即便用户启动安全软件，如果不人为检查安全软件信任区或安全日志也很难发现异常。而且攻击载荷多为开源加载器，涉及C/C++、C#、Nim、Pascal等多种语言，由于开源的缘故且涉及多种编程语言，在一定程度上加大了安全人员的分析和研判难度，使其在受控终端更难以被发现。

海莲花在2022年攻击活动使用的网络资产大多为境内地区的IoT设备，在利用漏洞获得IoT设备的控制权后，将开源的端口转发程序植入IoT设备当作跳板，以此将流量转发至境外网络资产，提高了境外攻击的隐蔽性。同时海莲花的境外网络资产也针对访问其的IP地域归属做了限制，一定程度增加了安全人员挖掘和捕获攻击者网络资产的成本和难度。而在2022年下半年，随着相关IoT厂商的漏洞逐渐修复，被当作跳板利用的IoT设备数量呈下降趋势，海莲花组织的攻击频率也有所降低。

海莲花利用远程控制软件漏洞进行攻击示意图

东欧 | Advanced Persistent Threat

2022年爆发的俄乌冲突成为国际社会关注的焦点，两国在网络战场的对抗活动，伴随着军事冲突的发展而不断出现。一系列网络攻击对抗活动也引发了广泛的关注，网络空间也已经成为了俄乌间对抗的重要战场。

俄乌冲突发生前后，多个东欧背景的APT组织异常活跃，新启用的网络资源数量也大幅增加，如APT-C-13 (SandWorm) 、APT-C-25 (APT29) 等，运用各种技术手段，持续对相关目标发动各类攻击。主要包括东欧地区相关政府和媒体组织、互联网基础设施和数字网络服务的分布式拒绝服务攻击和破坏攻击。而针对俄罗斯的DDoS攻击从2月7日就开始，数量呈不断增加趋势。

俄乌冲突背景下的一系列网络攻击活动旨在通过网络攻击，在敌对方制造混乱、阻碍通信、削弱军事反应速度，降低军民士气，并借机窃取情报信息。

1月10日

360捕获到处于测试阶段的WhisperGate

1月15日

微软公开披露观察到伪装成勒索软件的数据擦除器攻击

1月31日

相关安全厂商披露APT组织Gamaredon针对东欧地区的定向攻击活动

2月12日

360截获Mirai、Gafgyt、ripprbot、moobot等僵尸网络攻击指令

2月18日

360捕获Gamaredon组织启动多个新的基础设施对相关目标发起攻击，包括政府机构、医疗、军事后勤等

2月24日

ESET披露数据擦除器攻击（HermeticWiper），并且有黑客组织开始泄露政府机构网站的数据库

2月26日

疑似北美背景的匿名者黑客组织和个体开始组织针对东欧地区的无差别网络攻击

3月5日

俄罗斯国家计算机事故协调中心 (NKTsKI) 公布了一份包含17576个IP地址和166个域的列表，称这些地址针对信息资源发起了DDOS攻击

3月11日

乌克兰Cert发布了APT组织UAC-0056相关攻击活动报告

3月15日

ESET新发现一种新型数据擦除软件：CaddyWiper

3月16日

乌克兰Cert披露了疑似APT28组织的邮件钓鱼活动

4月4日

Gamaredon组织以“俄罗斯联邦战犯信息”为诱饵发起鱼叉邮件攻击

4月10日

NB65黑客组织使用Conti勒索软件的修改版本发起网络攻击

4月12日

SandWorm使INDUSTROYER2和CADDYWIPER恶意软件攻击能源设施目标

5月3日

GhostWriter通过凭据钓鱼攻击Gmail账户

5月6日

APT28使用CredoMap_v2恶意软件发起攻击

5月10日

Gamaredon利用GammaLoad.PS1_v2向东欧地区目标单位发起攻击

6月30日

GhostWriter向东欧地区国家发起攻击

7月8日

APT29利用EnvyScout恶意软件发起网络攻击活动

7月19日

Turla组织利用Android恶意软件发起攻击

8月15日

微软破坏COLDRIVER组织发起的网络钓鱼行动

8月17日

黑客攻击东欧某国核电运营商网站

9月19日

SandWorm组织冒充电信公司传播恶意软件

11月8日

APT29针对欧洲外交机构的攻击活动中滥用Windows凭据漫游功能

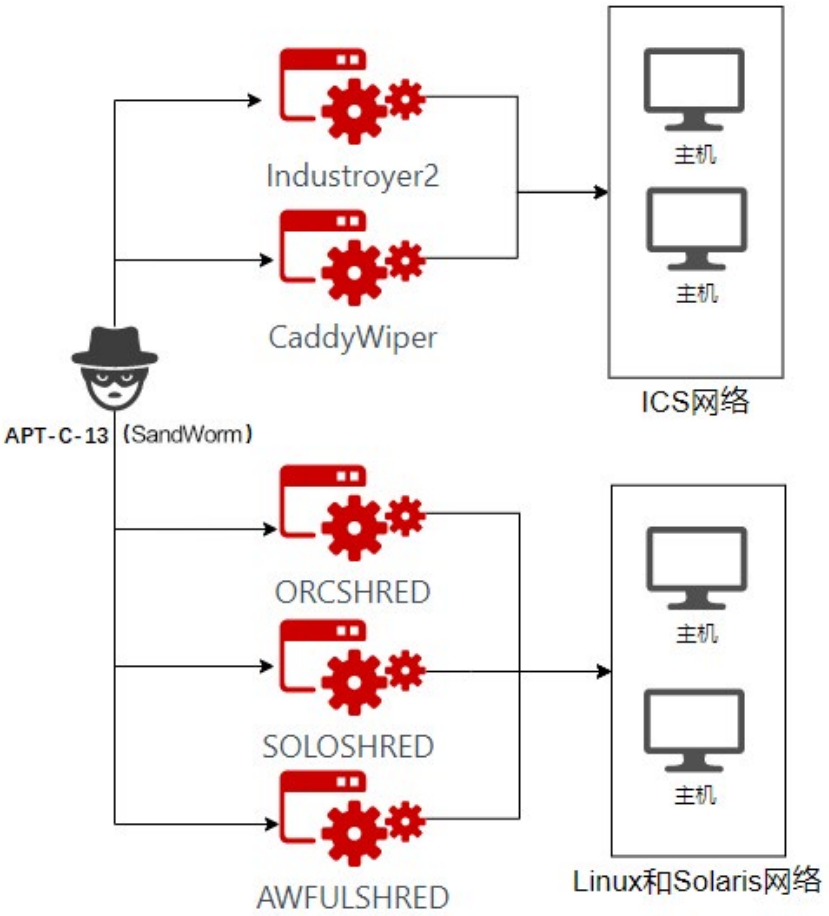
12月9日

CloudAtlas组织对东欧地区发起攻击活动

• APT-C-13 (SandWorm)

APT-C-13 (SandWorm) 是一个东欧背景的具有破坏性的APT组织，该组织在俄乌冲突爆发期间，攻击活动较以往明显活跃。2022年4月开始，该组织向东欧地区能源领域目标投递了Industroyer2[24]，该恶意程序实现了IEC-104 (又名IEC 60870-5-104) 协议来与工业设备通信。为了配合在ICS网络中部署Industroyer2，攻击者部署了新版本的具有破坏性的恶意擦除软件CaddyWiper，试图阻止能源公司运营商对ICS的控制权。

SandWorm组织还在2022年的攻击活动中，使用了针对Linux 和Solaris 系统的恶意擦除软件。该恶意软件主要由蠕虫和擦除器构成，蠕虫在Bash环境下利用计划任务启动擦除器软件，并扫描局域网主机利用内置凭据进行传播。

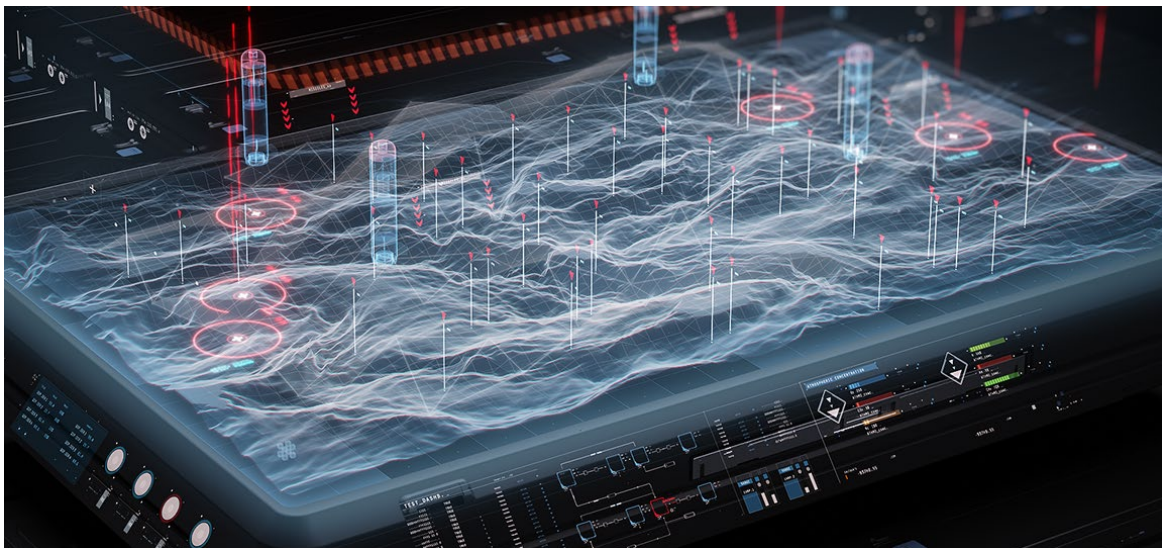


SandWorm组织所使用的恶意软件

• APT-C-20 (APT28)

APT-C-20 (APT28) 又称FancyBear，长期以来活跃在欧亚大陆地区，擅长使用鱼叉攻击进行网络钓鱼。该组织的zebrocy家族木马长期以来作为第一阶段载荷被大范围投递，其语言版本包括C++、Delphi、Nim和go。2022年5月，名为CredoMap的后门程序被披露，该程序采用.net平台，会尝试窃取当前计算机中常见浏览器的账号密码、cookie等信息，并发送到远程服务器。2022年5月末，Office组件远程执行漏洞CVE-2022-30190披露后，出现多起在野利用攻击。我们持续监测发现APT28组织也利用该漏洞进行相关载荷下发和执行。

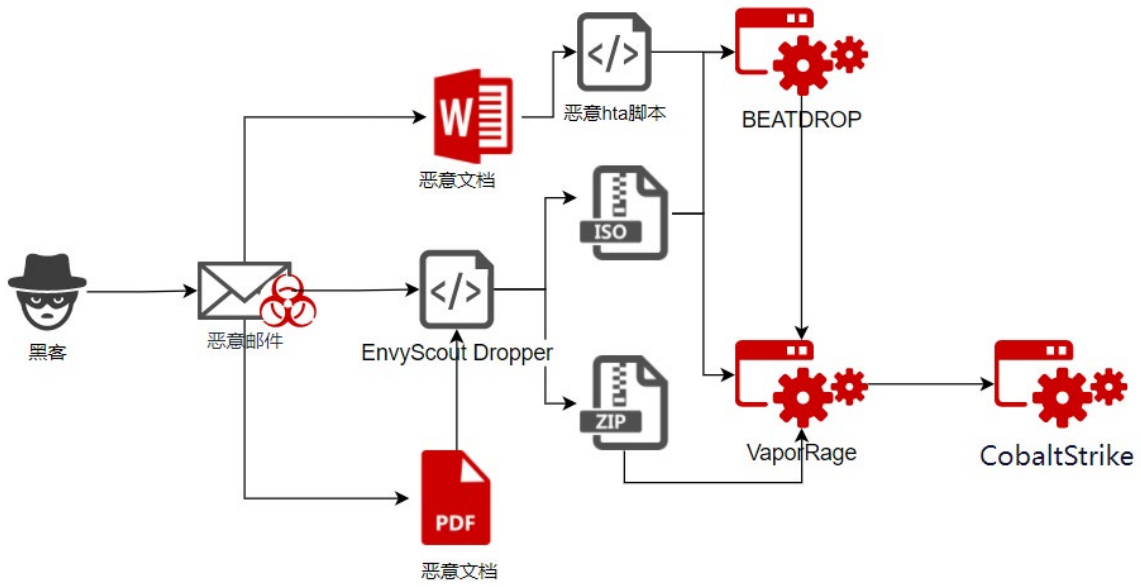
```
while (true)
{
    try
    {
        File.Copy(Environment.GetFolderPath(Environment.SpecialFolder.LocalApplicationData) + "\\Google\\Chrome\\User Data\\Default\\Network\\Cookies", "cc", overwrite: true);
    }
    catch
    {
        Thread.Sleep(10000);
        continue;
    }
    break;
}
SQLiteConnection val = new SQLiteConnection("Data Source=cc");
((DbConnection)(object)val).Open();
SQLiteCommand val2 = new SQLiteCommand("SELECT host_key, name, encrypted_value FROM cookies", val);
SQLiteDataReader val3 = val2.ExecuteReader();
while (((DbDataReader)(object)val3).Read())
{
    byte[] array = (byte[])((DbDataReader)(object)val3)["encrypted_value"];
    string text = File.ReadAllText(Environment.GetEnvironmentVariable("APPDATA") + "/../Local/Google/Chrome/User Data/Local State");
    text = ((object)JObject.Parse(text).get_Item("os_crypt").get_Item((object)"encrypted_key")).ToString();
```



CredoMap后门代码片段

• APT-C-25 (APT29)

2022年，APT-C-25 (APT29) 组织攻击活主要针对欧洲相关重点目标，尤其是政府和外交事务部门。其攻击技战术主要通过伪装成与各个大使馆相关的行政通知类钓鱼邮件，向目标主机投递EnvyScout Dropper或EnvyScout Dropper的诱饵文档，并利用EnvyScout Dropper向目标主机投递IMG/ISO/压缩文件，进而打开IMG/ISO文件或压缩文件，运行BEATDROP恶意程序，获取并投递VaporRage，继而利用合法软件侧加载VaporRage，或者直接利用合法软件加载VaporRage，之后再投递CobaltStrike载荷进一步控制目标主机。



EnvyScout执行流程图

• APT-C-53 (Gamaredon)

APT-C-53 (Gamaredon) 组织是一个有东欧政治背景的APT组织，该组织长期以来保持着对东欧地区目标的活跃攻击。360安全大脑监测到在俄乌冲突期间，Gamaredon组织异常活跃，自2月起，启用多个新的基础设施对东欧地区相关目标发起攻击。

Gamaredon组织从2022年3月份开始，向多个东欧地区受控设备下发并执行了DDoS组件。该组件源于一个名为LOIC的开源.net平台的DDoS木马，其下发途径为历史受感染机器中的vbs脚本及powershell指令。受攻击的IP及端口以硬编码形式写在代码中，通过分析推断现阶段相关组件的下发仅用于测试活动。

```
// PS5.Program
using System;
using System.Windows.Forms;

[STAThread]
private static void Main(string[] cmdLine)
{
    bool hive = true;
    bool hide = true;
    string ircserver [redacted]
    string ircport = [redacted]
    string ircchannel = "#loic";
    int num = 0;
    foreach (string text in cmdLine)
    {
        if (text.ToLowerInvariant() == "/hidden")
        {
            hide = true;
        }
        if (text.ToLowerInvariant() == "/hivemind")
        {
            hive = true;
        }
        num++;
    }
    Application.SetCompatibleTextRenderingDefault(defaultValue: false);
    Application.Run(new frmMain(hive, hide, ircserver, ircport, ircchannel));
}
```

DDoS木马代码片段

2022年5月以来，360高级威胁研究院陆续发现了Gamaredon组织在攻击活动使用的以俄乌冲突话题作为诱饵的html样本，样本中嵌有js脚本，通过浏览器打开该html页面后会启动带有恶意lnk文件的压缩包的下载任务。

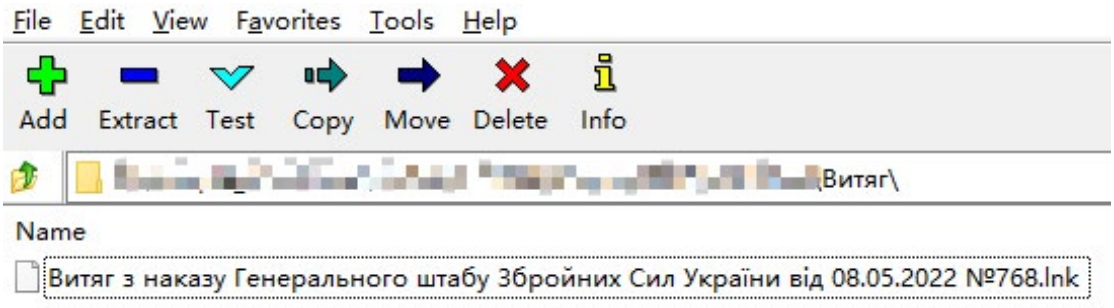


图1

Витяг з наказу Генерального штабу Збройних Сил Укра ни в д 08.05.2022 №768（翻译：摘自乌克兰武装部队总参谋部 2022年5月8日№768的命令）。

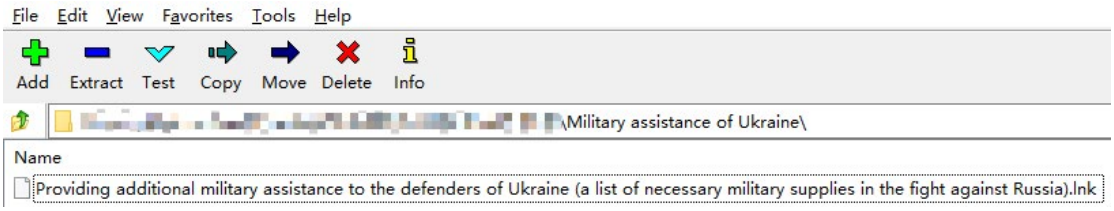


图2

Providing additional military assistance to the defenders of Ukraine (a list of necessary military supplies in the fight against Russia)（翻译：向乌克兰的捍卫者提供额外的军事援助（对抗俄罗斯的必要军事物资清单））

图1 包含诱导性标题的恶意lnk示例1　　图2 包含诱导性标题的恶意lnk示例2

其他 | Advanced Persistent Threat

2022年，全球除上述地域范围外，中东和南美地区APT组织网络攻击和对抗活动也保持较高热度，中东地区的网络攻击尤其活跃。

2022年初，MuddyWater组织利用Telegram恶意软件对中东地区国家政府和全球其他地区的政府和商业网络展开了一系列攻击活动。2022年下半年，中东地区APT组织攻击活动频繁，先是对欧洲地区目标政府机构发起攻击，随后在攻击活动中利用漏洞展开了数据勒索和磁盘加密攻击。与此同时，中东部分地区的金融、制造等相关企业也在2022年遭受了有组织的网络攻击，成为网络攻击的受害者。

2021年12月Apache Log4j2核弹级漏洞事件曝光后[25]，360高级威胁研究院预测APT组织将会利用Log4j2漏洞展开攻击活动。2022年APT35组织利用Log4j2漏洞分发新的模块化PowerShell工具包，并在3月开发了新的PowerShell后门PowerLess，同样中东背景的APT组织TunnelVision组织也在后续的攻击行动积极利用Log4j2漏洞发起攻击。

受到中东地区地缘政治事件的影响，APT34组织利用新的Saitama后门，向目标发起攻击活动。与APT34可能属于同一组织的Lyceum组织也活动频频，先是针对高科技芯片行业发起攻击活动，随后又对中东发起攻击，攻击的同时频繁对其攻击组件进行更新。

• APT-C-23 (双尾蝎)

APT-C-23 (双尾蝎) 又被称为AridViper、Micropsia、FrozenCell、Desert Falcon，是一个以窃取敏感信息为主的网络攻击组织，该组织具备针对Windows与Android双平台的攻击能力，习惯利用以政治、军事等热点敏感话题为主题的网络钓鱼邮件对中东地区相关国家的教育机构、军事机构等领域展开攻击。

2022年，双尾蝎组织被披露持续针对阿拉伯语国家相关目标发起攻击，包含一系列利用政治主题的网络钓鱼攻击活动。360高级威胁研究院监测到双尾蝎在攻击活动中，将商业RAT伪装成开源的端到端加密即时通讯应用程序Threema，诱使用户点击打开。以前的双尾蝎样本大多采用VC版本、Delphi版本，此次使用公开商业RAT组件进行攻击的行为，可能是该组织正在进行攻方式的演变，也可能是双尾蝎组织内部新分支成员所采用的攻击手法。

在2022年世界杯期间，360高级威胁研究发现双尾蝎组织将攻击样本伪装成世界杯相关应用针对阿拉伯语用户发起攻击，攻击者主要通过制作精良的阿拉伯语钓鱼网站进行载荷投递，利用Facebook账号传播钓鱼网站，诱导受害者下载安装恶意应用。双尾蝎组织使用了以往攻击活动中相似钓鱼页面源码与相同的文件命名方式，并适配了移动端和PC端。值得注意的是，双尾蝎组织针对世界杯的攻击活动并非首次出现，早在2018年俄罗斯世界杯期间，双尾蝎组织就通过仿冒世界杯相关应用对巴以地区实施网络攻击。

图1

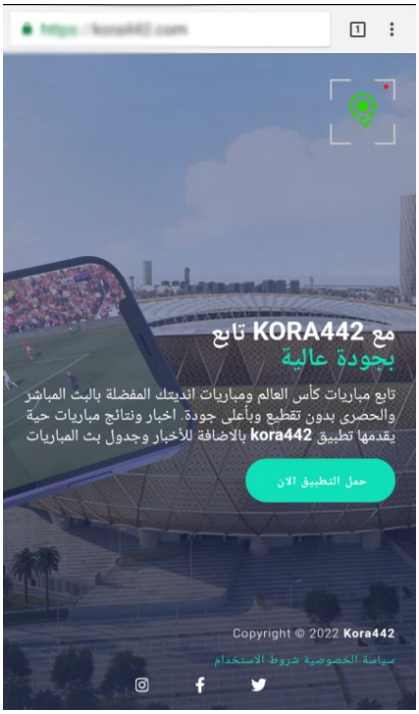


图2

图3

图1 双尾蝎传播钓鱼网站的帖子　　图2 移动端双尾蝎钓鱼网站显示内容　　图3 PC端双尾蝎钓鱼网站显示内容

• APT-C-36 (盲眼鹰)

APT-C-36 (盲眼鹰)，是疑似来自南美洲的APT组织，该组织攻击目标也主要是南美地区政府机构，自身也会通过伪装成相关部门、仿冒政府网站展开钓鱼或鱼叉攻击。

2022年，360高级威胁研究院监测到了多次针对目标机构的钓鱼邮件定向攻击，在攻击行动中，RAR解压密码和下载链接常通过PDF伪装文档提供，攻击者诱导受害者点击实为恶意短链接的网址，进一步诱导用户下载并打开恶意文件，由于样本都经过层层解密释放，加大了传统查杀的难度。通过样本内部解密算法关联，我们判断两次行动归属于盲眼鹰组织。

SIMIT
Sistema Integrado de Información sobre multas y sanciones por infracciones de tránsito

Bogotá D.C, 11 DE ABRIL 2022

SECRETARIA DISTRICTAL DE MOVILIDAD Y SEGURIDAD VIAL

ASUNTO: COBRO COACTIVO.

Por medio del presente comunicado se le notifica que en su contra quedo ejecutoriado un comparendo por foto multa con radicado 0012-0057 adeudado por un valor de **2`150.000 pesos M/CTE con mora de 28 dias.**

Tenga en cuenta que el objetivo de este procedimiento es recaudar el pago forzado de los recursos o multas fiscales de tránsito en favor de la administración pública, por medio de **los bienes que se encuentren a nombre del titular de dicha infracción.**

Por lo anterior consulte la información detallada del comparendo en el siguiente enlace:

Por seguridad digitar la contraseña: **2022**

Cordialmente;

María Del Pilar López Sierra
Secretaria

两次攻击活动都采用了邮件投递第一阶段的载荷，第一次行动通过伪装DHL包裹投递，使用出货通知单为主题来迷惑中招目标；第二次投递伪装成政府邮件，发送伪装成PDF文件的恶意文档。完成载荷投递后，通过自解密得到可执行文件， 展开进一步的窃密和攻击行动。

带有恶意文件下载链接的pdf文档

全球高级持续性威胁研究报告
RESEARCH REPORT

2022 /
PART.03

2022年APT攻击态势总结

2022年APT攻击态势总结

Advanced Persistent Threat

1. TOP20 ATT&CK技战术

360高级威胁研究院综合分析全球安全厂商2022年公开披露的APT报告，针对业界披露的对于APT组织符合ATT&CK知识标准的攻击技术进行了分析统计，给出了APT组织在2022年攻击活动过程中使用最为集中的TOP20 ATT&CK技战术。

ATT&CK技术编号	技战术名称（英文）	技战术名称（中文）
T1059	Command and Scripting Interpreter	滥用命令和脚本解释器
T1071	Application Layer Protocol	应用层协议
T1566	Phishing	网络钓鱼
T1036	Masquerading	伪装白文件
T1204	User Execution	依靠用户自行执行
T1082	System Information Discovery	检测操作系统和硬件的信息
T1140	Deobfuscate/Decode Files or Information	解码加密/混淆的文件信息
T1547	Boot or Logon Autostart Execution	启动或登录时自动执行
T1027	Obfuscated Files or Information	混淆文件或信息
T1083	File and Directory Discovery	收集文件和目录信息

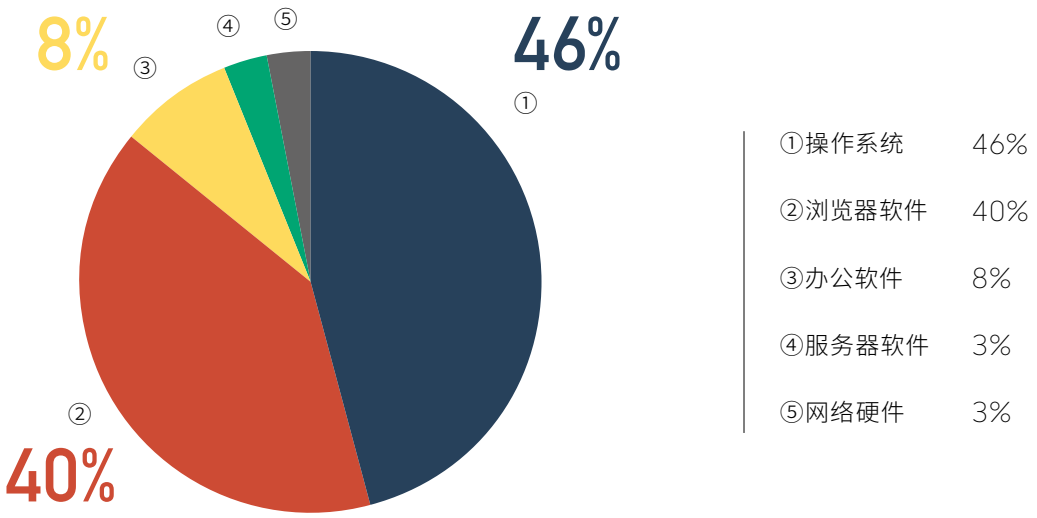
ATT&CK主技术	英文	翻译
T1573	Encrypted Channel	使用已知加密算法
T1041	Exfiltration Over C2 Channel	通过C2渗透通道
T1070	Indicator Removal	删除主机上的痕迹
T1560	Archive Collected Data	打包收集的数据
T1053	Scheduled Task/Job	计划任务/工作
T1105	Ingress Tool Transfer	从外部系统转移文件
T1021	Remote Services	登录远程服务
T1003	OS Credential Dumping	获取系统转储凭据
T1057	Process Discovery	收集正在运行的进程的信息
T1055	Process Injection	代码注入

2.利用0day漏洞的攻击活动增长势头放缓，但仍处高位

基于Google Project Zero项目统计，2022年APT攻击活动被披露利用的0day漏洞共计36个[26]，涉及7个厂商的13个产品。虽然比2021年披露的APT攻击利用的0day漏洞大幅减少，但漏洞利用数量仍处于高位。360高级威胁研究院对2022年全球范围APT组织攻击活动进行分析：全年APT攻击活动中利用的0day和Nday漏洞近70个，涉及超过40个APT组织。

2022年2月，360高级威胁研究院全球范围内率先捕获到APT-C-06（DarkHotel）组织利用Firefox浏览器的2个在野0day漏洞（CVE-2022-26485、CVE-2022-26486）针对特定目标进行水坑攻击。这也是2022年国内唯一一家捕获APT攻击活动中利用0day漏洞的安全厂商。2017年至今，360捕获的APT组织攻击使用的在野0day漏洞数量，连续6年位居国内第一。

通过对2022年APT组织在攻击活动中利用的0day漏洞进行分析，得出以下类型分布：



2022年上半年0day漏洞产品类型分布

厂商	涉及产品	CVE漏洞编号
Apple	iOS	CVE-2022-22587
		CVE-2022-42827
	iOS/macOS	CVE-2022-22675
		CVE-2022-32894
		CVE-2022-32917
	macOS	CVE-2022-22674
	WebKit	CVE-2022-22620
		CVE-2022-32893
		CVE-2022-42856
Atlassian	Confluence Server & Data Center	CVE-2022-26134
Google	Chrome	CVE-2022-0609
		CVE-2022-1096
		CVE-2022-1364
		CVE-2022-2294
		CVE-2022-2856
		CVE-2022-3075
		CVE-2022-3723
		CVE-2022-4135
		CVE-2022-4262
	Pixel	CVE-2021-22600
		CVE-2021-39793

厂商	涉及产品	CVE漏洞编号
Sophos	Firewall	CVE-2022-1040
Mozilla	Firefox	CVE-2022-26485
		CVE-2022-26486
Microsoft	Exchange Server	CVE-2022-41040
		CVE-2022-41082
	Internet Explorer	CVE-2022-41128
	Windows	CVE-2022-21882
		CVE-2022-24521
		CVE-2022-26925
		CVE-2022-30190
		CVE-2022-22047
		CVE-2022-41033
		CVE-2022-41073
		CVE-2022-41125
Trend Micro	Apex Central	CVE-2022-26871

01. APT攻击呈现利用0day漏洞修复不全或者0day漏洞变种发起攻击的趋势

在APT组织攻击活动中掌握0day漏洞意味着获得了目标系统的控制权限。但0day漏洞复用性低、易泄露，目前主要靠漏洞挖掘人才进行挖掘。近期网络武器0day漏洞价格大幅攀升，某漏洞收录平台对高风险漏洞甚至开出了数百万美金的高额赏金，0day漏洞成为APT组织越来越稀缺的战略资源。在2022年APT组织在攻击活动中，展现出利用漏洞修复不全或者0day漏洞变种来展开攻击的趋势。

通过对2022年披露的APT组织攻击活动利用的36个0day漏洞进行分析，发现至少有14个是之前修复不全或已修复漏洞的变体。由于0day漏洞的稀缺性，APT组织更加注重通过漏洞的补丁绕过等方式，充分发挥0day漏洞的价值。在野0day被修复后，攻击者利用原始0day漏洞的变体，再次发起攻击。2022年APT组织利用0day漏洞发起的攻击活动，有较大比例可通过更全面的打补丁和回归测试得以有效阻止。

面对持续披露的APT利用0day漏洞攻击，重点单位可通过持续跟踪APT组织攻击趋势，及时和全面的打补丁和回归测试，对此类攻击活动实现拦截和防御。同时，维护国家网络安全需要不断完善国家级漏洞收集和获取机制，掌握网络空间对抗的主动权。

02. APT和网络犯罪组织持续利用log4j2漏洞展开网络攻击活动

2021年12月Apache Log4j2核弹级漏洞事件曝光后，360高级威胁研究院预测APT组织利用Log4j2漏洞的攻击活动会进一步活跃。在2022年，使用Log4j2漏洞展开的网络攻击活动陆续被披露。

具有中东背景的APT35组织在年初吸引了大量的关注，其率先被披露利用Log4j2漏洞分发新的模块化PowerShell工具包，并在三月开发了新的PowerShell后门PowerLess，另外Lazarus组织等部分APT和网络犯罪组织也在上半年被披露利用Log4j2漏洞展开相关的攻击活动。

披露时间	组织	相关报告
2022年1月11日	APT35	APT35利用Log4j漏洞分发新的模块化PowerShell工具包[27]
2022年2月17日	APT35	Log4j2野外|威胁组织 “TunnelVision” 积极利用VMware Horizon[28]
2022年4月27日	Lazarus	Stonefly:与朝鲜半岛有关的间谍行动继续打击高价值目标[29]
2022年3月28日	UNC961	Forged in Fire: MobileIron Log4shell漏洞利用研究报告[30]
2022年5月12日	APT35	COBALT MIRAGE开展勒索攻击活动[31]
2022年5月12日	Lazarus	利用Log4Shell漏洞的Lazarus组织 (NukeSped) [32]
2022年8月25日	MERCURY	MERCURY组织利用未修补系统中的Log4j2漏洞发起攻击活动[33]
2022年9月8日	Lazarus	分析Lazarus组织的三个RAT[34]
2022年9月14日	CharmingKitten	APT组织利用漏洞进行数据勒索和磁盘加密[35]
2022年12月9日	CharmingKitten	分析COBALT MIRAGE的新恶意软件Drokbk[36]

3.APT组织针对移动平台私有化武器趋势显露

2022年1月，安全厂商披露了针对中东和南亚的APT组织Bahamut[37]，使用钓鱼网站投递未被披露过的移动RAT样本。该样本伪装成聊天软件，聊天功能和远控功能单独开发，聊天功能的服务器和远控功能的C2使用相同地址。样本恶意代码高度模块化编写质量高，使用数据库存储各类信息。除了窃取短信、联系人、通话记录等常见用户隐私信息外，还会借助辅助功能重点窃取大量知名社交软件的聊天信息，属于该组织的特有攻击武器。

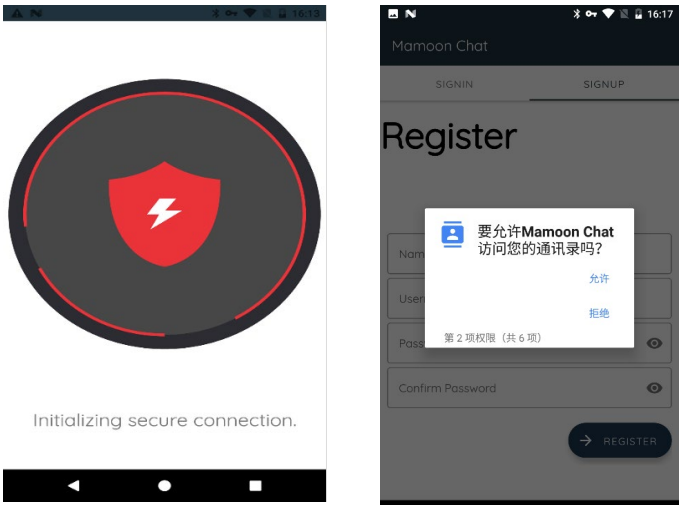


图1

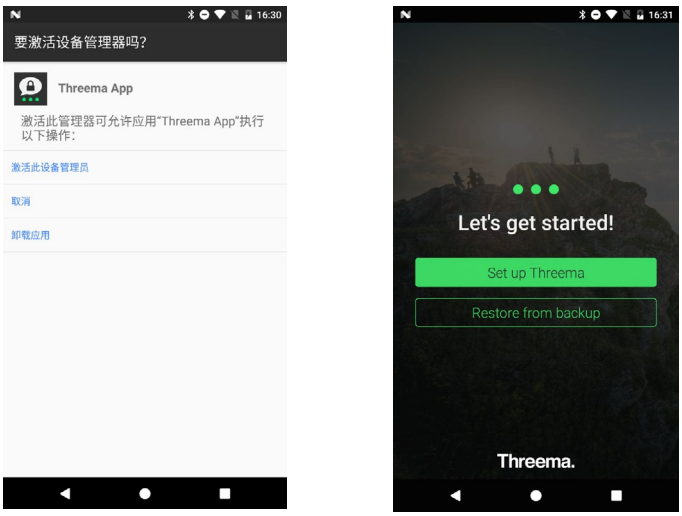


图2

图1 Bahamut组织伪装聊天软件的移动平台恶意样本　　图2 APT-C-23（双尾蝎）组织移动平台恶意软件样本

2022年上半年，我们监测到了具有间谍功能的Android植入样本VolatileVenom和VajraSpy，攻击者能够从受害终端窃取大量数据。VolatileVenom使用HTTPS和Google Firebase Cloud Messaging (FCM) 进行C2通信，同时通过链接指定网站读取网站标题和接收短信消息的方式来查询C2；VajraSpy通过将窃取到的数据存储到指定的Firebase Cloud Firestore中，包括通话记录、通讯录、短信、文档、图片以及各种知名即时通讯软件聊天记录等。

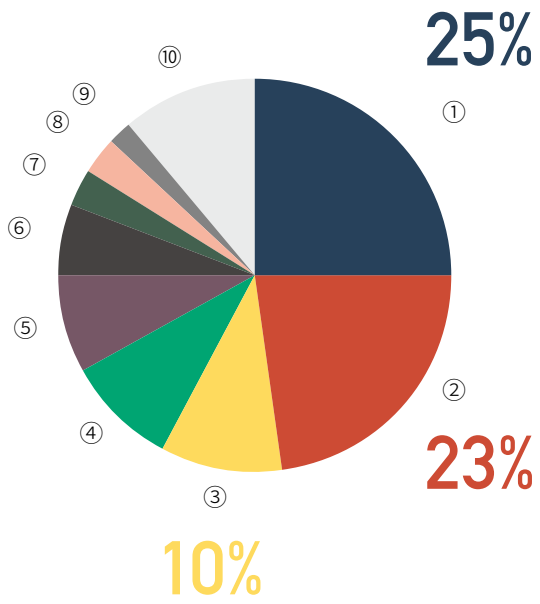
另外，在2022年，针对iOS平台的攻击活动也保持活跃。安全厂商披露了两起Pegasus监控活动[38]，主要集中在iOS用户，表明NSO Group组织在iOS平台上的攻击活动仍然活跃。

商业间谍软件供应商RCS Lab SpA和Tykelab Srl开发的Hermit间谍软件曾被发现用于针对中东和欧洲地区的攻击活动，2022年被发现在中亚地区也有部署。Hermit是一款高度可配置的监控软件，具有收集和传输数据的企业级功能，恶意功能隐藏在下载的其他有效负载中，在样本投递阶段，攻击者可能会和ISP合作以禁用目标的移动数据连接，进而向受害者发送钓鱼短信。攻击者通过将样本设置为专有内部应用分发iOS样本，样本包含多个iOS漏洞，能够窃取例如Whatsapp的数据库。

4.针对我国重点行业目标的攻击活动依然保持高热度

2022年，APT组织针对我国重点行业领域的攻击活动仍旧保持较高热度，360高级威胁研究院在2022年监测到的APT组织攻击活动中，针对中国发起的攻击活动共涉及14个APT组织，政府、教育、信息技术、科研和国防军工等15个行业领域依然是APT组织攻击活动主要的目标领域。

2022年，在全球疫情相关热点事件和话题热度在今年回落之后，360高级威胁研究院捕获到的APT攻击活动中投递使用的与“疫情防控”相关主题的钓鱼和诱饵样本，所占比例有所下降。

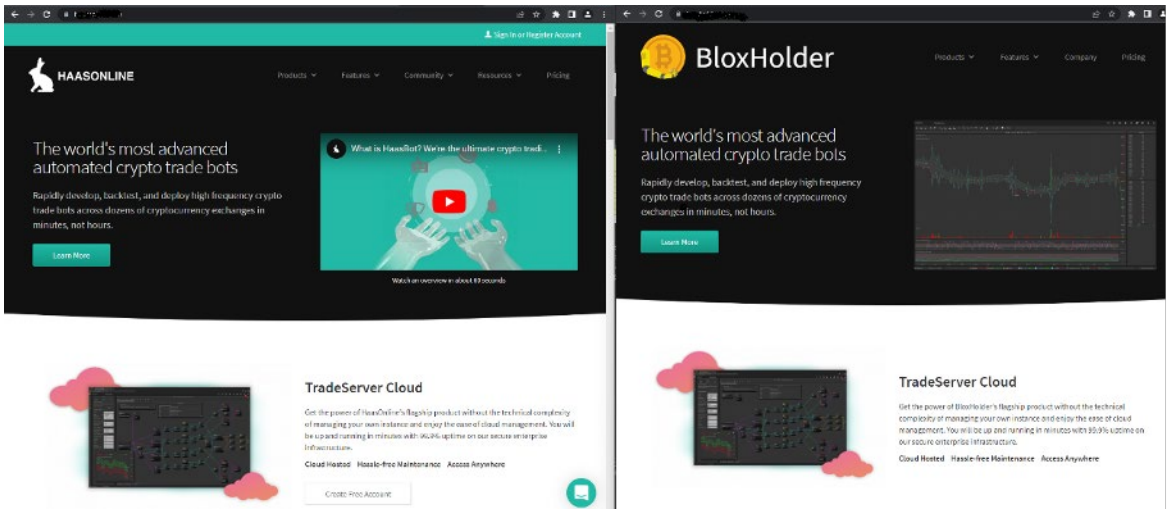


①政府	25%
②教育	23%
③信息技术	10%
④科研	9%
⑤国防军工	8%
⑥交通运输	6%
⑦制造	3%
⑧贸易	3%
⑨医疗卫生	2%
⑩其他	11%

2022年中国地区受APT攻击影响行业分布

5.涉及网络经济犯罪的APT攻击活动持续披露

2022年APT组织涉及挖矿勒索攻击、窃取加密货币等形式的攻击活动持续被披露，呈现不断上升的趋势。APT组织展开勒索攻击或窃取加密货币攻击活动的真实意图，既存在本身以牟利为目的，也包含利用勒索加密攻击做真实攻击目的掩护。2022年自朝鲜半岛地区的APT组织APT-C-26（Lazarus），通过各种攻击方式持续对金融和加密货币领域展开攻击渗透，同时其地区的APT组织，如归属中东地区的Charming Kitten组织也被披露对攻击目标展开勒索攻击活动。



加密货币交易网站与Lazarus组织克隆网站（右）

发布时间	事件描述	涉及类型
2022年1月13日	卡巴斯基披露Lazarus组织针对加密货币初创公司的攻击活动[39]	加密货币
2022年4月18日	Lazarus组织被披露攻击区块链公司[40]	加密货币
2022年4月19日	360发布隐藏在投资推介书中的淘金者——APT-C-26 (Lazarus) 攻击活动分析报告[41]	加密货币
2022年5月3日	Trellix披露与Lazarus有关的VHD勒索软件[42]	勒索攻击
2022年7月6日	朝鲜半岛组织被披露使用Maui勒索软件攻击医疗保健和公共卫生部门[43]	勒索攻击
2022年8月10日	卡巴斯基披露DeathStalker对外汇和加密货币交易所的持续攻击[44]	加密货币
2022年9月14日	SecureWorks披露COBALT MIRAGE的勒索软件活动[45]	勒索攻击

全球高级持续性威胁研究报告
RESEARCH REPORT

2022 /
PART.04

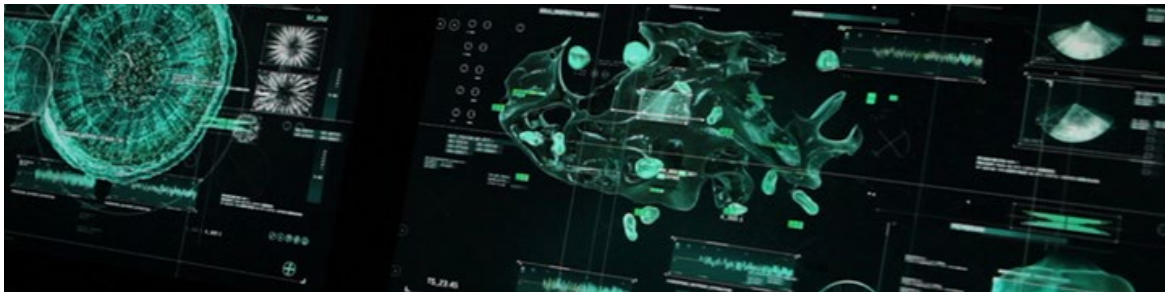
关键威胁形势分析

关键威胁形势分析

Advanced Persistent Threat

1、俄乌冲突爆发，APT攻击急剧增加

2022年俄乌冲突期间，围绕俄乌冲突这一热点地缘政治事件的网络战和信息战，从暗处走向前台呈现愈演愈烈的态势，网络战的形态初现端倪。



01.东欧APT组织异常活跃，破坏性网络攻击频发

地缘政治冲突为APT组织的攻击活动和发展提供了更为自由的空间，一直以来是APT组织和网络攻击活动和发展的关键驱动因素。在俄乌冲突期间，地缘归属东欧的APT组织异常活跃，破坏性网络攻击频发，同时像DDoS攻击、数据擦除器攻击等传统网络攻击活动也不断上演。

360高级威胁研究院监测发现，在两国网络空间对抗中，具有国家背景的APT组织以及网军攻击活动持续活跃。地缘归属东欧的一系列APT组织，在俄乌网络间对抗中活跃度大幅上升，针对东欧地区政府、能源、外交等重要目标展开的攻击活动不断被发现和披露。例如：SandWorm组织使用恶意软件针对电力系统的新一轮攻击，Gamaredon组织对相关重点目标的持续网络攻击，APT28组织针对政府部门的多轮钓鱼攻击等。

在此期间，APT组织新启用作为攻击活动的网络资源数量也大幅增加，网络空间资源的武器化成为趋势，网络战向全民战争的形式发展。包括国家、组织乃至个人都可能成为网络战的发动者和打击对象，乌克兰政府就曾呼吁地下黑客组织参与网络安全防护与攻击对抗。网络空间资源的武器化不仅会在某种程度上影响俄乌冲突的进程和走势，还将对未来网络空间国际秩序的形成产生深远的影响。

02.利用“俄乌冲突”热点事件为诱饵进行定向攻击

2022年3月以来，APT组织利用正在进行的俄乌冲突话题作为诱饵展开的定向攻击活动不断被披露。部分攻击者还存在将战争作为主题，引诱潜在受害者运行恶意代码的攻击行为。

以热点事件或话题制作诱饵文件进行恶意样本投递，是APT组织惯用的攻击手法。使用俄乌冲突相关话题展开的APT攻击活动，已经不仅限于地缘归属于东欧地区的APT组织，在中东、亚洲等世界其他地区，也不断有以俄乌冲突为话题的APT攻击事件被披露。

中东地区活跃APT组织Lyceum，使用以“俄乌”题材的文章链接，针对中东能源领域目标发起攻击[46]；APT-C-24（响尾蛇）组织，使用标题为“聚焦俄乌冲突对巴基斯坦的影响”针对相关目标展开攻击[47]；APT-C-01（毒云藤）利用“俄乌冲突”相关话题为主题的诱饵文档等多起攻击事件。

俄乌冲突的进一步发展，将对世界格局产生更加深远的影响，俄乌冲突相关的热点话题也将继续吸引全世界的关注。APT组织还将继续利用与俄乌冲突相关的热点话题，展开针对性的网络钓鱼和攻击活动。

2.保障国家网络空间安全，需时刻保持战时状态

网络空间领域的对抗，已逐渐成为地缘政治斗争，大国间博弈的主要对抗形式。网络空间领域的传统强国，往往会利用自身在网络空间技术能力和技术储备上的优势，长期对全球范围的高价值目标实施无差别的渗透攻击、远程控制和情报窃取，以此来不断扩大自身在政治、军事、外交上的优势。

2022年3月，360连续发布美国国家安全局（NSA）对全球以及我国进行网络攻击的相关报告，展示出美国持续常态化网络攻击活动。环球时报在报道中指出：“ 持续不断曝出的美国对他国的网络入侵计划早已不新鲜。如“酸狐狸平台”般构造精巧、处心积虑且长期为害的网络攻击武器，显示网络空间对抗博弈进入了新阶段。一个国家网军主力装备长期运行，本身便说明网络空间“平战”区分早已无意义[48]。我们要接受始终处于网络空间“战时”状态的现实，从应对网络战的角度做好关键信息基础设施安全保护工作。”

常态化的网络对抗不仅可以在战时配合、传统军事行动，还可以在冲突前、冲突中、冲突后持续发挥作用。俄乌冲突期间两国势力间的网络对抗，向我们呈现了网络战与热战相互交织的“混合战”走向常态化的态势。在正式军事行动前，乌克兰遭受的一系列网络攻击，使前方战场与后方指挥中心的网络通信信号被切断，进而使二者无法联系，同时通过大规模网络舆论战，开展心理战术迫使对手作出战略误判和错误决策。俄乌正面冲突不断发展的同时，俄罗斯也遭遇了全球最大的黑客组织“匿名者”的网络攻击。

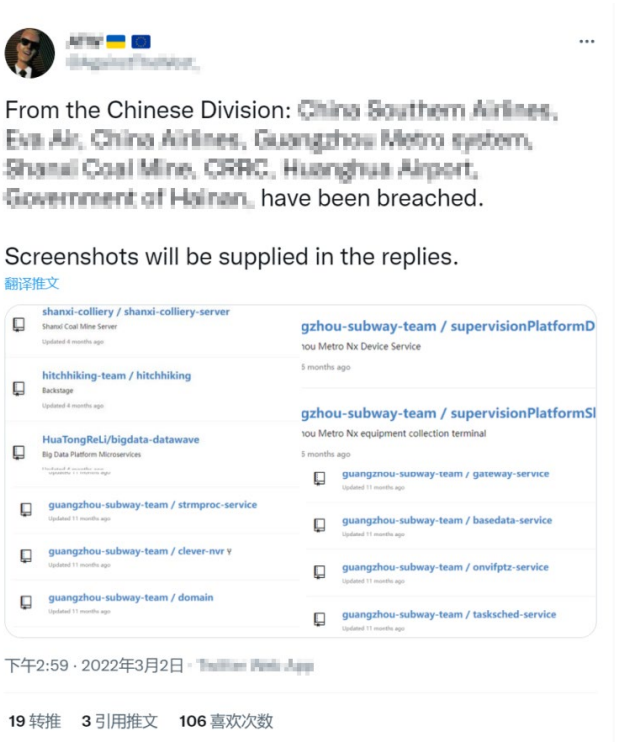
总书记指示：网络安全的本质在对抗，对抗的本质在攻防两端的能力较量。面对传统网络安全强国在网络安全领域常态化的攻击渗透这一实际威胁，需保持网络空间常态化战时状态思维，应对网络间的攻防对抗，来保障国家网络空间安全。

3.从“技术对抗”逐渐扩展到“舆论对抗”

当下网络安全和信息安全变得越来越重要，而国与国之间的网络对抗愈演愈烈，成为了国家间对抗的重要形式。而一直以来有地缘政治背景的APT组织和APT组织跨国攻击事件的披露，都会成为国际社会关注的焦点。这使得一系列的网络犯罪组织逐渐将以往的“技术对抗”不断扩展到“舆论对抗”、“舆论造势”，通过网络空间公开自身攻击成果、发布有利于己方和不利于对方的虚实信息，借助网络攻击事件的高敏感和关注程度，博取自身的“声誉”或达成其他政治目的。而面对一系列真假莫辨的网络攻击成果和情报信息的披露，网络安全人员不得不时刻做防范和甄别。

2022年年初，某黑客组织多次通过推文发布其攻击了中国多个组织机构。360对此事件进行了持续的跟踪和分析。经分析，源代码泄露事件主要是由于Gogs和GitLab两款代码仓库平台，在部署的时候普遍存在未授权访问情况导致。

虽然该组织在此次代码泄露事件中披露的攻击成果和实际影响范围，存在一定造势成分，但也给我国的网络安全、基础设施信息安全敲响了警钟。根据统计中国是受Gogs和GitLab未授权代码泄露威胁最为严重的国家，这些代码暴露在互联网上将会严重危害我国基础设施的信息安全。



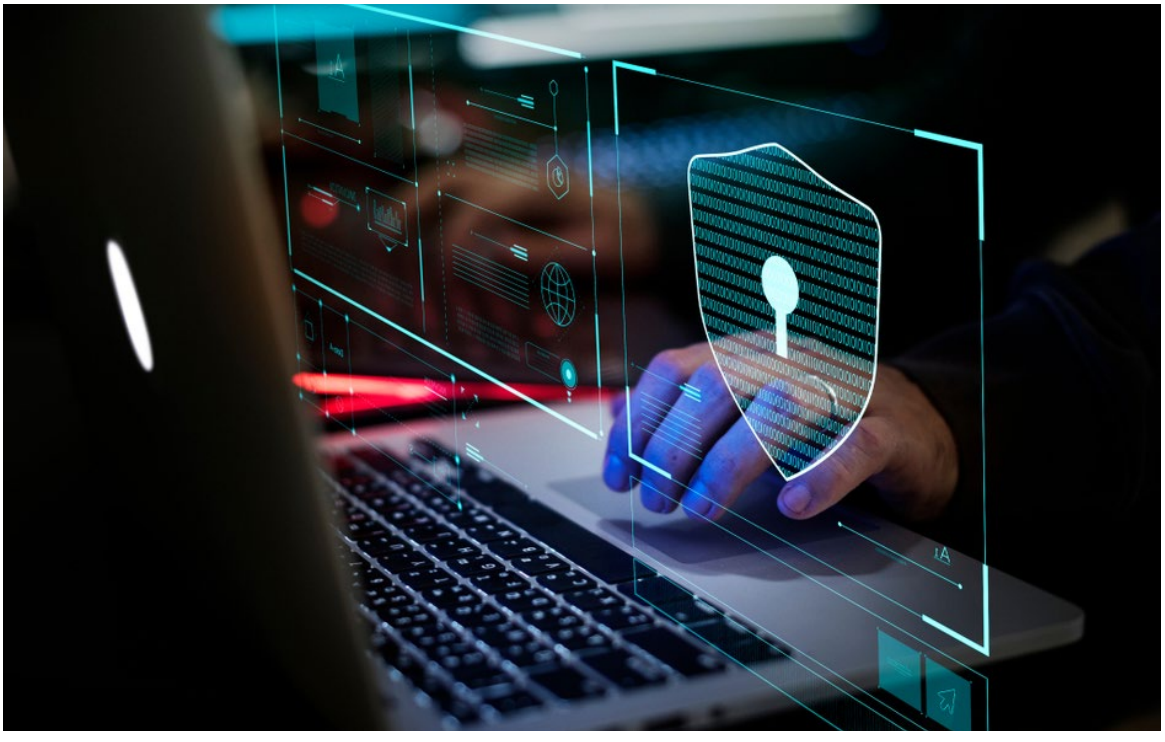
黑客组织发布的所窃取的单位源码资产推文

4.APT攻击瞄准我国自主可控领域

“十四五”期间，我国大力推进的信息技术应用创新，旨在实现信息技术领域的自主可控。信息技术自主可控是保障国家网络安全、国家信息安全的前提。信创产业是数字经济、信息安全发展的基础，也是新基建的重要内容，已经成为我国经济数字化转型、提升产业链发展的关键，信创产业受到前所未有的重视。

与此同时，复杂严峻的外部环境下，各方势力对我国信创产业发展的关注度也在不断提高。在2022年APT组织针对我国展开的攻击活动目标，包含我国国产化操作系统和自主软件供应商，显示出了攻击活动瞄准我国自主可控领域发展的趋势。

2022年，360高级威胁研究院在对海莲花攻击活动的深入跟踪和分析中，分别发现了海莲花针对MIPS和Arm架构，使用境内失陷IoT设备作为跳板的恶意样本，以此推断海莲花组织已经具备了针对MIPS和Arm架构系统的攻击方案。我国自主研发的龙芯、鲲鹏等CPU芯片系统以MIPS和Arm架构为基础，海莲花组织针对IoT设备的一系列攻击活动，体现出该组织已具备向针对国产化系统目标展开攻击的能力和发展趋势。这一趋势需要我国信创和国产化系统相关厂商提高警惕。



5.数字化转型面临更加复杂多样的网络威胁

“十四五”规划纲要专门设置了“加快数字化发展 建设数字中国”章节[49]，并对加快建设数字经济、数字社会、数字政府，营造良好数字生态作出明确部署。利用数字化新技术驱动城市战略发展是城市在持续数字化转型过程中保持领先的的核心要素，随着城市的数字化建设的不断深化、融合，数以亿计的物联网设备、工业互联网设备、数字化终端投入数字化城市的建设中，成为数字化城市的传感器。

在数字化转型进程中，网络安全威胁风险也日益凸显。网络资产数量和类型众多、网络边界难以定义、网络攻击的暴露面无限扩大，安全漏洞难以及时消除等一系列实际问题，使数字化转型面临更加复杂多样的网络威胁。而数字化城市中的单点遭到渗透突破，可能影响到整个面，导致业务的停摆，甚至进一步渗透，威胁到整个数字化城市的安全，造成更加严重的后果。数字化城市建设过程中网络威胁将超越传统安全威胁，成为数字时代最大的威胁。

网络黑客、具有国家背景的网军以及APT组织，对我国数字化进程也保持着持续关注，在实施网络攻击时往往突破常规，寻找安全缺口。一系列针对IoT设备的勒索软件攻击和针对ICT供应商的APT攻击事件表明，供应链、IoT设备这些城市数字化建设的基础，成为了网络攻击的重要目标。

数字化程度越高，安全挑战越大。沿用传统的网络安全思路无法解决数字城市的安全问题，需要将安全体系与数字体系融合、攻防能力与管控能力融合，构建面向数字城市的新一代安全能力框架。

附录

01 360安全大脑

360基于安全大数据、知识库和专家，建设了360全网数字安全大脑和网络安全基础设施（情报、漏洞、专家、实战、培训、测绘、开发），以云服务方式为政府、企业、个人用户提供安全公共服务，形成了新的安全理念和方法论。

360全网数字安全大脑强化了“精准防控为要、实战有效为王”的价值取向，着眼安全事件的“高效发现和及时处置”，理顺识别、防御、监测、预警、响应流程，推动一般常见风险及时处置、高级重大威胁有效解决、预防关口主动前移。着眼防范化解重大风险，聚焦最难啃的骨头、最突出的隐患、最明显的短板，及时总结网络安全风险防控经验，研究开发务实有效的安全原生服务。强化互联网体系与政企体系的协同联动，让网络安全体系回归保障业务的本质。

02 研究机构

360高级威胁研究院

360数字安全集团的核心能力支持部门，由360资深安全专家组成，专注于高级威胁的发现、防御、处置和研究。下设APT技术分析、情报分析、引擎研发等6个核心部门，业务主要涵盖了高级威胁相关威胁鉴定、溯源拓线、监测预警、智能安全引擎、核心安全技术推导等多个关键领域。曾在全球范围内率先捕获双杀、双星、噩梦公式等多起业界知名的0day在野攻击，独家披露多个国家级APT组织的重要攻击行动，赢得业内外的广泛认可，为360保障国家网络安全提供有力支撑。

参考链接

1.https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26485 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26486

2.https://www.pangulab.cn/post/the_bvp47_a_top-tier_backdoor_of_us_ nsa_equation_group/

3.https://mp.weixin.qq.com/s/Qthrx6FNeY38saHjyVbAVw 4.http://www.cverc.org.cn/head/zhaiyao/news20220218-1.htm

5.https://www.antiy.cn/research/notice&report/research_report/20220315.html

6.https://mp.weixin.qq.com/s/27sVSUNA3aVkUDAigM3Jbg

7.https://www.cverc.org.cn/head/zhaiyao/news20220629-FoxAcid.htm

8.https://www.anquanke.com/post/id/275517 9.https://mp.weixin.qq.com/s/tygPMy9DxNMZ6zkV-bL7-A

10.https://mp.weixin.qq.com/s/CfkLGhqLB3hyVcDzqUQwJQ

11.https://mp.weixin.qq.com/s/dMFyLxsErYUZX7BQyBL9YQ

12.https://mp.weixin.qq.com/s/qsGxZliTsuI7o-_XmiHLHg

13.https://securelist.com/the-bluenoroff-cryptocurrency-hunt-is-still-on/105488/

14.https://blog.google/threat-analysis-group/countering-threats-northkorea/

15.https://www.cisa.gov/uscert/ncas/alerts/aa22-108a

16.https://www.zscaler.com/blogs/security-research/naver-ending-game-lazarus-apt

17.https://asec.ahnlab.com/ko/34107

18.https://blog.malwarebytes.com/threat-intelligence/2022/01/north-koreas-lazarus-apt-leverages-windows-update-client-github-in-latest-campaign/

19.https://securelist.com/andariel-deploys-dtrack-and-maui-ransomware/107063/

201.https://www.welivesecurity.com/2022/09/30/amazon-themed-campaigns-lazarus-netherlands-belgium/

21.https://asec.ahnlab.com/ko/40495/

22.https://securelist.com/dtrack-targeting-europe-latin-america/107798/

23.https://www.volexity.com/blog/2022/12/01/buyer-beware-fake-cryptocurrency-applications-serving-as-front-for-applejeus-malware/

24.https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/

25.https://mp.weixin.qq.com/s/I1XtkVeETM3y93YLTjrs5A

26.https://docs.google.com/spreadsheets/d/1IkNJ0uQwbeC1ZTRrxdtuPLCIl7mlUreoKfSIgajnSyY/view#gid=1662223764

27.https://research.checkpoint.com/2022/apt35-exploits-log4j-vulnerability-to-distribute-new-modular-powershell-toolkit/

28.https://www.sentinelone.com/labs/log4j2-in-the-wild-iranian-aligned-threat-actor-tunnelvision-actively-exploiting-vmware-horizon/

29.https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/stonefly-north-korea-espionage

30.https://www.mandiant.com/resources/mobileiron-log4shell-exploitation

31.https://www.secureworks.com/blog/cobalt-mirage-conducts-ransomware-operations-in-us

32.https://asec.ahnlab.com/ko/34107/

33.https://www.microsoft.com/security/blog/2022/08/25/mercury-leveraging-log4j-2-vulnerabilities-in-unpatched-systems-to-target-israeli-organizations/

34.https://blog.talosintelligence.com/2022/09/lazarus-three-rats.html

35.https://www.cisa.gov/uscert/ncas/alerts/aa22-257a

36.https://www.secureworks.com/blog/drokbk-malware-uses-github-as-dead-drop-resolver

37.https://mp.weixin.qq.com/s/YAAybJBAvxqrQWYDg31BBw

38.https://citizenlab.ca/2022 /04/catalangate- extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/

39.https://securelist.com/the-bluenoroff-cryptocurrency-hunt-is-still-on/105488/

40.https://www.cisa.gov/uscert/ncas/alerts/aa22-108a

41.https://mp.weixin.qq.com/s/Xs54_RDKU5MvkvsPPCGKEw

42.https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/the-hermit-kingdoms-ransomware-play.html

43.https://www.cisa.gov/uscert/ncas/alerts/aa22-187a

44.https://securelist.com/vilerat-deathstalkers-continuous-strike/107075/

45.https://www.secureworks.com/blog/opsec-mistakes-reveal-cobalt-mirage-threat-actors

46.https://research.checkpoint.com/2022/state-sponsored-attack-groups-capitalise-on-russia-ukraine-war-for-cyber-espionage/

47.https://research.checkpoint.com/2022/state-sponsored-attack-groups-capitalise-on-russia-ukraine-war-for-cyber-espionage/

48.https://opinion.huanqiu.com/article/49HwiYUPXIx

49.http://www.gov.cn/xinwen/2022-03/23/content_5680843.htm

2022年
全球高级持续性威胁APT
研究报告

RESEARCH
REPORT

360数字安全
数字安全的领导者

360
高级威胁研究院