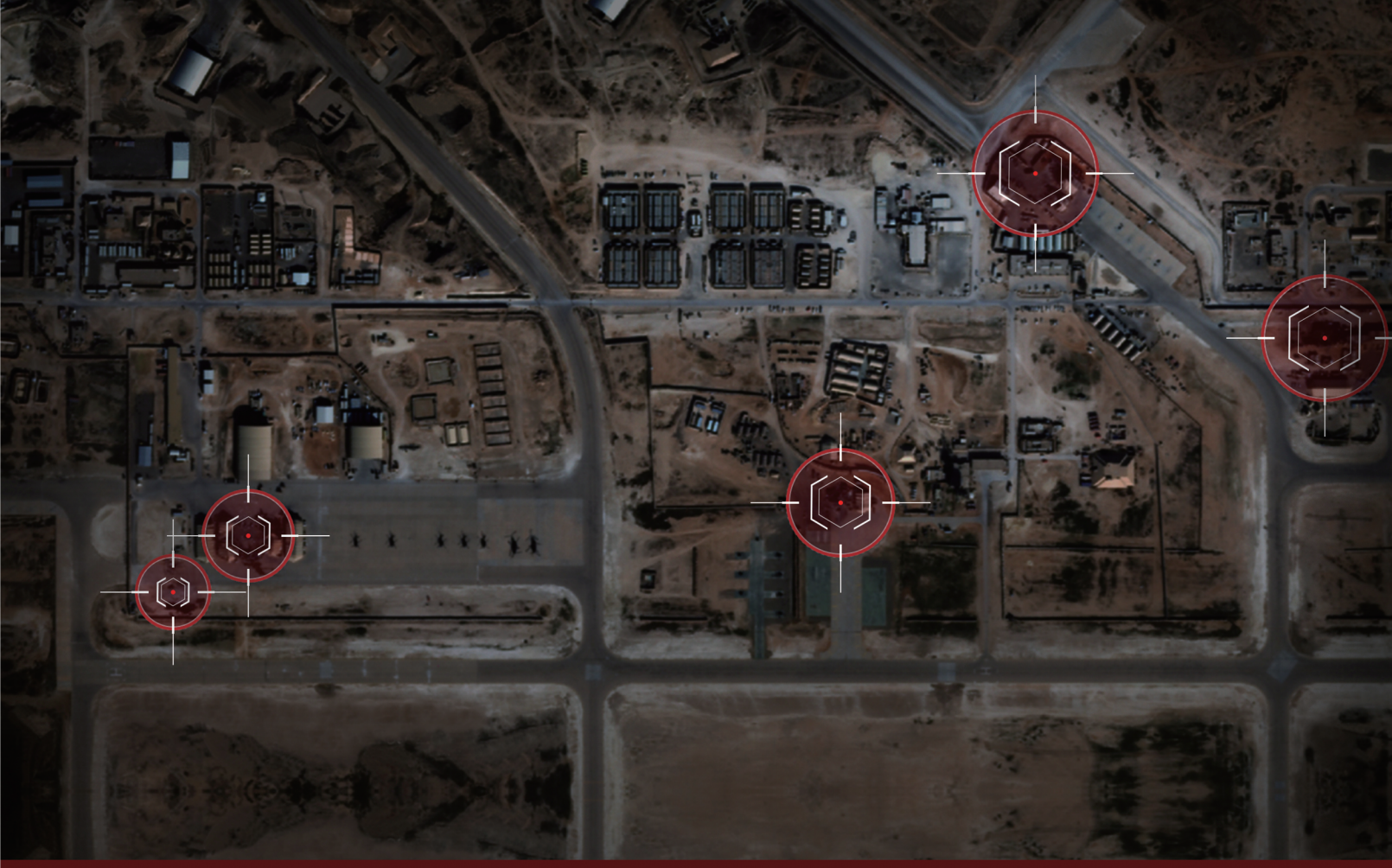


APT

全球高级持续性威胁（APT）2019年报告

奇安信 威胁情报中心

2020年1月

序 言

过去的一年，在网络威胁（Cyber Threat）领域度过了颇为不平静的一年。网络威胁和攻击似乎更为广泛的应用于地缘政治和军事冲突之下，其作为除了军事打击之外更为有效的手段。通常，实行军事行动或军事打击，往往受制于国力、财力、军力、国际舆论、政治压力等多方面因素，而实施网络攻击行动则是利用更加隐蔽的方式达成类似的效果。

网络行动（CNO）在美国军事领域被视为信息作战的核心能力之一，其由网络攻击（CNA）、网络防御（CND）和网络利用（CNE）组成。过去我们讨论的更多的APT威胁都属于CNE范畴，其主要的意图在于收集目标系统或网络的情报数据并加以利用。因此，持久化和隐匿性是实施CNE的重要基础。

而CNA的主要目的在于干扰（Disrupt）、拒绝（Deny）、降级（Degrade）、破坏（Destroy）目标的设施、设备、网络甚至数据信息。当下像政务系统、电力能源、医疗、工业制造等具备更高的信息化和智能化，导致一旦出现网络攻击，其不仅仅是面临财产的损失，而且对社会和民生造成极大的影响。由于CNA所造成的影响和现象是明显的，其类似于现代军事行动具备在较短时间范围就能达到行动目标，而实施CNA的基础则在于对潜在目标的了解程度和网络武器的装备化，所以其往往依赖于历史的网络利用活动，或是结合网络利用。像震网事件、乌克兰停电事件、WannaCry爆发都是较为典型的网络攻击的形态。

过去，我们在分析、发现、识别和跟踪网络攻击和利用活动时，不仅关注于攻击的战术技术特点，以及总结和归纳其攻击来源和攻击组织的手法和变化，从而提高对对手的了解程度以及研究APT威胁的趋势。结合过去我们对APT威胁的研究基础，APT威胁正在变得更加复杂化，其不光体现在对手的策略和能力的提升，而且更加注重对自身的操作安全（OPSEC），通过隐藏、伪装、误导、模仿的方式减少留下自身的行为指纹，对APT威胁的归因分析带来挑战。APT组织寻求更高维度的攻击链路，包括对广域网的流量劫持，基础设施劫持，供应链攻击等等，导致对于APT威胁分析依赖于更广维度的数据来源和元数据类型。

我们在每次全球高级持续性威胁的研究总结报告中对近一年内全球APT威胁活动和APT研究成果的分析和总结，并提出我们对APT威胁的变化趋势的看法。也寄希望于对业内的APT研究和防御提供一些基础性思路。

概 要

结合2019年全年高级持续性威胁活动情况来看，我们认为近一年来高级威胁活动呈现出如下的趋势。

- 2019年，奇安信威胁情报中心收录了高级威胁类公开报告总共596篇，其中涉及了136个命名的攻击组织或攻击行动，被认为活跃在东亚半岛范围的3个APT组织被披露的频率最高。政府、防务行业的目标依然是APT威胁的主要目标，而不可忽视的是，能源和通信行业也已经成为APT威胁的重要针对对象。

- 在此次报告中，我们依然围绕地缘特征总结了6大地区总共22个APT组织在近一年的攻击活动情况以及使用的主要攻击工具。按照地缘特征划分来研究APT威胁活动：一方面是因为按地域划分下其通常拥有较为相似的地缘政治因素，导致APT活动和APT组织的意图和动机具备相似性和可比性；另一方面也是为了在归因困难和攻击TTP出现重叠的情况下，对同一地域范围的威胁活动进行类比分析。

- 在报告中，我们也从行业视角分析了针对金融、能源和电信行业在2019年面临的高级威胁问题，并且总结了一年来主要的攻击组织和攻击活动。我们也认为未来APT类威胁活动可能会更多的扩展到金融、能源和电信行业，并且更具有针对性。

- 在文中我们也总结了全年公开披露的在野0day攻击情况，无论从披露的在野漏洞攻击案例还是利用0day漏洞的攻击组织数量都较去年有所增长。在漏洞类型上，未发现公开披露新的文档类0day漏洞案例，而针对PC和移动终端的浏览器的完整漏洞利用链数量大大增加。

- 我们在此次的报告中也讨论了网络攻击造成的破坏性影响以及疑似网络战相关的活动，我们也认为网络攻击破坏活动相对于军事行动来说，更加具有隐蔽性和溯源难的特点，从而攻击源头可以进行否认。由此可以预见未来网络攻击破坏活动可能更加频繁。

研究方法

在此报告的开始，我们列举了本研究报告所依赖的资料来源与研究方法，其中主要包括：

- 内部和外部的情报来源，其中内部的情报来源包括奇安信威胁情报中心旗下红雨滴团队对APT威胁的持续分析跟踪及相关的威胁情报参考链接[1]；外部的情报来源包括主要发布APT类情报200多个公开数据源，涉及安全厂商、博客、新闻资讯网站、社交网络等。

- 以MITRE ATT&CK框架[2]和NSA/CSS CTF框架[3]为基础，作为对威胁组织攻击战术技术的标准化表达。

- 基于网络杀伤链模型（Kill-Chain）对攻击步骤的定义，我们结合APT威胁分析中易于观测到的阶段进行简化和合并：筹备阶段、攻击入口和立足阶段、持久化维持和横向移动阶段、命令控制和数据渗出阶段。

- 基于钻石模型，我们总结对APT威胁组织画像依赖的重要要素：攻击活动、目标（地域目标、行业目标）、能力（恶意程序、工具、漏洞利用程序）、资源（网络基础设施）。

- 对于APT组织的评判和定义，我们参考了ATT&CK Groups[6]，MISP项目[4]、国外安全研究人员Florian Roth的APT组织和行动表格[5]等等。

- APT组织的国家和地域归属判断是综合了外部情报的结果，并不代表奇安信威胁情报中心自身的判定结论。

目　录

第一章　全球高级持续性威胁趋势

奇安信威胁情报中心在2018年的全球高级威胁总结报告中就基于公开来源APT情报的收集数据对APT威胁趋势进行图表可视化展示。在2019年的总结报告中，我们沿用了相同的方式。本章内容是基于奇安信威胁情报中心对200多个主要发布APT类情报来源渠道的数据收集、统计和分析结果，其中包括但不限于以下类型：

APT攻击团伙报告、APT攻击行动报告、疑似APT的定向攻击事件和APT攻击相关的恶意代码和漏洞分析，以及我们认为需要关注的网络犯罪团伙及其相关活动。

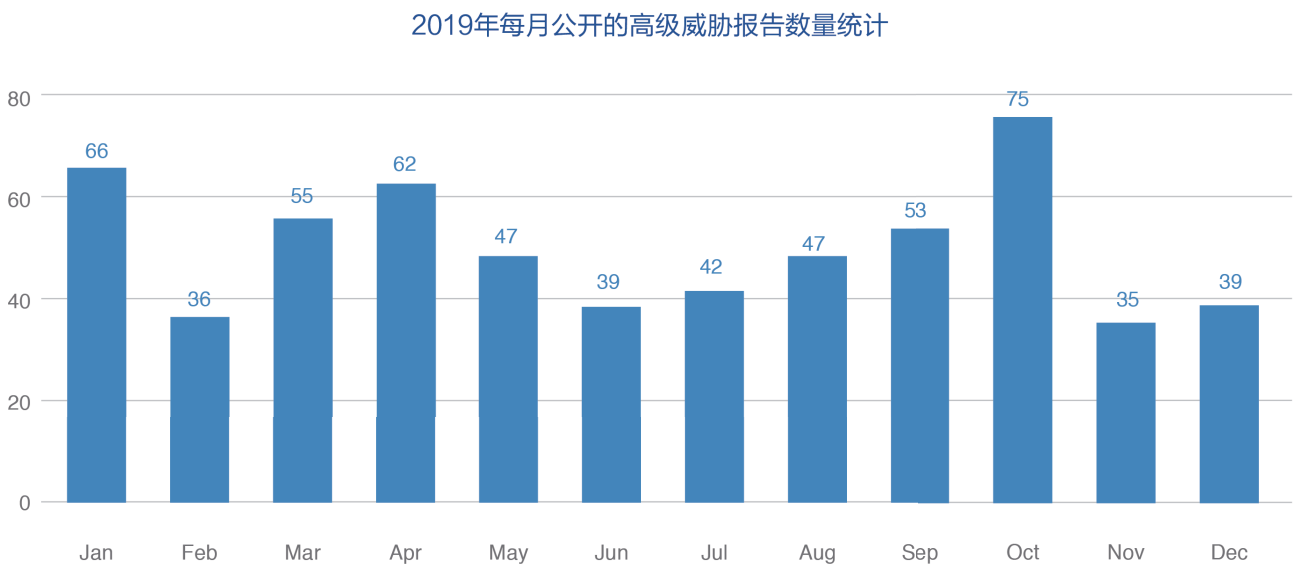
国内外安全厂商、安全研究人员通常会对高级持续性威胁活动涉及的攻击团伙、攻击活动进行命名，并以"Actor / Group / Gang"等对威胁背后的攻击者进行称谓，其中包括了明确的APT组织，明确的网络犯罪团伙，以及暂时不太明确攻击者信息的攻击活动命名。

不同的安全厂商有时候会对同一背景来源的威胁进行不同的别名命名，这取决于其内部在最早跟踪威胁活动时的命名约定，所以往往需要根据威胁攻击的同一来源进行归类。

我们结合上述说明对自身收集渠道收集的公开报告内容进行分析，并从公开披露的信息中公布2019年全球高级持续性威胁的态势情况。

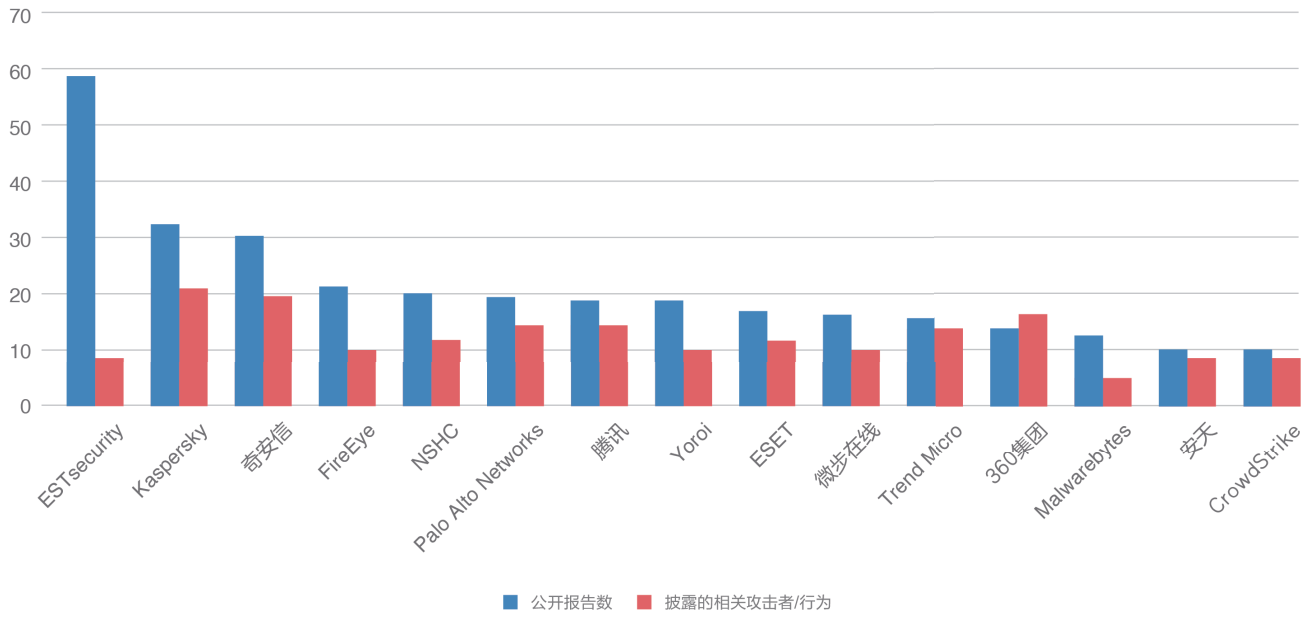
一、数量和来源

奇安信威胁情报中心在2019年监测到的高级持续性威胁相关公开报告总共596篇。



从公开报告的发布渠道统计来看，韩国安全厂商ESTsecurity发布了最多的高级威胁类报告，不过其披露的主要为针对韩国本土目标的攻击组织和攻击行动。除此以外，像奇安信、Kaspersky、FireEye、Palo Alto Networks和腾讯等依然保持着较高的高级威胁的跟踪、分析和披露，并且跟踪和披露全球范围内的多个APT组织和攻击行动。

2019年国内外安全厂商披露高级威胁类报告及相关组织情况统计

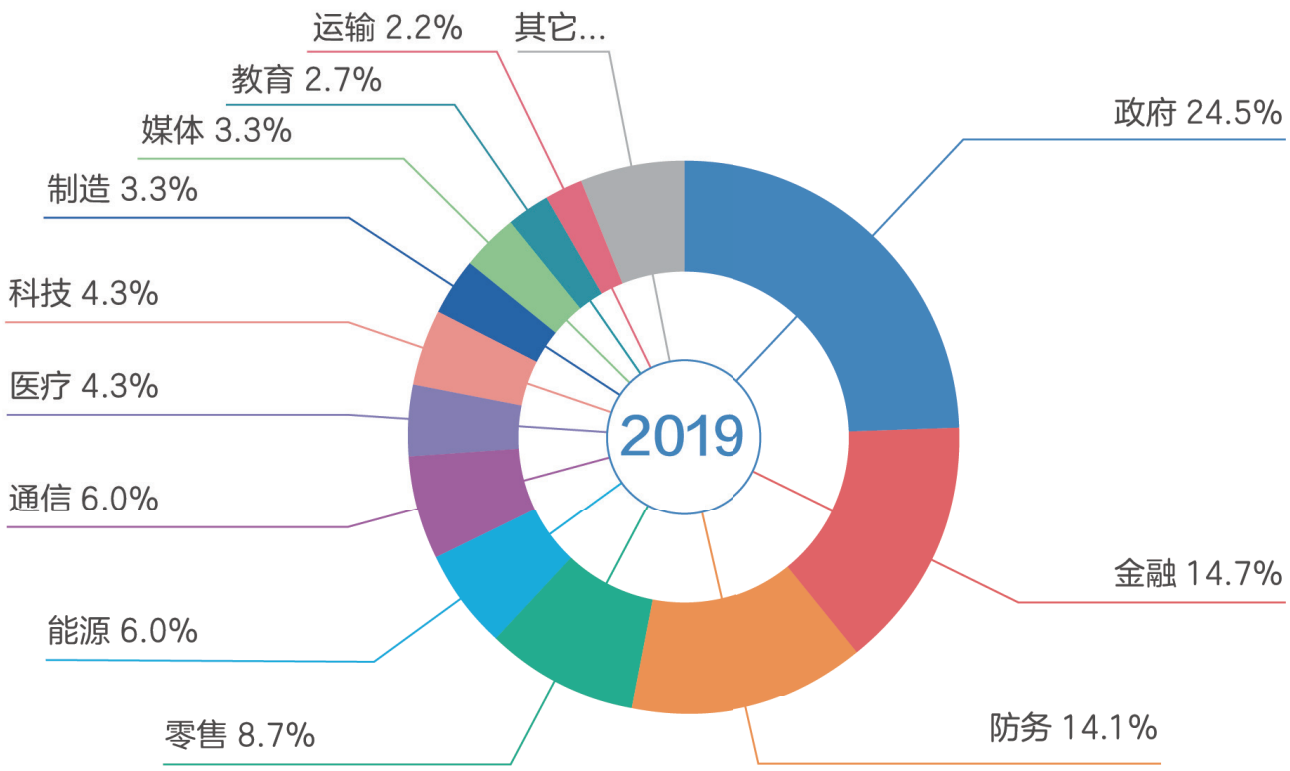


二、受害目标的行业与地域

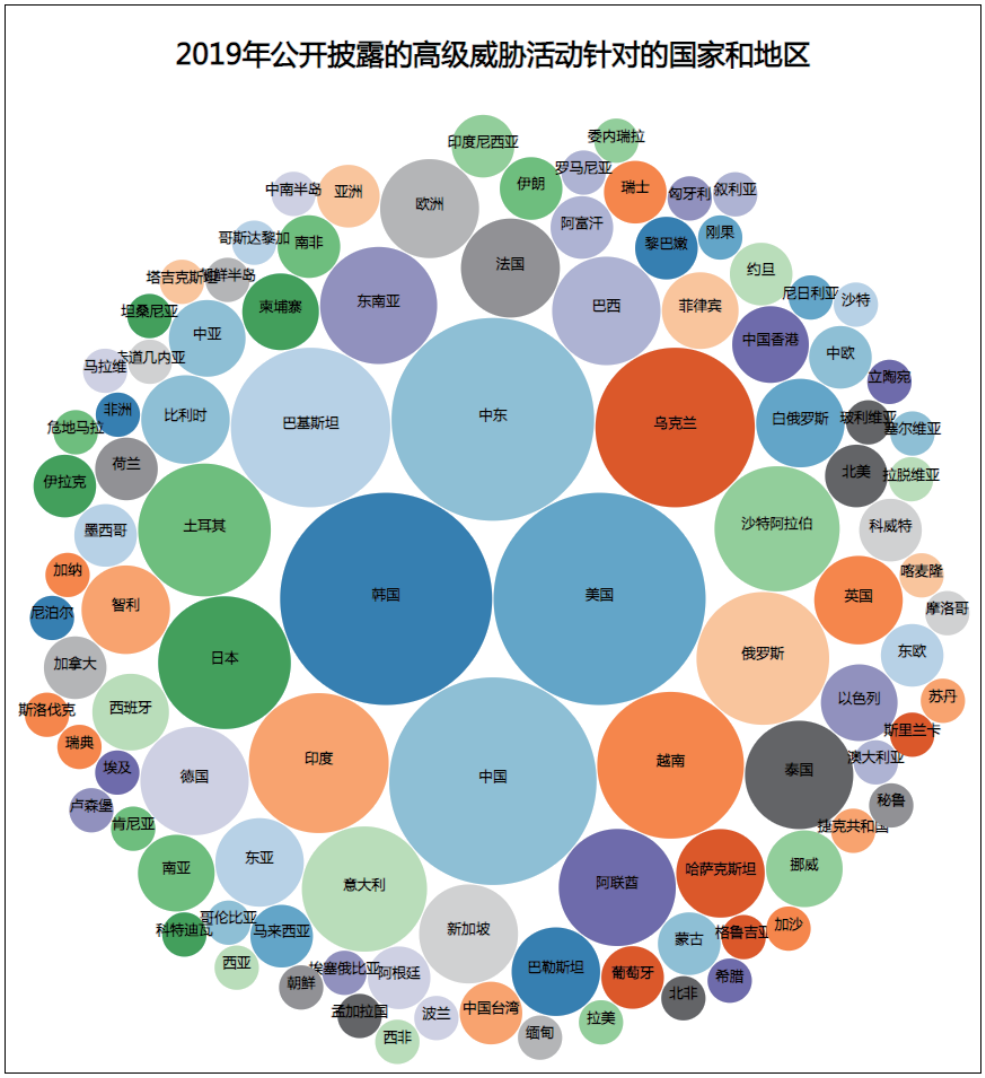
从公开披露的高级威胁活动中涉及目标行业情况来看（摘录自公开报告中提到的攻击目标所属行业标签），政府（包括外交、政党、选举相关）和军事（包括军事、军工、国防相关）依然是 APT 威胁的主要目标，能源（包括石油、天然气、电力、民用核工业等）、通信行业也是APT攻击的重点威胁对象。

由于更加组织化的网络犯罪团伙的活跃活动，导致金融（包括银行、证券、数字货币等）和零售（电子商务、餐饮等）行业所面临的高级威胁现象越发严峻。

2019年公开高级威胁事件报告涉及行业分布情况

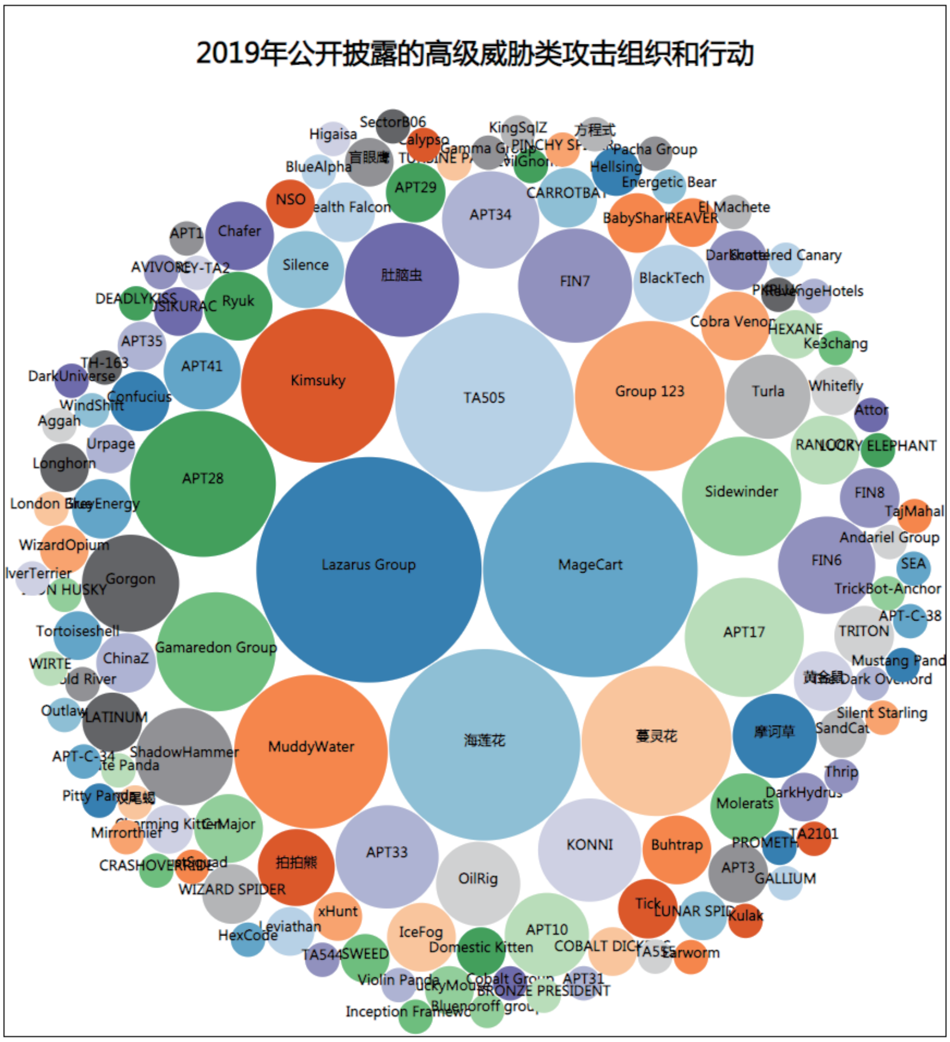


高级威胁活动涉及目标的国家和地域分布情况统计如下图（摘录自公开报告中提到的受害目标所属国家或地域），可以看到高级威胁攻击活动几乎覆盖了全球绝大部分国家和区域。



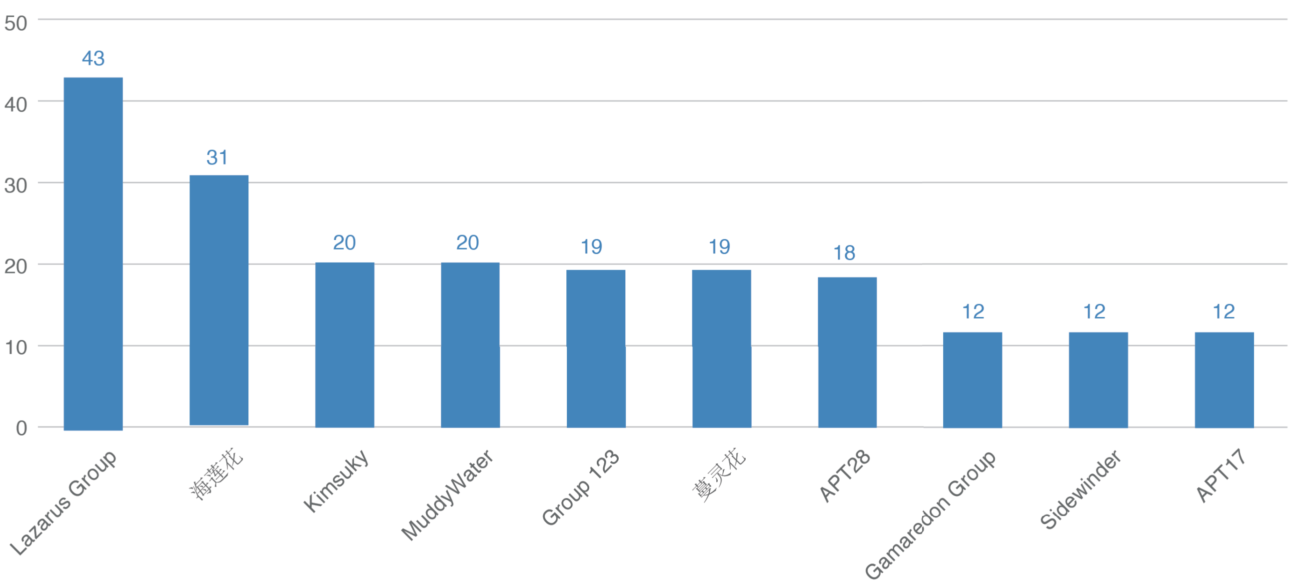
三、活跃的威胁攻击者

进一步对公开报告中高级威胁活动中命名的攻击行动名称、攻击者名称，并对同一背景来源进行归类处理后的统计情况如下，总共涉及136个命名的威胁来源命名，较2018年数量有所增长。



我们也统计了2019年公开披露最多的APT组织，跟2018年相比，疑似来自东北亚某地的Lazarus Group、Kimsuky和Group 123三个APT组织被频繁曝光。

2019年主要APT组织相关报告数量统计

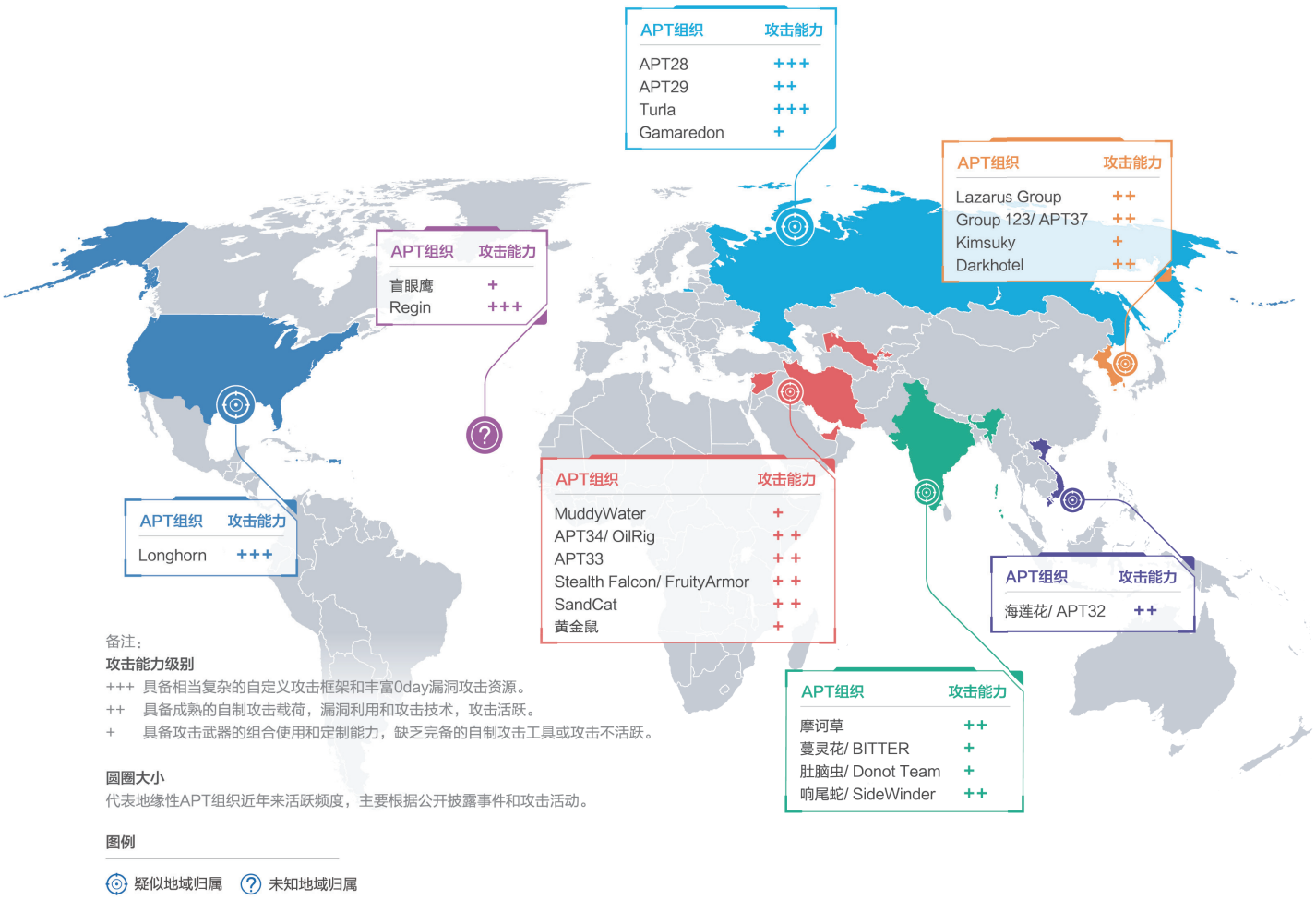


第二章　地缘下的APT组织、活动和趋势

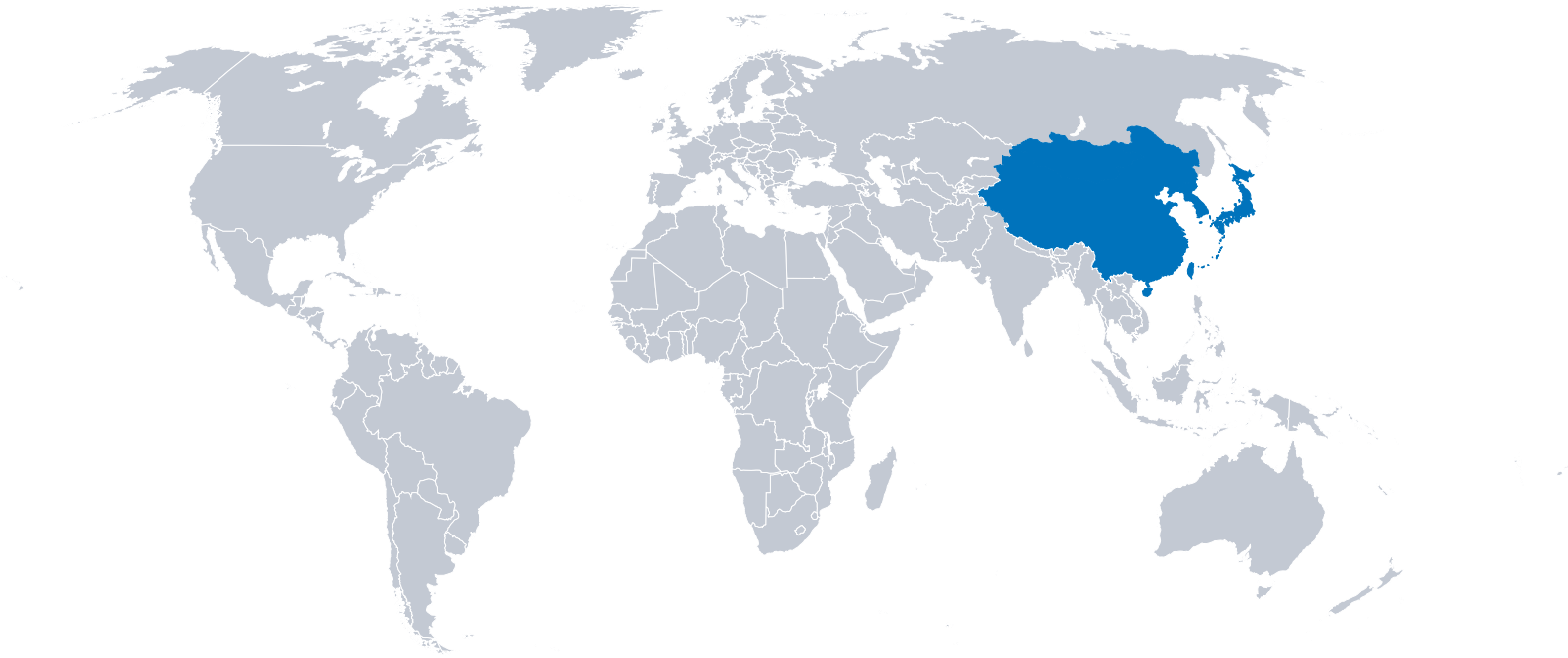
一、地缘下的活跃APT组织

从2018年中的APT威胁总结报告中，我们就开始从地缘划分的角度来研究APT组织活动，一方面往往由于在同一地域范围的APT组织和APT活动常常出现一些重叠，其可能针对相似的攻击目标或者使用类似的TTP。另一方面，按地域划分下其拥有相似的地缘政治因素，导致APT活动和APT组织的意图和动机具备相似性和可比性，即使是两个完全不同背景的APT组织。

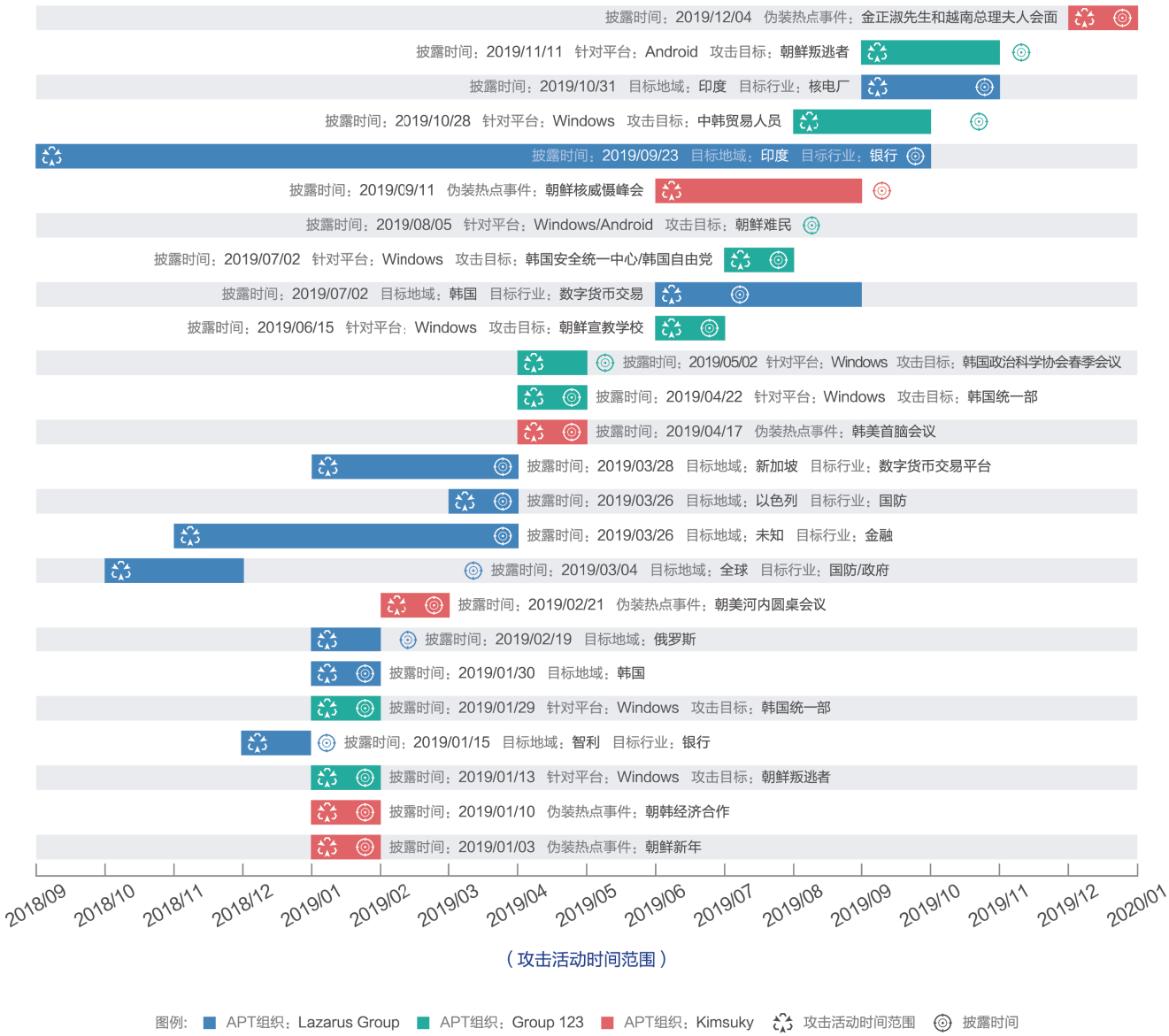
我们在下表中列举了2019年主要活跃的APT组织，全球主要APT组织列表也可以参见附录4。



（一）东亚



Lazarus Group、Kimsuky和Group 123是2019年公开披露最多，被指源自东北亚某地的APT组织，其中，Lazarus Group作为该地区最为活跃的APT组织，其目标是全球性的。我们整理了上述3个APT组织在最近一年来被披露的攻击活动。



Lazarus Group一直被安全厂商作为疑似来自东北亚某国的APT活动归属总称，个别国外安全厂商也将其针对金融、银行行业的攻击归属作为一个子组织来跟踪。从其2019年被披露的攻击活动来看，仍旧针对全球性的金融、银行、数字货币交易、政府、国防实施网络攻击活动。

今年，Lazarus组织被发现攻击了印度的核电厂，结合公开情报其并未进入到OT网络中，虽然不明确其攻击印度以及印度核工业的意图何在，但是我们可以合理推测核电厂的攻击意图并不在于进行网络破坏，其一方面可能希望收集和获得核工业相关的情报，另一方面可能在于测试和演练对于工业领域的入侵活动。

Lazarus组织也被发现其利用定制化TrickBot分发其后门程序的技术手段，这是首次发现该组织开始利用网络犯罪工具列入到其攻击武器库中。虽然不明确该TrickBot Anchor是否通过市场交易的方式获得，但显然的是该组织的TTP（即攻击的战术、技术和过程）正在发生变化。

Lazarus作为最为古老的APT组织之一，其开发和拥有一套完备的攻击工具集，下表列举了Lazarus组织常用的网络武器库。

攻击工具名称	功能说明
Rising Sun	第二阶段植入物，由Duuzer后门演化的新渗透框架
KEYMARBLE	RAT工具，使用伪TLS通信
HOPLIGHT	木马，使用公共SSL证书进行安全通信
ELECTRICFISH	网络代理和隧道工具
FALLCHILL	RAT工具
Brambul	SMB蠕虫
Joanap	构建P2P僵尸网络
AppleJeus	针对MacOS的木马
Dtrack	RAT工具，针对银行和ATM的恶意程序
NukeSped	RAT工具，其也针对MacOS
Dacls	RAT工具，针对Windows和Linux
TrickBot Anchor	利用定制的网络犯罪木马分发PowerRatankba
PowerRatankba	PowerShell实现的后门程序

Group 123是2016年曝光的APT组织，其最早活动可以追溯到2012年，该组织主要实施网络间谍活动。该组织拥有较为成熟的针对Windows和Android平台的攻击木马，常被命名为ROKRAT，其偏好于利用云盘作为载荷分发和数据回传的基础设施。值得一提的是，韩国安全厂商披露该组织伪装成Lazarus的假旗[51]。而Kimsuky组织则偏好于利用热点政治外交活动作为其攻击诱饵的主题。

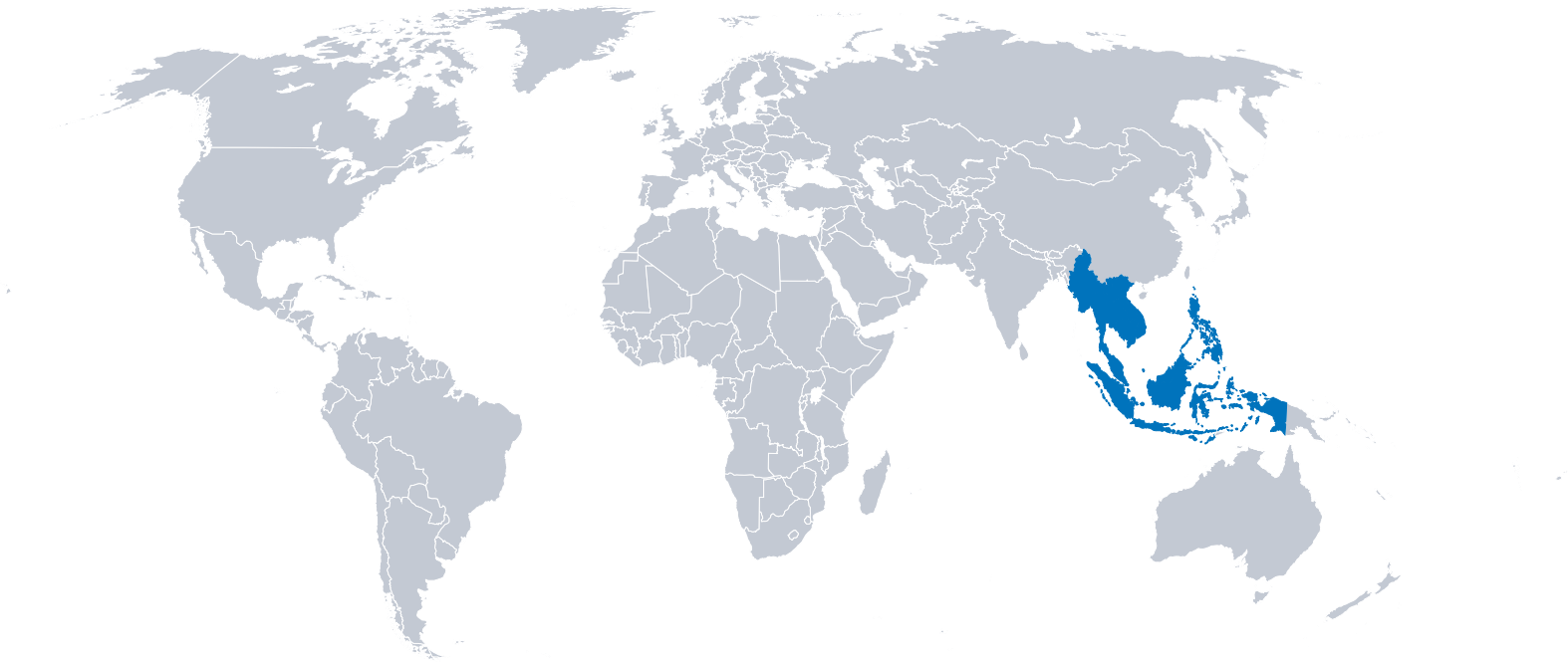
我们在年中报告中也总结了3个组织在目标选择和攻击意图上的不同，即使三个组织可能来源于同一地域范围，熟悉同样的语言。安全厂商也披露Group 123、Kimsuky以及Konni木

马家族之间存在联系，但这三者的TTP却存在较大的差异。

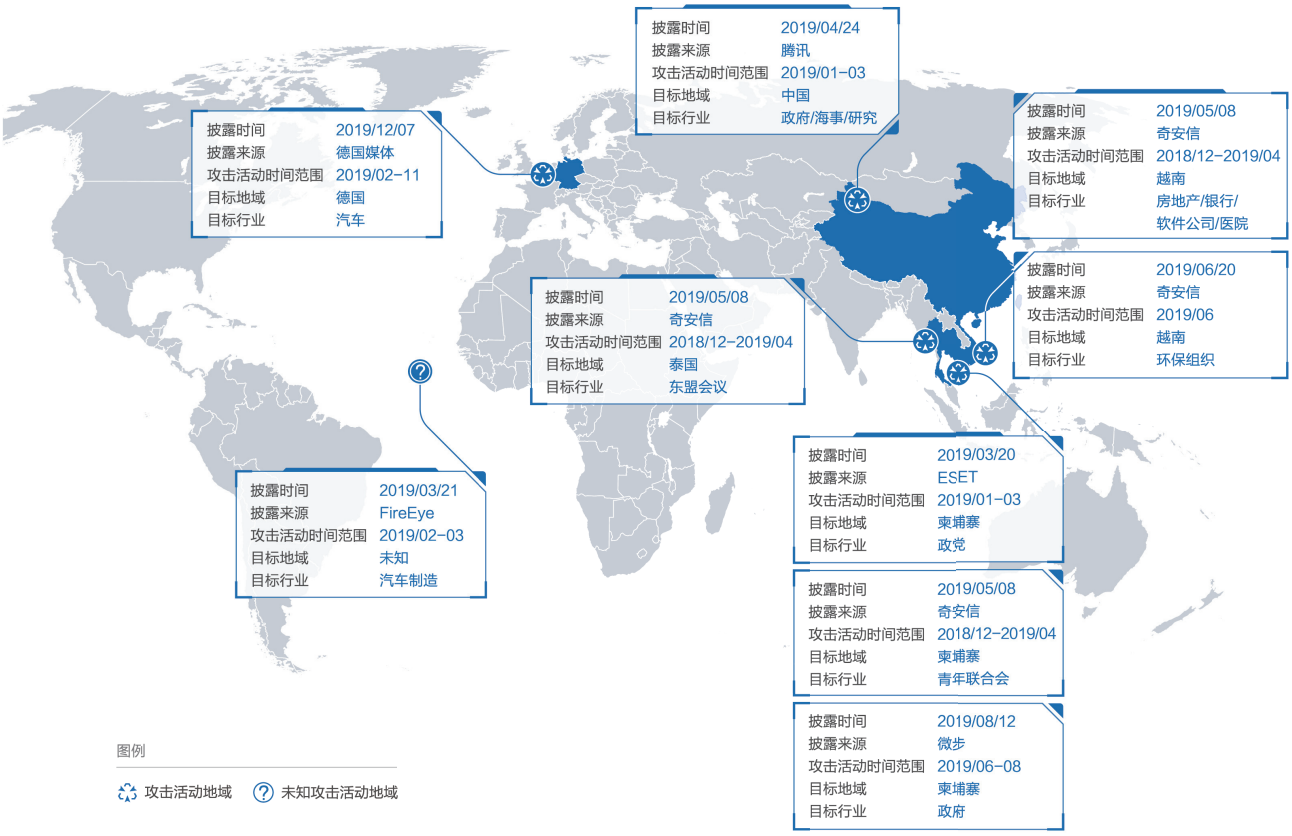
	Lazarus Group	Group 123	Kimsuky
主要别名	Hidden Cobra	APT37	无
目标行业	银行/数字货币/国防/政府	外交/投资/贸易	媒体
目标地域	全球范围	中国/韩国	韩国/美国
攻击动机	经济利益为主	情报获取	政治外交倾向

Darkhotel是另一个活跃在东亚地区的APT组织，其在2019年被公开曝光的攻击活动较过去来看存在下降趋势，但这并不代表该组织的攻击活动频率下降，其在2019年依然持续着对东亚地区实施APT攻击。

（二）东南亚



海莲花组织依然是在东南亚地区最为活跃的APT组织，其在2019年依然保持较高的活动频率。该组织已经由过去的网络间谍活动延伸至商业情报窃取领域，如汽车制造行业



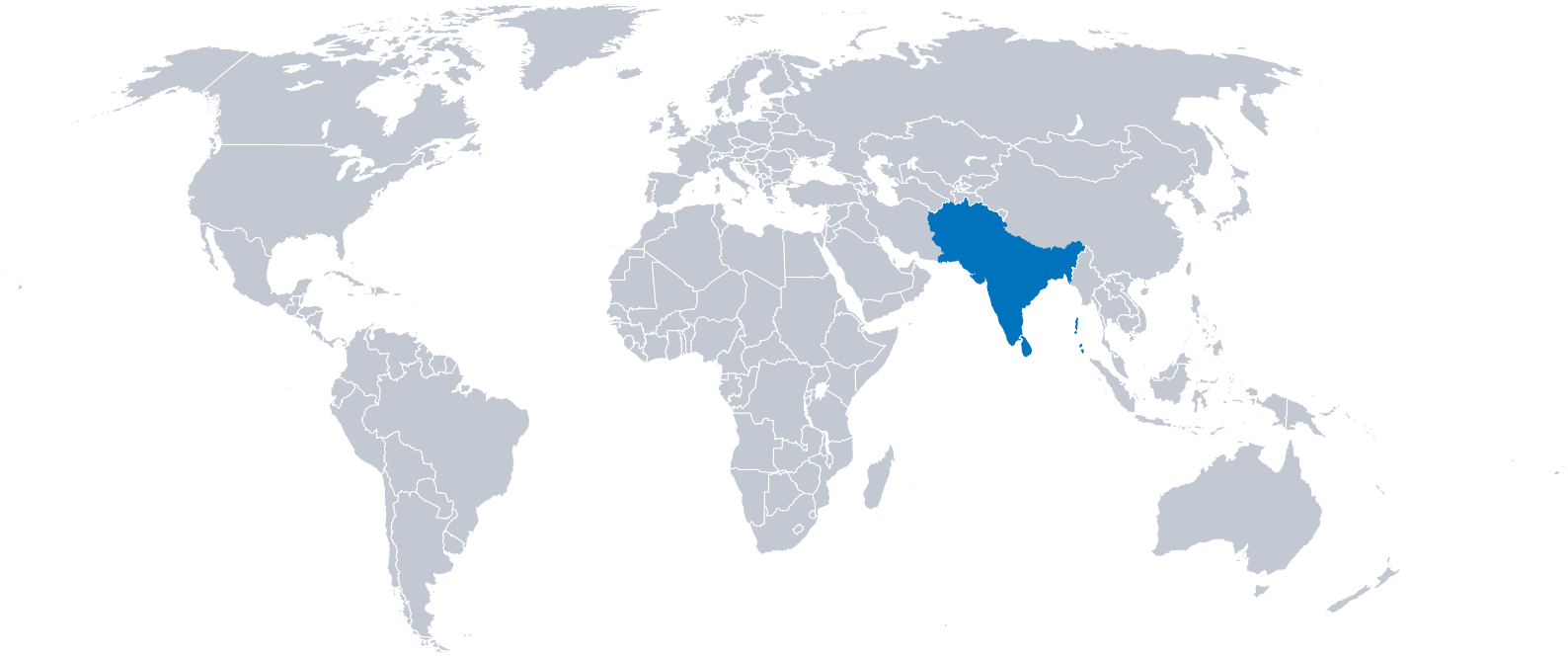
海莲花组织在过去常用Denis木马和Cobalt Strike beacon作为其最终的攻击载荷，安全厂商也发现其新的木马下载器实现，并命名为KerrDown。其擅长于攻击载荷的混淆和对抗手段避免下发的木马程序被检测。该组织也具备成熟的针对MacOS系统的攻击工具。

我们在年中的报告中曾总结过海莲花组织常用的攻击技术手段（见下图）。

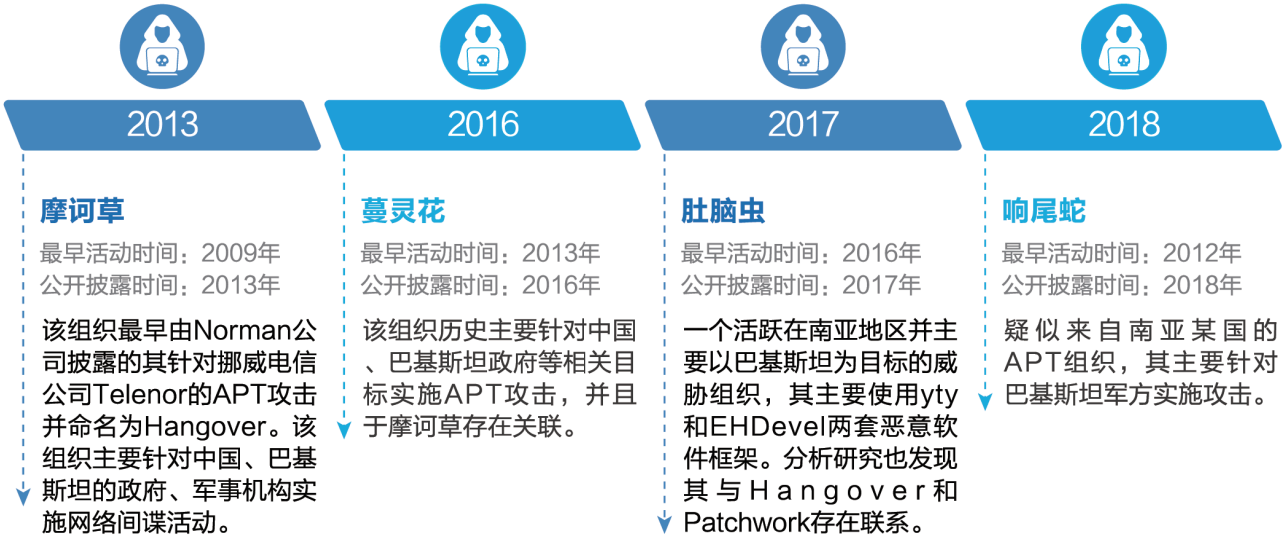
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
Drive-by Compromise	CMSTP	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	Command-Line Interface	Account Manipulation	Accessibility Features	Binary Padding	Brute Force	Application Window Discovery	Distributed Component Object Model	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Compiled HTML File	AppCert DLLs	AppCert DLLs	BITS Jobs	Credential Dumping	Browser Bookmark Discovery	Exploitation of Remote Services	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credentials in Files	Domain Trust Discovery	Logon Scripts	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Dynamic Data Exchange	Application Shimming	Application Shimming	CMSTP	Credentials in Registry	File and Directory Discovery	Pass the Hash	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Execution through API	Authentication Package	Bypass User Account Control	Code Signing	Exploitation for Credential Access	Network Service Scanning	Pass the Ticket	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Compile After Delivery	Forced Authentication	Network Share Discovery	Remote Desktop Protocol	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
Spearphishing via Service	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Network Sniffing	Remote File Copy	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Supply Chain Compromise	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Password Policy Discovery	Remote Services	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Network Denial of Service
Trusted Relationship	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt	Peripheral Device Discovery	Replication Through Removable Media	Input Capture	Fallback Channels		Resource Hijacking
Valid Accounts	LSASS Driver	Component Firmware	Hooking	Control Panel Items	Kerberoasting	Permission Groups Discovery	Shared Webroot	Man in the Browser	Multi-hop Proxy		Runtime Data Manipulation
	Mshta	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	LLMNR/NBT-NS Poisoning and Relay	Process Discovery	Taint Shared Content	Screen Capture	Multi-Stage Channels		Service Stop
	PowerShell	Create Account	New Service	Deobfuscate/Decode Files or Information	Network Sniffing	Query Registry	Third-party Software	Video Capture	Multiband Communication		Stored Data Manipulation
	Regsvcs/Regasm	DLL Search Order Hijacking	Path Interception	Disabling Security Tools	Password Filter DLL	Remote System Discovery	Windows Admin Shares		Multilayer Encryption		Transmitted Data Manipulation
	Regsvr32	External Remote Services	Port Monitors	DLL Search Order Hijacking	Private Keys	Security Software Discovery	Windows Remote Management		Remote Access Tools		
	Rundll32	File System Permissions Weakness	Process Injection	DLL Side-Loading	Two-Factor Authentication Interception	System Information Discovery			Remote File Copy		
	Scheduled Task	Hidden Files and Directories	Scheduled Task	Execution Guardrails		System Network Configuration Discovery			Standard Application Layer Protocol		
	Scripting	Hooking	Service Registry Permissions Weakness	Exploitation for Defense Evasion		System Network Connections Discovery			Standard Cryptographic Protocol		
	Service Execution	Hypervisor	SID-History Injection	Extra Window Memory Injection		System Owner/User Discovery			Standard Non-Application Layer Protocol		
	Signed Binary Proxy Execution	Image File Execution Options Injection	Valid Accounts	File Deletion		System Service Discovery			Uncommonly Used Port		
	Signed Script Proxy Execution	Logon Scripts	Web Shell	File Permissions Modification		System Time Discovery			Web Service		
	Third-party Software	LSASS Driver		File System Logical Offsets		Virtualization/Sandbox Evasion					
	Trusted Developer Utilities	Modify Existing Service		Group Policy Modification							
	User Execution	Netsh Helper DLL		Hidden Files and Directories							
	Windows Management Instrumentation	New Service		Image File Execution Options Injection							
	Windows Remote Management	Office Application Startup		Indicator Blocking							
	XSL Script Processing	Path Interception		Indicator Removal from Tools							
		Port Monitors		Indicator Removal on Host							
		Redundant Access		Indirect Command Execution							
		Registry Run Keys / Startup Folder		Install Root Certificate							
		Scheduled Task		InstallUtil							
		Screensaver		Masquerading							
		Security Support Provider		Modify Registry							
		Service Registry Permissions Weakness		Mshta							
		Shortcut Modification		Network Share Connection Removal							
		SIP and Trust Provider Hijacking		NTFS File Attributes							
		System Firmware		Obfuscated Files or Information							
		Time Providers		Process Doppelgänging							
		Valid Accounts		Process Hollowing							
		Web Shell		Process Injection							
		Windows Management Instrumentation Event Subscription		Redundant Access							
		Winlogon Helper DLL		Regsvcs/Regasm							
				Regsvr32							
				Rootkit							
				Rundll32							
				Scripting							
				Signed Binary Proxy Execution							
				Signed Script Proxy Execution							
				SIP and Trust Provider Hijacking							
				Software Packing							
				Template Injection							
				Timestomp							
				Trusted Developer Utilities							
				Valid Accounts							
				Virtualization/Sandbox Evasion							
				Web Service							
				XSL Script Processing							

海莲花组织常用ATT&CK

（三）南亚



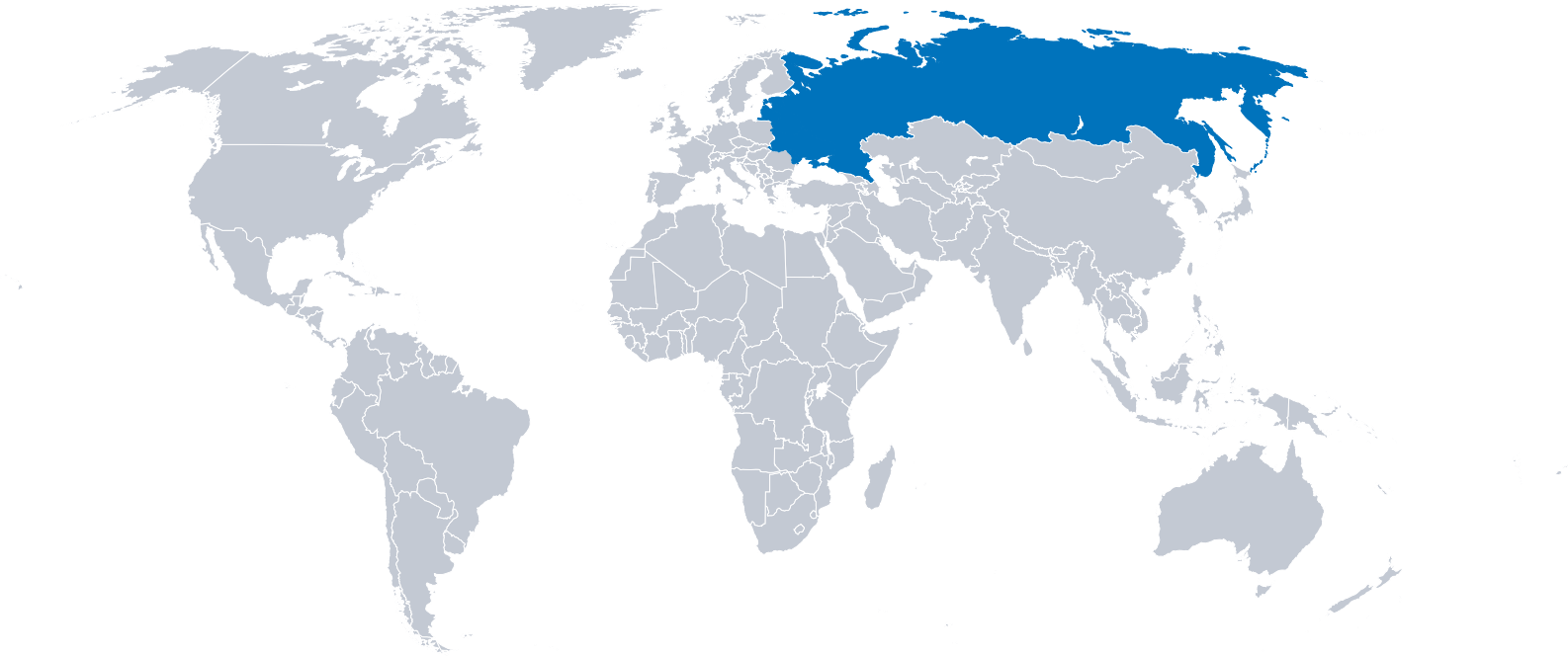
今年，南亚地区的几个APT组织活动频度较高，并且主要针对中国、巴基斯坦的政府、军事相关目标。我们对南亚地区主要活跃的APT组织情况进行总结。



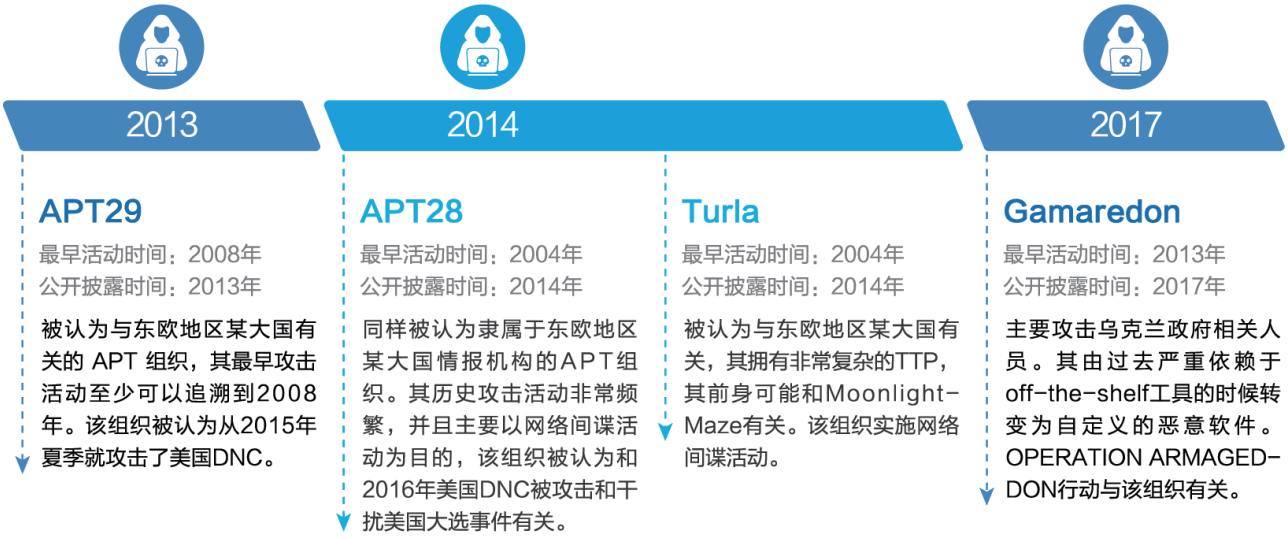
从历史的APT活动来看，南亚地区的APT组织互相存在TTP层面的重叠，其大多利用鱼叉邮件和社会工程学实施攻击，并且使用公开的文档型漏洞制作诱饵文档，如CVE-2017-11882。其大多同时具备针对Windows和Android平台的攻击工具，不过有意思的是，其攻击武器库似乎比较杂乱，无论从开发语言还是模块的重用性，大多不具备延续性。

我们总结了南亚APT组织在过去一年的主要攻击活动如下：

（四）东欧



东欧地区活跃着几个极为古老的APT组织，如APT28、APT29、Turla，其拥有高超的攻击技术，极为活跃的攻击频度。



整体来说，2019年东欧几个APT组织的公开披露次数较2018年有减少，我们整理了今年披露的主要攻击活动。

APT28组织是全球最为活跃的APT组织之一，其主要利用鱼叉邮件攻击，在过去主要可以通过XAgent木马与其联系到一起，后续该木马使用频率降低并频繁使用一个通过多种不同语言开发的Zebrocy木马，国外安全厂商还发现该组织使用Nim语言开发其下载器[55]。APT28除了使用自己的专用木马程序外，其还擅长于通过公开和开源工具的组合使用。

攻击工具名称	功能说明
Zebrocy	多种语言实现的下载器，包括Go、AutoIT、Delphi、C#、Python
LoJax	UEFI rootkit
Blitz	一个DLL后门
XAgent	历史常用的第二阶段木马

APT29组织在今年鲜有公开的披露报告，除了ESET披露了一个针对欧洲外交机构的Ghost 行动[56]，其中MiniDuke推测延续了过去的MiniDuke木马功能，还发现了其他的三个新的木马程序。从过去披露来看，该组织也常用鱼叉邮件和定制的专用木马。

攻击工具名称	功能说明
PolyglotDuke	使用社交网站存储C&C地址，利用图片隐写进行控制通信
RegDuke	第一阶段载荷，使用Dropbox作为控制基础设施
MiniDuke	汇编实现的第二阶段木马
FatDuke	第三阶段植入的复杂后门

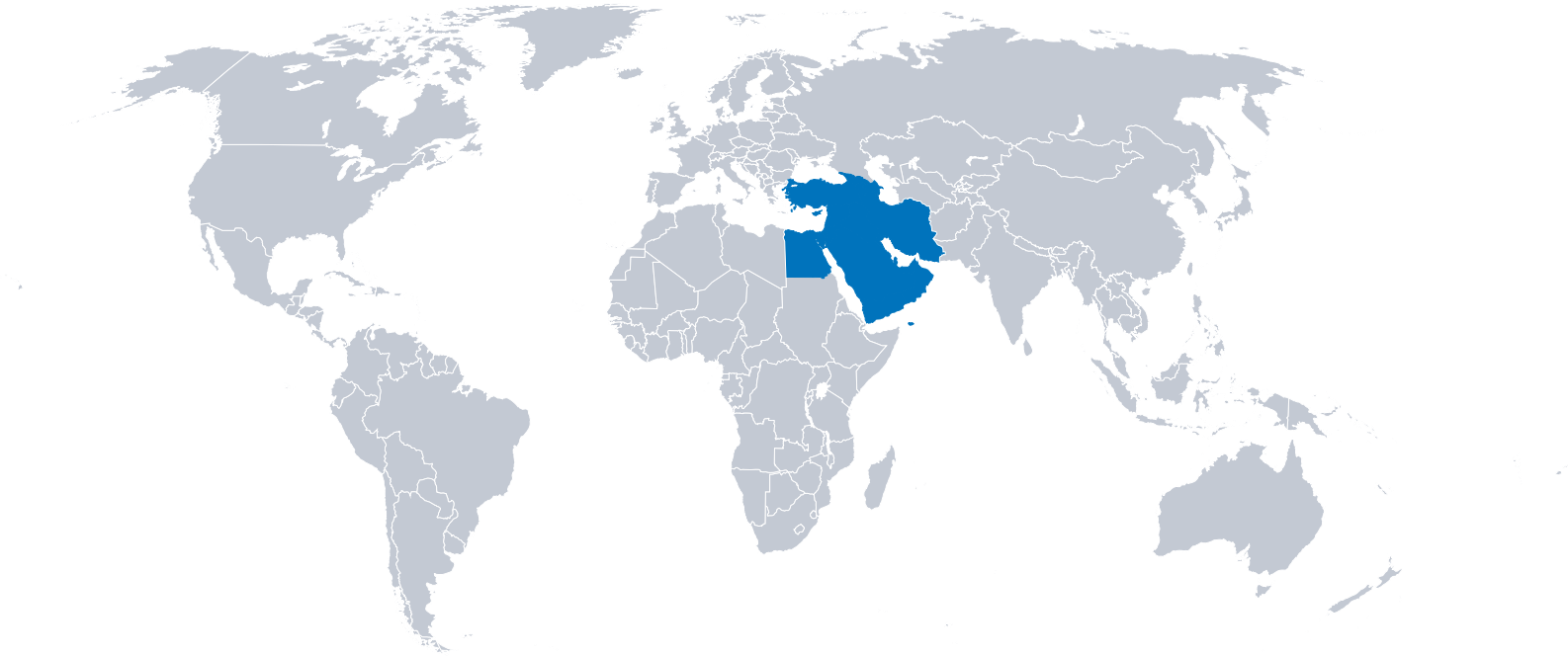
Turla是另一个古老而又富有创新性的APT组织，其在针对Exchange邮件服务器的后门程序中将其伪装成Transport Agent实现持久性。Turla还被发现其通过劫持APT34的控制基础设施用于自身的攻击活动[52-54]。

卡巴在VB2019会议上还披露了疑似与Turla有关的Reducor RAT工具[57]，其通过patch FireFox和Chrome浏览器中的伪随机数生成函数，在目标受害者进行TLS握手阶段，在生成的随机数中添加了对受害者的标识。

攻击工具名称	功能说明
LightNeuron	针对Exchange邮件服务器的后门
–	定制Posh-SecMod的PowerShell加载器
ComRAT	第二阶段后门
PowerStallion	PowerShell实现的后门，利用OneDrive作为C&C
Topinambour	.Net下载器，用于分发KopiLuwak
KopiLuwak	JavaScript木马，其似乎还存在一个PowerShell版本
Reducor	RAT工具

Gamaredon group是由Palo Alto Networks最早披露的针对乌克兰的APT组织，据公开资料，乌克兰安全局SBU在过去将该组织与东欧某强国联系到一起[58]。相对于上述三个组织来说，Gamaredon使用的攻击能力似乎较弱，其利用SFX诱饵或者模板注入技术分发和植入自定制的Pteranodon载荷。

（五）中东



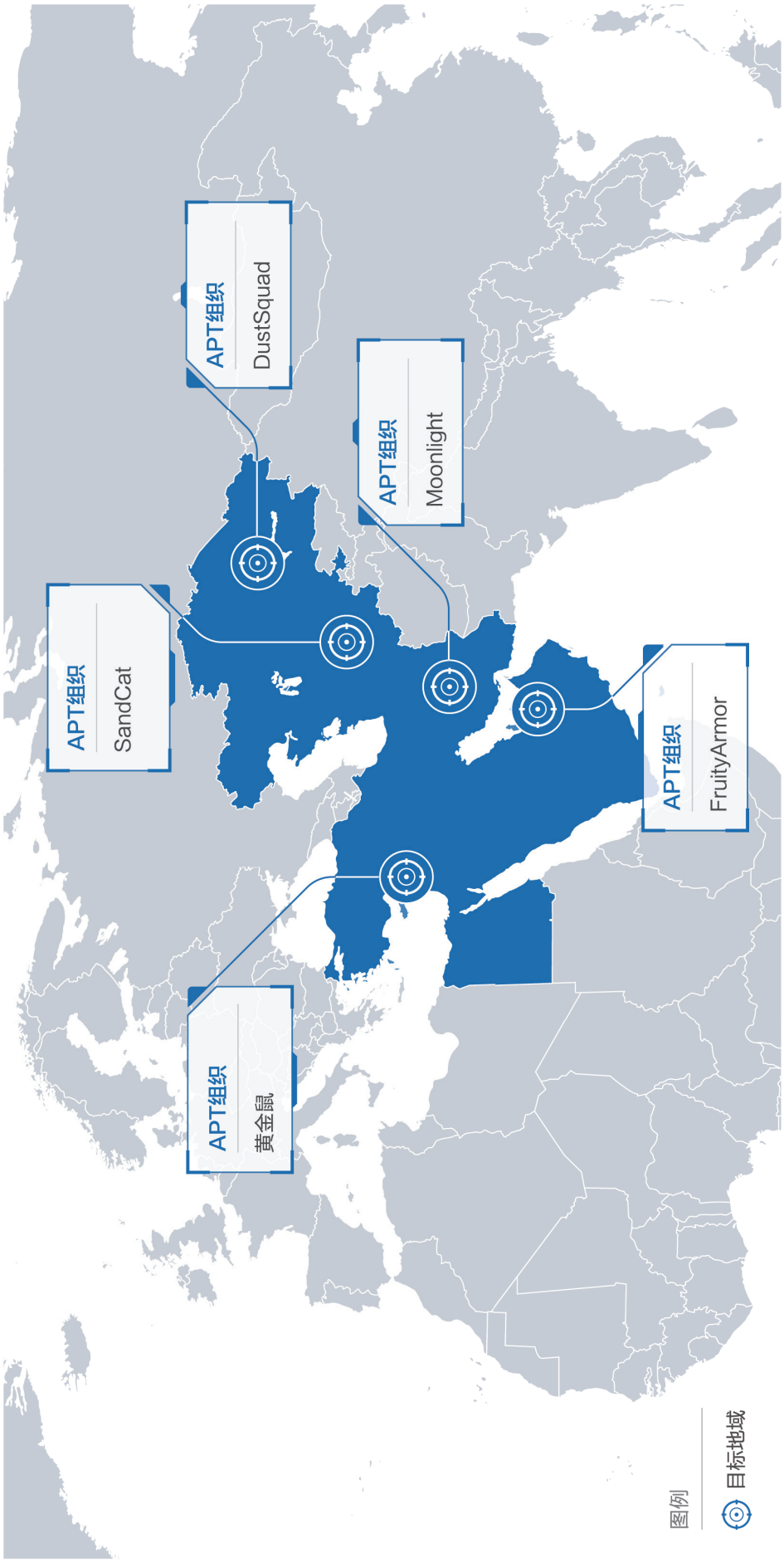
中东地区，具有着极为复杂的政治外交局势，其地域下充满了疑似政府背景的情报监控活动，网络间谍活动。结合公开情报来看，虽然中东地区APT组织的攻击能力整体并不高，但其会大量依赖网络武器库交易来实现自身的网络攻击能力。

APT33，APT34和MuddyWater是被公开认为是中东地区某国背景的三个比较活跃的APT组织，其攻击活动似乎并未因为其武器库和攻击人员资料被泄露而停止。

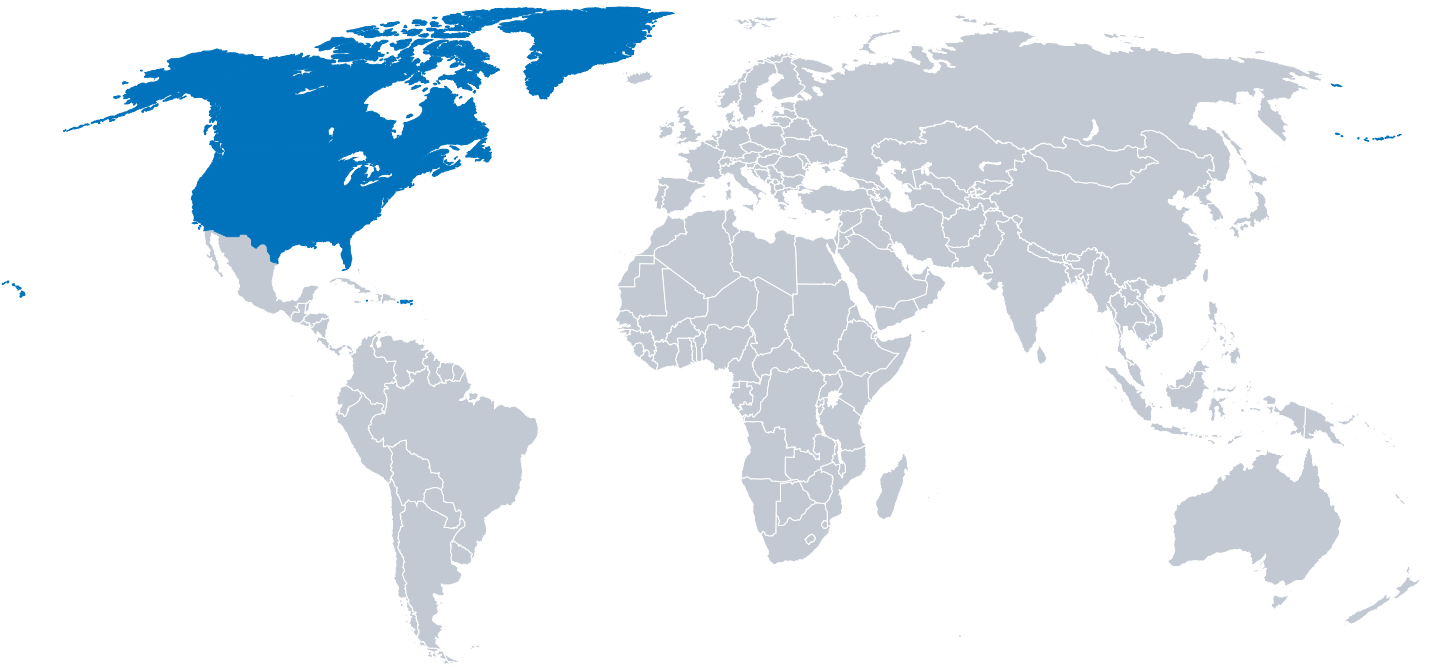
上述的三个APT组织，其偏好基于鱼叉钓鱼邮件，社工等方式建立攻击立足，其会开发自定义的攻击程序，并多使用脚本类和公开工具。我们从其上半年泄露的网络武器工具来看，其网络武器的构建能力相对较弱。我们在年中的报告中也曾总结过APT34（OilRig）组织泄露的网络武器库。

攻击工具名称	功能说明
Poison Frog	Powershell后门，通过DNS和HTTP通信，也称为BONDUPDATER
Glimpse	Powershell后门，通过DNS通信，也称为Updated BONDUPDATER
多个Webshell	FoxPanel222、HighShell、HyperShell、Minion
webmask	Python实现的DNS劫持和中间人攻击工具，Cisco Talos也称为DNSpionage
Jason	Exchange密码爆破工具

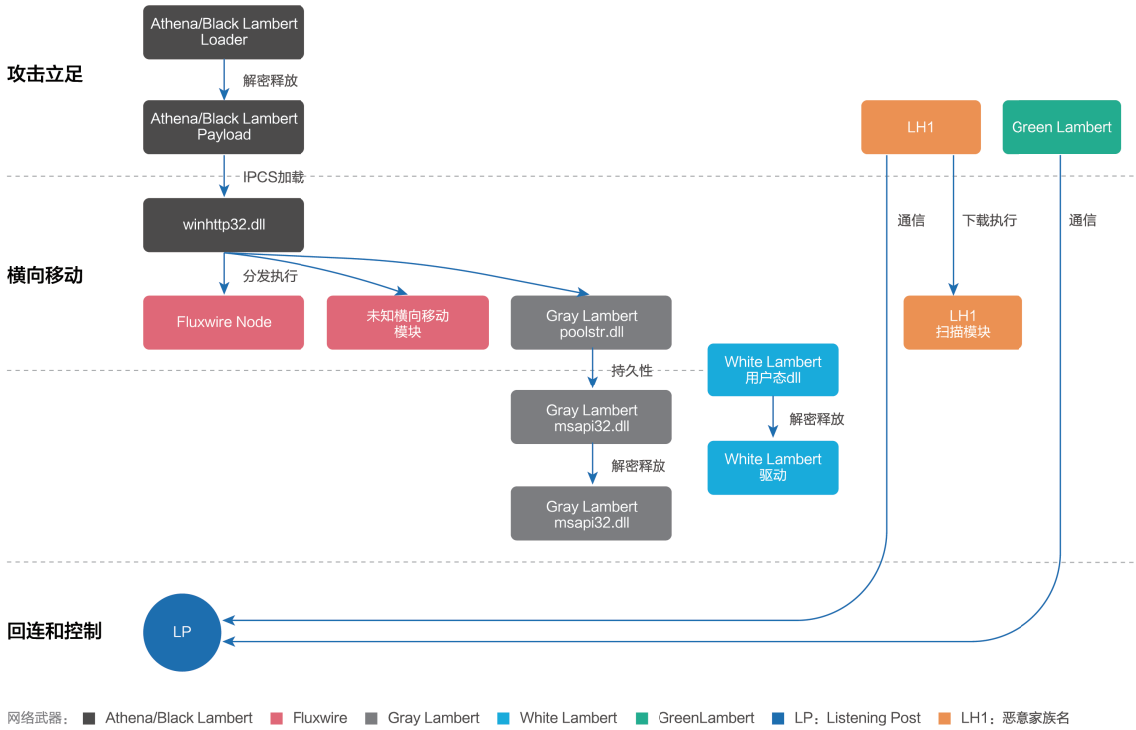
除此以外，中东还活跃着数个APT组织，其主要攻击目标通常为本国的目标人员或周边地缘的目标人员，以实施持续的网络监控和间谍活动为目的。


APT组织 DustSquad
APT组织 Moonlight
APT组织 SandCat
APT组织 FruityArmor
APT组织 黄金鼠
图例
目标地域

（六）北美



奇安信威胁情报中心今年发布了一份详细分析某国情报机构相关的网络武器库的报告，其中涉及了至少8个不同的攻击程序类型。我们结合了赛门铁克和卡巴斯基的历史报告，以及维基解密披露的Vault7项目资料，最终将公开的项目代号或恶意代码命名与实际的攻击程序相对应，并结合攻击程序功能我们推测了其在实际攻击活动中被使用的攻击阶段和关联性。公开的研究人员也将此背景的网络武器库统一按照Lamberts（又名Longhorn）命名来跟踪。



自维基解密网站公开曝光某国情报机构下EDG部门开发的网络武器库资料以来，似乎攻击并未因此而停止，国外安全厂商ESET在今年也披露了一份关于Lamberts的报告[59]，其中介绍了攻击活动从2017年3月以来就一直处于活动状态，并且攻击了中欧和中东的少数机构。我们从其报告介绍来看，似乎部分特征也存在于我们分析的攻击工具集中。

结合过去的披露和研究基础来看，北美APT组织的网络武器库从最初构建时就是积木式的，在实际使用时会根据目标和攻击策略进行定制化组装。由于构建整个武器库所需要的资源和人力是巨大的，所以完全抛弃其历史的网络武器库而重新构建的代价也是极高的，也许这也是我们发现其攻击载荷和历史活动中使用的依然存在一些代码功能的重叠的原因。但由于其攻击操作安全（OPSec）做的足够好，导致对攻击载荷的完整捕获极为困难，也导致了在复盘分析和事件还原过程中缺失了很多关键环节。

（七）其他

南美地区也许是另一个容易忽视的APT活跃地区，奇安信威胁情报中心在今年也发现和披露了一个新的APT组织“盲眼鹰”，其从2018年4月起就一直针对哥伦比亚政府机构和大型公司（金融、石油、制造等行业）等重要领域展开了有组织、有计划、针对性的长期不间断攻击。其攻击平台主要为Windows，利用鱼叉邮件和诱饵文档投递最终的Imminent后门程序。

盲眼鹰并不是南美地区唯一发现的APT组织，另一个由卡巴最早发现和命名的APT组织Machete，其最早活动被发现从2010年开始，其主要针对拉美地区国家说西班牙语的人员，而在今年其又被安全厂商发现新的攻击活动并且针对军事相关目标人员，该组织主要使用

Python语言开发的后门并编译成可执行文件进行分发。

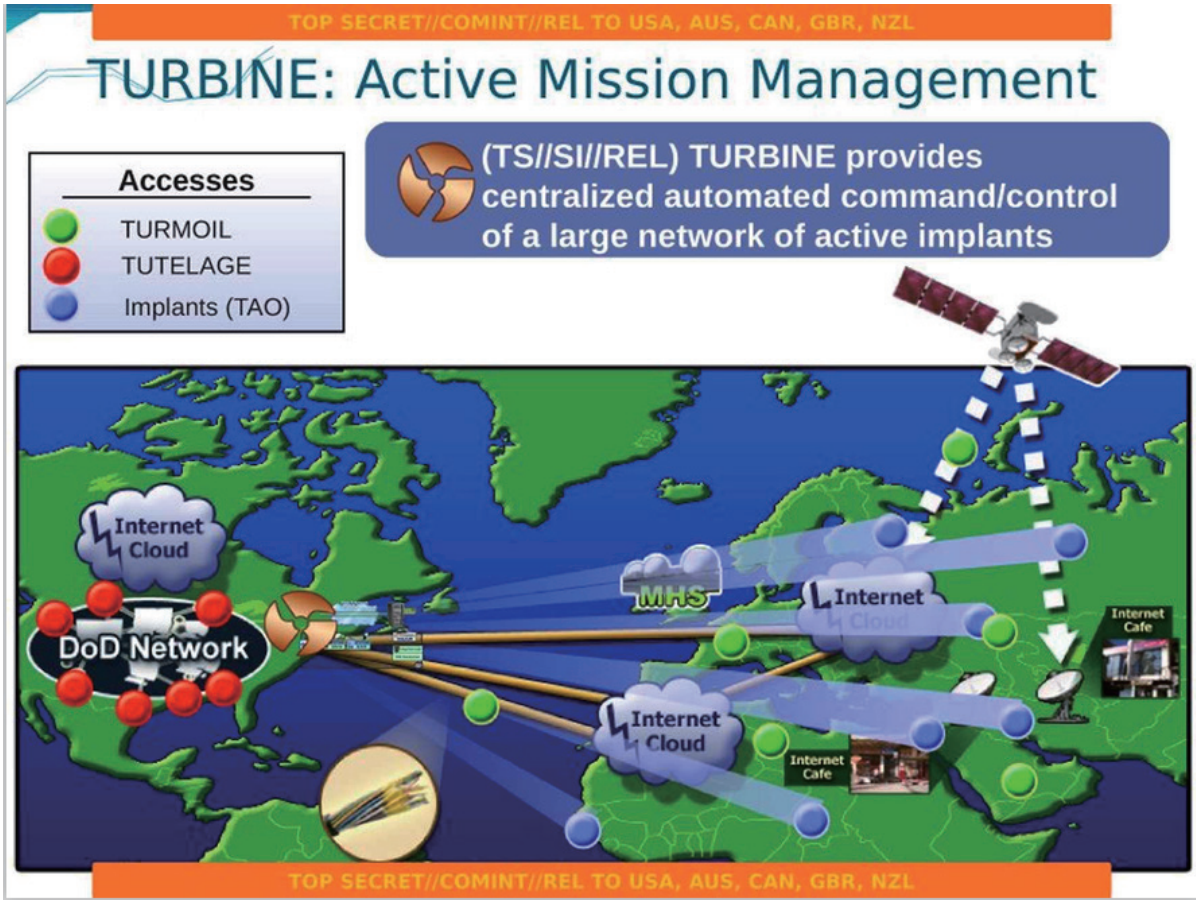
另外值得一提的是，Regin恶意软件被发现重新活跃[50]。今年6月，路透社披露在2018年10月至11月，Regin新的变种被发现用于攻击俄罗斯的Yandex公司。Regin在过去已被公开认为是由某个知名的政府间情报联盟共同制作的攻击平台，曾被用于攻击比利时电信公司Belgacom。也有安全研究人员也分析推测了Regin可能就是代号DAREDEVIL和WARRIORPRIDE项目的结合[60]。

二、广域网下的APT威胁

从过去的APT威胁研究来看，绝大多数的APT威胁场景依然在受害目标所属的组织机构网络下，APT攻击需要选择合适的攻击入口突破企业网络边界，并且在攻击达成后通过网络基础设施进行命令控制或数据渗出。

APT组织通过构建诱饵文件或是利用失陷网站实施鱼叉邮件和水坑攻击并诱导目标点击触发载荷的执行和恶意网站的访问，从而获得初始的攻击立足。而在过去，部分APT组织和攻击活动利用广域网的网络协议，实施DNS劫持、BGP劫持，以达到对广域网下流量的重定向，劫持和中间人攻击的目的。

在历史斯诺登泄露的文档中，曾披露过某国通过其具备的广域网下部分骨干节点的控制能力而建立的TURBULENCE项目，并用于数据监听和情报收集[67]。其包含TURMOIL项目用于互联网络上的被动信号情报收集，TURBINE是基于自动化和批量化攻击植入的系统实现主动信号情报收集。而后续QUANTUM INSERT项目实现的man on the side攻击技术以及将目标重定向到FOXACID服务器，也是基于TURBULENCE实现的。下图参考自公开文章[67]。



而对于APT组织来说，往往不具备对因特网核心基础设施的控制能力，其只能通过广域网的劫持攻击来达到类似的目的。

我们收集和列举了近两年来针对DNS和BGP劫持的恶意攻击活动。

2018.01

ESET 安全厂商披露 Turla 可能利用对 ISP 的流量劫持或者 BGP 劫持手段用于向目标分发虚假恶意的 Flash Player 安装器 [26]，而该组织曾在 2015 年也被发现过利用类似的劫持手段用于其攻击活动。

2018.04

有攻击组织通过劫持 BGP 窃取数字加密货币 [23]。

2018.11

Google 发现其网络流量被劫持，后续尼日利亚 ISP MainOne 声称其错误配置了 BGP 导致事件的发生 [24]。

2018.11

Cisco Talos 披露其发现疑似波斯湾某国利用 BGP 劫持对 Instagram 和 Telegram 用户的攻击 [25]。

2018.11

Cisco Talos 披露了名为 DNSpionage 的行动，其劫持了 DNS 用于攻击黎巴嫩、阿联酋政府部门 [30]。

2019.01

FireEye和Crowd-Strike同时披露疑似波斯湾某国实施的DNS劫持，主要影响了中东和北非地区的包括政府、电信和互联网基础设施实体 [28、29]。

2019.04

Cisco Talos 披露了名为 Sea Turtle 的攻击活动，其利用 DNS 劫持攻击了至少 13 个国家的 40 个组织，并且用于 VPN 凭据收集和中间人攻击 [31]。

2019.05

我国台湾地区网络中心（TWNIC）运行的 Quad101 DNS 系统遭受 BGP 劫持，路由重定向到巴西的某个实体，并持续了三分半钟 [19]。

2019.07

英国 NCSC 机构发布了 DNS 劫持攻击的预警，包括涉及 Sea Turtle 活动和在巴西超过 18 万台路由器被黑客攻击并篡改了 DNS 配置事件 [32]。

针对因特网广域网下的DNS劫持、BGP劫持可以让攻击者重定向目标的网络流量到自身的控制基础设施，从而实现数据监听、收集、中间人攻击的目的，并且为广域网提供基础设施服务的ISP、域名服务商、CDN服务商都有可能成为APT威胁的目标。

三、利用供应链攻击实施APT活动

利用供应链的攻击在APT活动中时常有发生，我们在年中的报告中也总结过上半年的APT类供应链攻击活动。

下表整理了2019年的APT类供应链攻击活动。

披露时间	披露厂商	针对目标	相关APT组织/行动	概要
2019.1.16	Trend Micro	在线广告公司	MageVcart	通过植入在线广告公司的JavaScript库来感染电子商务网站 [33]
2019.3.11	ESET	游戏开发人员	Winnti	针对游戏行业的供应链攻击 [34]
2019.3.25	Kaspersky	华硕	ShadowHammer	在预装的ASUS Live Update程序植入后门，通过匹配用户 mac 地址实施针对特定目标的攻击 [35]
2019.5.14	ESET	华硕	BlackTech	疑似攻击华硕 WebStorage [38]
2019.5.14	RiskIQ	CMS、分析服务提供商、广告平台提供商、Web应用的IT提供商	Magecart	针对网站多类供应商的攻击 [39]
2019.9.18	Symantec	IT供应商	Tortoiseshell	通过攻击沙特阿拉伯的IT提供商以达到攻击其客户的目的 [37]
2019.10.3	Context	合作伙伴、供应商	AVIVORE	针对英国和欧洲航空航天与国防的攻击 [36]

从过去的供应链攻击来看，其一方面通过攻击软件供应链的各个环节，包括第三方库的引用，开发人员，产品构建阶段，另一方面通过攻击和目标相关的IT供应商、软件供应商、硬件供应商、合作伙伴等。其针对带有签名的合法应用、预装程序植入后门，能够实现更加隐蔽的攻击立足效果。

四、网络军火、0day与APT威胁

0day漏洞一直是作为实施APT攻击的重要利器，无论是影子经纪人黑客组织泄露的NSA武器库中曝光了大量的0day漏洞利用装备，还是维基解密披露的Vault7项目中CIA用于管理的针对Android和iOS的漏洞利用列表文档，都展示了0day漏洞或成熟的漏洞利用链是实施网络攻击利用的关键能力。

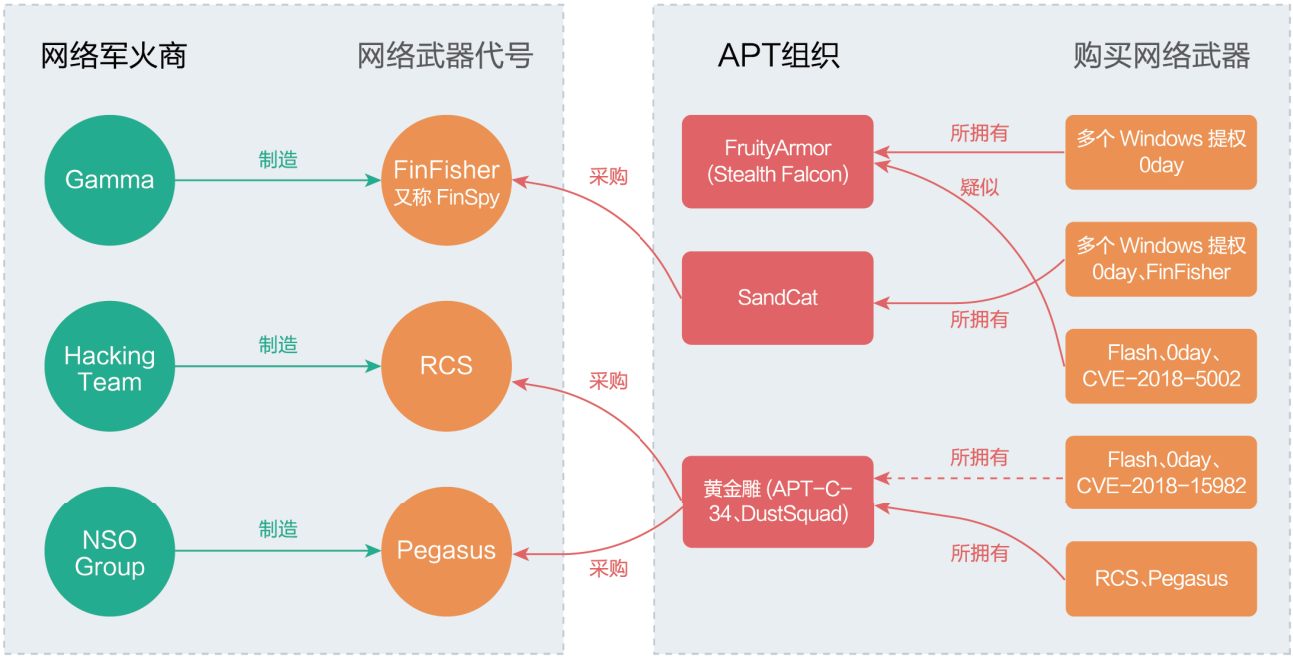
我们整理了2019年用于在野攻击活动的漏洞列表（见下表）。相比2018年来说，在野攻击活动中利用的文档型0day漏洞并未发现，针对浏览器的远程代码执行漏洞数量提升，并且配合沙盒逃逸和提权漏洞使用。

漏洞编号	漏洞类型	是否0day	是否在野利用	利用的APT组织	披露厂商
CVE-2018-20250	WinRAR ACE路径穿越漏洞	否	是	多个APT组织	Check Point[17]
CVE-2019-0797	Windows提权漏洞	是	是	FruityArmor、SandCat[14]	Kaspersky
CVE-2019-5786	Chrome UAF	是	是[15]	未知	官方披露
CVE-2019-0808	Windows提权漏洞	是	是[15]	未知	官方披露
CVE-2019-0859	Windows提权漏洞	是	是[16]	未知	Kaspersky
CVE-2019-1132	Windows提权漏洞	是	是	Buhtrap[13]	ESET
CVE-2019-1367	IE JScript	是	是	Darkhotel[12]	官方披露
CVE-2019-13720	Chrome	是	是	Operation WizardOpium[10,11]，疑似 DarkHotel	Kaspersky
CVE-2019-1458	Windows提权漏洞	是	是	Operation WizardOpium[10,11]，疑似DarkHotel	
CVE-2019-0708	RDP	否	是[8]	非APT	安全研究人员
CVE-2019-11707 CVE-2019-11708	Firefox	是	是[9]	未知	官方披露
CVE-2018-6055	浏览器	否	是	虎木槿	奇安信
CVE-2019-7287 CVE-2019-7286	iOS	是	是	未知	Google[18]
CVE-2019-6225 CVE-2019-8518	iOS	否	是	未知	Google[18]
CVE-2019-2215	Android	是	是	NSO	Google[27]
CVE-2019-3568	WhatsApp	是	是	NSO[7]	官方披露

但不是所有的APT组织都完全具备0day漏洞的挖掘能力，所以0day漏洞也一直作为网络武器在地下市场买卖交易。例如卡巴斯基在过去发现和披露了某熟悉俄语或乌克兰语的黑客在地下论坛以BuggiCorp的ID贩卖0day漏洞，卡巴以内部代号Volodya进行跟踪。在WizardOpium行动中使用的CVE-2019-1458以及APT28历史使用的CVE-2016-7255都被认为是购买的该黑客开发的0day漏洞。

网络军火商是另一个在0day漏洞和网络武器交易市场的重要角色，像Gamma、Hacking Team、NSO Group都是知名的网络军火商，其开发一套完备的网络监控系统并出售给其客户。

在过去，披露最多的网络军火商的客户大都是活跃在中东地区的APT组织，并且通常具备国家情报机构背景，其通常用于监控人权组织、异见人士、记者、本土的外交人员等等以达到其政权控制的意图。



网络军火商的存在大大降低了部分APT组织实施网络攻击活动所需的能力，而网络武器的制作者和实施攻击活动的真实来源被完全分隔开来，难以通过网络武器本身对实际的攻击组织进行追溯和定位。

五、网络战与CNA

网络战往往可能伴随着国际形势变化，军事冲突，政治外交手段，地缘冲突等因素，其也可能出现和军事行动相结合。如同在序言中所说，网络战成功的基础则是很大依赖于对潜在目标的了解，所以针对潜在目标的网络利用和情报收集往往用来弥补对对手认知的缺失，并且进行针对性的武器化储备。

与现实的军事行动不同的是，由于网络攻击更容易隐匿攻击源头导致行动难以归因，并且双方都不总是公开承认，使得实施网络战造成的国际舆论影响远小于发起一次军事行动，并且达成可能类似的行动效果。

由于真实的网络战活动难以实际观测到，也难以和APT组织本身联系起来，我们仅从公开披露的新闻事件列举出这一年发生的疑似网络战事件列表。

六、移动终端场景的APT威胁

针对智能手机的攻击是APT威胁的另一个威胁场景，其主要的目的在于实现监控和窃听，并针对特定的个人或群体。在过去的移动APT活动中，通常通过远程代码执行漏洞、钓鱼消息或者将间谍软件混入应用市场等方式在智能手机中植入后门程序，获取包括短信、通讯录、定位、文件、应用数据、录音和录像的数据。

在手机间谍应用和监控系统的背后，不乏存在不少网络军火商的身影，包括NSO、Hacking Team、Gamma都提供针对Android、iOS的监控系统和木马，并且利用漏洞利用链植入后门程序。在2019年中，老牌的网络军火商依旧持续提供更新版本的间谍服务。例如卡巴斯基发现FinSpy针对Android和iOS的新版本[40]；还有一份公开的Pegasus产品文档也展示了NSO Group提供了极其完备的移动终端监控服务，而Pegasus正是之前NSO利用3个针对iOS的0day漏洞攻击中东某政治人士的植入程序。

新的网络军火商正在开发制作新的间谍木马。在2019年3月安全研究机构也披露了名为Exodus 的新的间谍软件平台[41]，并将其与一家欧洲公司eSurv联系到了一起。

针对移动终端的0day漏洞和完整利用链在野攻击的爆发。今年8月，Google Project Zero团队披露了一个针对iOS 10到iOS 12几乎所有版本的在野攻击案例，其使用了5个完整漏洞利用链，总共14个漏洞，其中7个都是针对iPhone的Web浏览器[18]。后续公民实验室也发布了相关事件中针对Android系统的漏洞利用[42]。

APT组织开发移动终端木马程序用于APT活动。APT组织中同时具备移动端攻击武器的包

括了Group 123、蔓灵花、肚脑虫、黄金鼠、拍拍熊等等，其通常利用社工、聊天应用、钓鱼等方式诱导目标安装伪装的手机木马程序，以收集目标收集上的信息。

国家情报机构背景的移动终端监控。在历史泄露的某国情报机构资料中，多次提及其针对移动智能终端的攻击利用工具。在今年1月，路透社曝光了一个名为Raven的项目，其是由某国情报机构和中东某国政府共同开发和构建的网络攻击工具，其中的Karma间谍平台用于攻击iPhone设备，其用来监听包括激进分子，政治领导人和恐怖分子嫌疑犯等[43]。除了直接攻击智能终端本身，还有通过攻击运营商，移动蜂窝网和信令系统，以及移动通信协议来实现数据监听、定位的能力。例如今年在VB2019会议上披露的Simjacker漏洞，其通过攻击SIM卡上的应用缺陷实现，并已经被用于攻击南美地区国家的用户手机，我们也曾对该漏洞的原理和危害进行了分析说明，详情可参见奇安信威胁情报中心公众号发布的《5G降级、设备位置跟踪等漏洞被发现，或可用于网络通信军事打击》[44]。

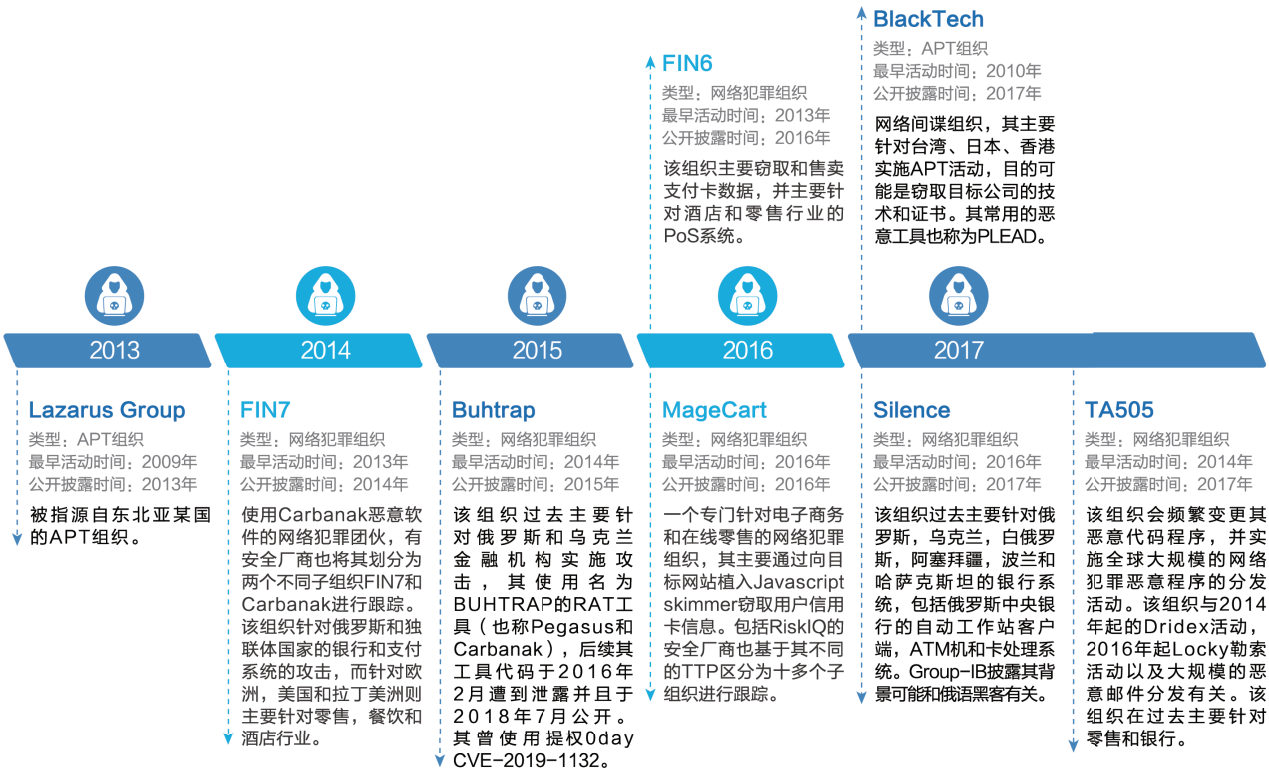
第三章针对行业性的高级威胁活动

APT威胁是定向性的，其会选择攻击的行业、地域、目标以及要达到的目的，这些是由APT组织在实施行动前制定的需要达到的阶段性目标和动机所决定的。从过去的APT威胁来看，APT组织在一段时间内会保持其攻击目标行业的专注程度，这可能也与攻击组织在针对新的行业实施攻击时，需要时间收集和熟悉目标，并弥补自身能力与目标行业的缺失部分，以及构建相应的攻击武器库。

我们在2019年的威胁报告中首次加入从行业视角的APT威胁分析和研究，并且重点关注当年内针对特定行业的活跃攻击组织和攻击活动情况。除了政府、军事相关行业外，金融、能源和电信是APT威胁的主要行业目标，所以本报告对这3个行业在2019年的APT威胁情况进行总结。

一、金融行业

这里，我们将金融行业包括了传统的银行、证券行业以及新兴的数字货币交易所，以及像电子商务，在线的零售商家这些在线交易机构。针对金融行业的攻击主要以牟利为目的，除了像Emotet这样极为流行的银行木马外，也活跃着不少组织化的网络犯罪团伙，其通常拥有自己独立的攻击TTP和定制化的攻击武器集合。少数APT组织同样也针对金融行业目标实施攻击，我们列举了2019年公开披露的主要活跃的针对金融行业的攻击组织。



Lazarus Group最早被发现针对金融银行的攻击是2016年2月，其针对孟加拉国银行SWIFT系统的APT攻击，并试图窃取9.51亿美金[61]。之后该组织就一直针对全球范围的金融银行机构实施攻击活动。由于其牟利的攻击动机和过去实施网络间谍活动和情报窃取不一致，所以一些安全厂商也将其攻击金融银行机构的活动以独立的子组织命名进行跟踪，例如卡巴作为Bluenoroff，FireEye作为APT38。

我们在上表中也列举了多个2019年公开披露过并且持续活跃的网络犯罪团伙。我们总结了网络犯罪团伙在2019年的主要攻击活动。

组织化的网络犯罪团伙和APT组织类似，其会定制化自有的攻击工具集，并且拥有自己的TTP模式。其通常会利用BEC攻击，垃圾邮件，钓鱼等方式活动初始的攻击立足，其也会结合公开或开源的渗透工具，包括Meterpreter，Cobalt Strike和Empire之类，并用于横向移动阶段。我们列举了数个网络犯罪团伙常用的攻击工具。

如FIN6组织的攻击工具集：

攻击工具名称	主要别名	功能说明
FrameworkPOS	Trinity	FIN6常用的针对PoS系统的后门
More_eggs	Terra Loader，SpicyOmelette	JScript后门
Meterpreter	–	公开工具
Cobalt Strike beacon	–	公开工具
TrickBot-Anchor	–	TrickBot变种

FIN7组织的攻击工具集，安全厂商也披露FIN7组织和新的僵尸网络AveMaria的运营有关[62]。

攻击工具名称	主要别名	功能说明
CARBANAK	–	FIN7常用木马
SQLRat	–	一个以SQL Server为控制基础设施的RAT
DNSbot	–	支持DNS，HTTPS和SSL多种通信方式
TinyMet	–	开源的meterpreter stager
GRIFFON	–	轻量级JS植入程序
BOOSTWRITE	–	新的加载器
RDFSNIFFER	–	新的RAT，由BOOSTWRITE加载

TA505网络犯罪组织会频繁新增和变更其攻击工具集，下表也列举了其在2019年活动中使用的攻击木马程序。

攻击工具名称	主要别名	功能说明
ServHelper	–	后门程序
FlawedGrace	–	RAT，由ServHelper下载
FlawedAmmyy	–	常用的远控木马
tRat	–	RAT后门
LOLbins	–	开源工具
AndroMut	Gelup	下载器
FlowerPippi	–	后门
Get2	–	下载器
Snatch	–	RAT，由Get2下载
SDBbot	–	RAT，由Get2下载

而MageCart组织似乎与上述组织有所不同，其主要以攻击目标网站和Web应用的供应链并在失陷的网站和Web程序中植入Javascript实现的skimmer脚本，从而窃取受害用户的信用卡信息。该组织的活动非常频繁，并针对全球化的电子商务平台，在线零售等等。

与APT组织不同的是，网络犯罪组织的主要目的在于牟利，其更换其攻击工具或使用其他的网络犯罪程序更加容易，在网络犯罪的地下市场充斥着商业工具提供者或制作者，服务提供商，运营团伙等多类角色，所以更容易出现工具和恶意程序的重叠。并且由于角色的划分，攻击活动的归属和背后实施攻击活动的运营团伙可能出现变更。例如2018年8月1日，美国DoJ宣布逮捕了涉及FIN7相关的黑客人员，但FIN7的活动并未因此而停止，其极有可能是有新的运营人员接管了相关的攻击工具和网络犯罪平台以持续运营[62]。

从2019年主要的网络犯罪组织和APT组织针对金融行业目标的攻击活动来看，金融银行机构的PoS系统，ATM终端，SWIFT交易系统，以及与电子商务和在线支付相关的网站都是攻击组织的主要攻击对象，并且通过非授权的资金交易转账，获取和售卖支付卡和信用卡数据，以及地下市场交易来进行非法牟利。

二、能源行业

能源行业包括了如石油、天然气、电力、核能、矿业等等领域，无论是从国家经济层面还是社会民生层面都和能源行业息息相关。随着能源行业这些传统行业的组织和机构如今也向着

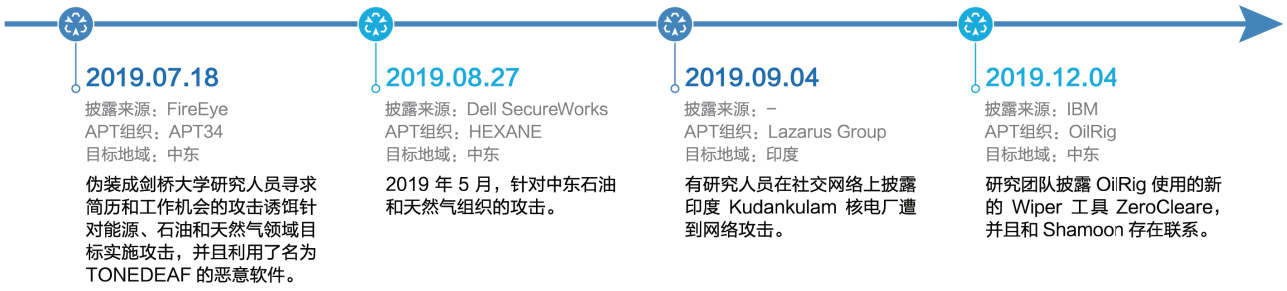
信息化程度的建设，也必然带来了其可能作为网络攻击和网络利用的重要目标之一。

从网络攻击的动机来看，能源行业可能主要面临着APT威胁，其用于在必要时对目标进行破坏和影响，导致目标产线异常甚至出现生产错误。由于能源行业部分也涉及了敏感的信息和数据，其也是APT威胁中的重要目标。

而对于能源行业来说，甚至是扩展到工业控制领域，其主要可以划分为IT和OT两个部分，其网络通常与互联网隔离，重要的工业产线控制甚至是在隔离网络下，并可能由专用的系统和软件加以控制，然而其依然会存在被攻击的风险。在今年，一份外媒报道[63]也披露了当年的Stuxnet事件中，由欧洲某国情报人员招募的一名工程师，由其携带了带有病毒的USB设备并插入到内部系统，从而获得了访问权。

对能源行业目标的攻击和破坏对于国家、社会和民生安定来说影响是巨大的，例如2015年乌克兰的两次停电事件，2019年南美地区包括委内瑞拉、阿根廷和乌拉圭地区的停电事件都对当地人名的生活造成了巨大的影响。虽然今年上半年南美地区的大规模停电事件并没有明确的证据显示和网络攻击有确凿的联系，但结合当年乌克兰的停电事件我们依然可以评估网络攻击针对电力系统的攻击破坏所造成的影响会是巨大的。

我们在这里也列举出2019年公开披露的针对能源行业的APT攻击活动和主要的APT组织。



从公开披露的APT威胁报告来看，中东是针对能源攻击活动的重点活跃地域之一，这也与中东地区复杂的地缘政治因素和已有的丰富能源产业有关。

像OilRig组织，后续国外安全厂商常和APT34进行合并跟踪，能源行业是其主要的目标之一，如知名的Shamoon恶意程序就被公开认为和起相关，并曾经用于攻击和破坏沙特阿拉伯的石油公司造成了其服务停止。

HEXANE，又称LYCEUM，其是由国外安全公司Dragos披露的主要针对工业控制领域攻击的团伙[64]，其最早可能从2018年4月开始活动。其攻击手法被认为和APT33、APT34存在相似，但并未出现明确的线索重叠[65]。

另一个值得关注的是，疑似Lazarus Group在9月-10月期间被发现针对印度Kudankulam核电厂的网络攻击，虽然主要攻击的是核电厂的IT网络，并未进入到OT网络中。该事件中似乎使用了一个Dtrack样本，其用于横向移动阶段，并且硬编码了疑似核电厂相关的登录名称。

三、电信行业

电信行业是另一个APT威胁中的重要目标行业之一，由于电信行业承担着互联网骨干网络和核心基础设施的运营，以及包括电信网、蜂窝网、移动通信和有线电视等。

针对电信行业目标实施APT攻击往往能够建立在更高维度的基础设施控制能力下实现包括劫持、监听、篡改等目的。

我们总结了2019年公开披露的针对电信行业的攻击活动和活跃组织如下：

第四章　2020年高级持续性威胁预测

我们基于2019年APT威胁的趋势以及近年来APT威胁组织和活动的变化情况对2020年高级持续性威胁进行预测。

一、APT威胁归因困难导致攻击归属命名更加碎片化

奇安信威胁情报中心一直在收集、分析和研判全球范围APT类威胁的归属命名和公开披露情报，但我们发现APT威胁的归因问题变得更加复杂和困难。

APT攻击组织在实施攻击活动的操作安全上变得更加谨慎，并且利用多种方式避免其行为特征被发现和关联，在过去我们看到了攻击组织使用如下的方法：

- 频繁更换攻击程序的形态，避免代码重用；
- 利用和定制化公开的或开源的攻击工具，利用脚本语言和商业工具；
- 利用无文件攻击技术尽量避免攻击载荷的留存；
- 利用本地命令，也称为live off the land攻击；
- 故意留下假旗标志误导安全分析人员；
- 劫持其他攻击组织的控制基础设施。

归因的问题最终导致了归属命名的碎片化，从而依赖于更丰富维度的元数据和线索证据来佐证最终的归因判定。

另外，一些高价值目标可能会同时作为不同APT组织的攻击目标，造成攻击活动重叠的冲突，也可能给归属分析判定带来影响。

二、出现更多的在野0day攻击案例

在2018年的全球高级持续性威胁报告中，我们总结了在2018年公开披露的在野攻击活动中利用的0day漏洞总共有14个，涉及明确的攻击组织6个。在2019年的报告中，我们总结了2019年内公开披露的在野攻击活动中利用的0day漏洞总共有17个，涉及明确的攻击组织至少7个，相对于2018年来说略有增长。然而2019年的0day攻击案例中，似乎并未出现新的文档型漏洞的利用，并且随着Adobe Flash生命的完结，未来利用Flash的漏洞可能会越来越少。

在2019年中，针对浏览器的完整利用链在被曝光的在野攻击活动中出现的越来越多，不光是针对PC，还有针对Android、iOS移动设备，其漏洞利用往往需要更少的用户交互即可完成。从趋势上来看，我们也认为未来会出现更多的在野0day攻击案例。

三、针对行业性的APT威胁越发凸现

我们预测在未来针对行业性的APT威胁活动会越来越多，也就是说APT威胁活动不光局限于政府、国防、军工、外交等领域的目标，金融、能源和电信也可能作为未来APT威胁中的重点攻击目标。

从今年的威胁活动来看，网络犯罪团伙正向着高度组织化，高度武器化和高度战术化的趋势发展，其大多拥有一套自定义的攻击工具集和战术技术过程。以牟利为动机的针对金融银行行业的攻击活动，不光是针对受害用户自身的在线资金的攻击（包括银行卡信息盗窃），还会针对金融机构本身的系统、终端、网络实施攻击活动，并尝试获得更大的战果。

从APT攻击的动机来看，金融、能源和电信是高度符合攻击组织需要的，通过攻击金融银行机构实现所需资金的补充，攻击能源行业会对目标国家发展和社会安定的破坏，甚至获取重要的情报，例如针对核能领域的攻击，以及攻击电信通信行业能够获取到骨干网或核心网络基础设施的控制权。

由于APT威胁可能针对特定行业实施，攻击组织在筹备攻击活动以前会更多的尝试对目标行业情况进行情报收集，并积极弥补和目标的技术差距，并针对性构建攻击工具集。因此，攻击组织需要准备更加针对性的攻击能力和攻击战技术。

四、5G商业化和物联网或为APT威胁提供新的控制基础设施

今年，5G正在向商业化的趋势发展，5G网络提供的高质量和高速率的网络通信能力必将为物联网带来进一步的发展空间。物联网设备，家用智能设备，路由器，甚至智能手机等在未来都可能以某种形式连接在一起，然而其中的终端设备安全良莠不齐必然导致存在诸多的安全风险。

从过去的VPNFilter事件，名为Inception Framework APT组织利用路由器UPnP功能最为代理隐藏自身，可以看出基于物联网设备的攻击活动不再是网络黑客的专属，其同样会被应用到APT威胁攻击中。并且从2016年Mirai造成美国东海岸断网事件来看，其同样可以用于网络攻击破坏中，以瘫痪目标网络和基础设施服务。

五、更加频繁和隐蔽的网络攻击破坏活动

2019年从公开报道和披露，有不少疑似与网络攻击或者疑似网络攻击造成的破坏活动，其主要和电力系统，政府机构，核电厂，炼油厂相关。网络攻击所造成的破坏活动能够瘫痪目标系统或者造成目标运转的异常，最终导致国家发展、社会民生造成不安定的影响。

网络攻击破坏活动相对于军事行动来说，更加具有隐蔽性和溯源难的特点，从而攻击源头可以进行否认。由此可以预见未来网络攻击破坏活动可能更加频繁。

第五章　针对高级持续性威胁的分析和对抗

在本年度全球高级持续性威胁报告的最后，我们结合APT类威胁的趋势以及奇安信威胁情报中心过去在APT威胁分析研究的经验，在这里我们也提出在APT威胁分析和对抗中的几个观点，以供业界参考和讨论。

一、元数据是应对高级威胁的数据基础

从美国 DoJ 在2018年9月公开对朝鲜一名黑客成员和 Lazarus APT 组织的长达179页的指控书中[68]，其详细阐述了调查人员如何将历史的APT 攻击事件和Lazarus APT 组织以及朝鲜黑客成员通过电子证据联系到一起，其中涉及的数据维度包括：

- 针对攻击事件和被攻击目标的事件响应和取证证据；
- 邮件、社交网络数据、在线互联网应用和服务数据；
- 第三方安全厂商提供的威胁数据和分析结果；
- 公开来源威胁情报；
- 网络基础设施的历史信息，域名注册，动态域名注册，DNS记录等；
- 搜索历史，包括搜索引擎，社交网络应用搜索记录等；
- 终端设备指纹和设备访问互联网实体的记录；
- IP维度的访问互联网实体记录；
- 黑客论坛，黑客技术交流社区等相关数据；
- 安全厂商或团队的协助。

在179页的指控书中举证的不同维度元数据之间的关联性证据多达856条。

833	328	tty198410@gmail.com	register	mrkimjin123@gmail.com	
834	328	tty198410@gmail.com	access by same device	mrkimjin123@gmail.com	20141113
835	328	tty198410@gmail.com	access by same Proxy Service IP	mrkimjin123@gmail.com	20141214
836	328	MrDavid0818@gmail.com	access by same device	mrkimjin123@gmail.com	
837	328	Singapore VPN IP	access	mrkimjin123@gmail.com	
838	328	Singapore VPN IP	access	mrdavid0818@gmail.com	
839	328	Singapore VPN IP	access	tty198410@gmail.com	
840	329	mrkimjin123@gmail.com	access by same Proxy Service IP	surigaemind@hotmail.com	20120930
841	330.a	North Korean IP Address #4	access	ttykim1018@gmail.com	
842	330.a	North Korean IP Address #8	access	ttykim1018@gmail.com	
843	330.b	North Korean IP Address #4	access	business2008it@gmail.com	
844	330.b	North Korean IP Address #8	access	business2008it@gmail.com	
845	330.b	North Korean IP Address #7	access	business2008it@gmail.com	
846	330.c	North Korean IP Address #3	access	surigaemind@hotmail.com	
847	330.c	North Korean IP Address #4	access	surigaemind@hotmail.com	
848	330.c	North Korean IP Address #7	access	surigaemind@hotmail.com	
849	330.d	North Korean IP Address #4	access	pkj0615710@hotmail.com	
850	330.d	North Korean IP Address #7	access	pkj0615710@hotmail.com	
851	330.d	North Korean IP Address #8	access	pkj0615710@hotmail.com	
852	333.a	tty198410@gmail.com	contacts email addresses	ttykim1018@gmail.com	
853	333.b	tty198410@gmail.com	contacts email addresses	ttykim1018@gmail.com	
854	333.b	ttykim1018@gmail.com	use	getnotify.com	
855	333.b	surigaemind@hotmail.com	contacts email addresses	ttykim1018@gmail.com	
856	333.e	pkj0615710@hotmail.com	contacts email addresses	Hyon_u@hotmail.com	
857	333.f	mrkimjin123@gmail.com	access by same device	tty198410@gmail.com	20141113

在如今APT威胁的归因分析越来越困难的趋势下，构建更广维度的元数据集合以及元数据间直接或间接的关系图将会作为APT威胁关联和归属判断的重要依据。

二、构建高级威胁组织知识库

奇安信威胁情报中心一直致力于构建全球范围高级威胁组织和活动的知识库，由于APT类威胁归属命名的碎片化造成的“混乱”现象，导致在APT威胁追踪时往往不能明确两个命名归属的威胁活动是否关联或者是否需要合并导致给最终的归因分析造成困扰。

收集、分析和运营APT类威胁情报，构建围绕攻击组织或活动、情报来源、攻击武器或工具以及网络威胁情报指标四个维度的知识库能够帮助我们在APT威胁分析中研究攻击源头及其演变，以及研究APT威胁的现状和发展趋势。

奇安信威胁情报中心在今年也对外披露了一批我们收录的攻击组织和活动，及其归属的攻击工具集的Hash[66]，旨在向业内和研究APT威胁的机构和研究团队贡献出一份知识库。详情可参见奇安信威胁情报中心发布APT数字武器陈列项目：https://github.com/RedDrip7/APT_Digital_Weapon

三、高级威胁对抗需要人机结合

APT攻击组织正变得更加聪明和狡猾，因此对于APT攻防来说，最终是攻防双方背后人的角力，思路的角力，寄希望于机器完全解决APT防御的问题似乎是不可能的。高级威胁对抗需要人机协同，机器解决海量数据中筛选异常和可疑的行为并推荐给有经验的威胁分析师，并且从已知的元数据集中挖掘相关的碎片，由分析师最终将碎片化的证据形成证据链从而还原真实的攻击场景，并且最终完成知识库的更新。

附录1　奇安信威胁情报中心简介

奇安信威胁情报中心是奇安信集团旗下的威胁情报专业机构。该中心以业界领先的安全大数据资源为基础，基于长期积累的核心安全技术，依托亚太地区顶级的安全人才团队，结合强大的数据分析能力，实现全网威胁情报的实时、深入、全面综合分析，为企业和机构提供网络空间威胁防护的情报预警及分析能力。

奇安信 ALPHA威胁分析平台（https://ti.qianxin.com），是奇安信集团面向安全分析师和应急响应团队提供的一站式云端服务平台，该平台拥有海量互联网基础数据和威胁研判分析结果，为安全分析人员及各类企业用户提供基础数据的查询、攻击线索拓展、事件背景研判、攻击组织解析、研究报告下载等多种维度的威胁情报数据与威胁情报服务，提供全方位的威胁情报能力。

微信公众号：

奇安信威胁情报中心：

奇安信病毒响应中心：

附录2 红雨滴团队（Red Drip Team）简介

奇安信旗下的高级威胁研究团队红雨滴（RedDrip Team，@RedDrip7），成立于2015年（前身为天眼实验室），持续运营奇安信威胁情报中心至今，专注于APT攻击类高级威胁的研究，是国内首个发布并命名“海莲花”（APT-C-00，OceanLotus）APT攻击团伙的安全研究团队，也是当前奇安信威胁情报中心的主力威胁分析技术支持团队。

目前，红雨滴团队拥有数十人的专业分析师和相应的数据运营和平台开发人员，覆盖威胁情报运营的各个环节：公开情报收集、自有数据处理、恶意代码分析、网络流量解析、线索发现挖掘拓展、追踪溯源，实现安全事件分析的全流程运营。团队对外输出机读威胁情报数据支持奇安信自有和第三方的检测类安全产品，实现高效的威胁发现、损失评估及处置建议提供，同时也为公众和监管方输出事件和团伙层面的全面高级威胁分析报告。

依托全球领先的安全大数据能力、多维度多来源的安全数据和专业分析师的丰富经验，红雨滴团队自2015年持续发现多个包括海莲花在内的APT团伙在中国境内的长期活动，并发布国内首个团伙层面的APT事件揭露报告，开创了国内APT攻击类高级威胁体系化揭露的先河，已经成为国家级网络攻防的焦点。

红雨滴团队LOGO：

“红雨滴”背后的故事——“从100亿个雨滴中找一个红雨滴”

2006年11月20日，因发现J粒子而获得诺贝尔奖的著名华裔物理学家丁肇中教授来到中国驻瑞士大使馆，做了一场精彩的讲座。丁肇中教授形容自己发现构成物质的第四种基本粒子-J粒子的高精度实验时说到：“相当于在北京下雨时，每秒钟有100亿个雨滴，如果有一个雨滴是红色的，我们就要从这100亿个里找出它来。”

而奇安信威胁情报中心高级威胁分析团队同样需要在海量数据中精准找寻那些红色威胁。最终，我们选择了“红雨滴”作为团队的名称。

附录3　参考链接

1. https://ti.qianxin.com/blog/
2. https://attack.mitre.org/
3. https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/ctr-nsa-css-technical-cyber-threat-framework.pdf
4. https://www.misp-project.org/galaxy.html
5. https://docs.google.com/spreadsheets/u/0/d/1H9_xaxQHpWaa4O_Son4Gx0YOIzlcBWMsdvePFX68EKU/pubhtml#
6. https://attack.mitre.org/groups/
7. https://www.ft.com/content/4da1117e-756c-11e9-be7d-6d846537acab
8. https://www.kryptoslogic.com/blog/2019/11/bluekeep-cve-2019-0708-exploitation-spotted-in-the-wild/
9. https://www.bleepingcomputer.com/news/security/firefox-0-day-used-in-targeted-attacks-against-cryptocurrency-firms/
10. https://securelist.com/chrome-0-day-exploit-cve-2019-13720-used-in-operation-wizardopium/94866/
11. https://securelist.com/windows-0-day-exploit-cve-2019-1458-used-in-operation-wizardopium/95432/
12. https://twitter.com/craiu/status/1176525773869649921
13. https://www.welivesecurity.com/2019/07/11/buhtrap-zero-day-espionage-campaigns/
14. https://securelist.com/cve-2019-0797-zero-day-vulnerability/89885/
15. https://www.mcafee.com/blogs/other-blogs/mcafee-labs/analysis-of-a-chrome-zero-day-cve-2019-5786/

16. https://securelist.com/new-win32k-zero-day-cve-2019-0859/90435/

17. https://research.checkpoint.com/2019/extracting-code-execution-from-winrar/

18. https://googleprojectzero.blogspot.com/2019/08/a-very-deep-dive-into-ios-exploit.html

19. https://www.manrs.org/2019/05/public-dns-in-taiwan-the-latest-victim-to-bgp-hijack/

20. https://www.zdnet.com/article/mysterious-hacker-has-been-selling-windows-0-days-to-apt-groups-for-three-years/

21. http://blogs.360.cn/post/APT-C-34_Golden_Falcon.html#toc-096

22. https://www.cyberscoop.com/uzbekistan-sandcat-kaspersky/

23. https://www.bankinfosecurity.com/cryptocurrency-heist-bgp-leak-masks-ether-theft-a-10898

24. https://www.bankinfosecurity.com/who-hijacked-googles-web-traffic-a-11699

25. https://blog.talosintelligence.com/2018/11/persian-stalker.html

26. https://www.welivesecurity.com/2018/01/09/turlas-backdoor-laced-flash-player-installer/

27. https://www.zdnet.com/article/google-finds-android-zero-day-impacting-pixel-samsung-huawei-xiaomi-devices/

28. https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html

29. https://www.crowdstrike.com/blog/widespread-dns-hijacking-activity-targets-multiple-sectors/

30. https://blog.talosintelligence.com/2018/11/dnspionage-campaign-targets-middle-east.html

31. https://blog.talosintelligence.com/2019/04/seaturtle.html

32. https://securityaffairs.co/wordpress/88366/hacking/dns-hijacking-ncsc-report.html

33. https://blog.trendmicro.com/trendlabs-security-intelligence/new-magecart-attack-delivered-through-compromised-advertising-supply-chain/

34. https://www.welivesecurity.com/2019/03/11/gaming-industry-scope-attackers-asia/

35. https://securelist.com/operation-shadowhammer/89992/

36. https://www.contextis.com/en/blog/avivore

37. https://www.symantec.com/blogs/threat-intelligence/tortoiseshell-apt-supply-chain

38. https://www.welivesecurity.com/2019/05/14/plead-malware-mitm-asus-webstorage/

39. https://www.riskiq.com/blog/labs/cloudcms-picreel-magecart/

40. https://securelist.com/new-finspy-ios-and-android-implants-revealed-itw/91685/

41. https://securitywithoutborders.org/blog/2019/03/29/exodus.html

42. https://citizenlab.ca/2019/09/poison-carp-tibetan-groups-targeted-with-1-click-mobile-exploits/

43. https://www.reuters.com/investigates/special-report/usa-spying-raven/

44. https://mp.weixin.qq.com/s/QFCIeDR_J1NtMMPdyWE8kA

45. https://mp.weixin.qq.com/s/tzXcynzR4zZK7DjPidY6-A

46. https://www.nytimes.com/2019/08/28/us/politics/us-iran-cyber-attack.html

47. https://securityaffairs.co/wordpress/95169/apt/iran-foiled-2-attack.html

48. https://mp.weixin.qq.com/s/qoJ4yHCzdz1vwU7S9bngow

49. https://mp.weixin.qq.com/s/K5bkhWXbaKBiDD78H8tQcg

50. https://www.reuters.com/article/us-usa-cyber-yandex-exclusive/exclusive-western-intelligence-hacked-russias-google-yandex-to-spy-on-accounts-sources-idUSKCN1TS2SX

51. https://blog.alyac.co.kr/2453

52. https://www.symantec.com/blogs/threat-intelligence/waterbug-espionage-governments

53. https://www.recordedfuture.com/bluealpha-iranian-apts/

54. https://www.ncsc.gov.uk/news/turla-group-exploits-iran-apt-to-expand-coverage-of-victims

55. https://www.welivesecurity.com/2019/09/24/no-summer-vacations-zebrocy/

56. https://www.welivesecurity.com/2019/10/17/operation-ghost-dukes-never-left/

57. https://securelist.com/compfun-successor-reductor/93633/

58. https://arstechnica.com/information-technology/2018/11/ukraine-detects-new-pterado-backdoor-malware-warns-of-russian-cyberattack/

59. https://www.welivesecurity.com/2019/11/21/deprimon-default-print-monitor-malicious-downloader/

60. https://medium.com/@botherder/everything-we-know-of-nsa-and-five-eyes-malware-e8eac172d3b5

61. https://baesystemsai.blogspot.com/2016/04/two-bytes-to-951m.html

62. https://securelist.com/fin7-5-the-infamous-cybercrime-rig-fin7-continues-its-activities/90703/

63. https://securityaffairs.co/wordpress/90698/cyber-warfare-2/dutch-mole-stuxnet-attack.html

64. https://dragos.com/resource/hexane/

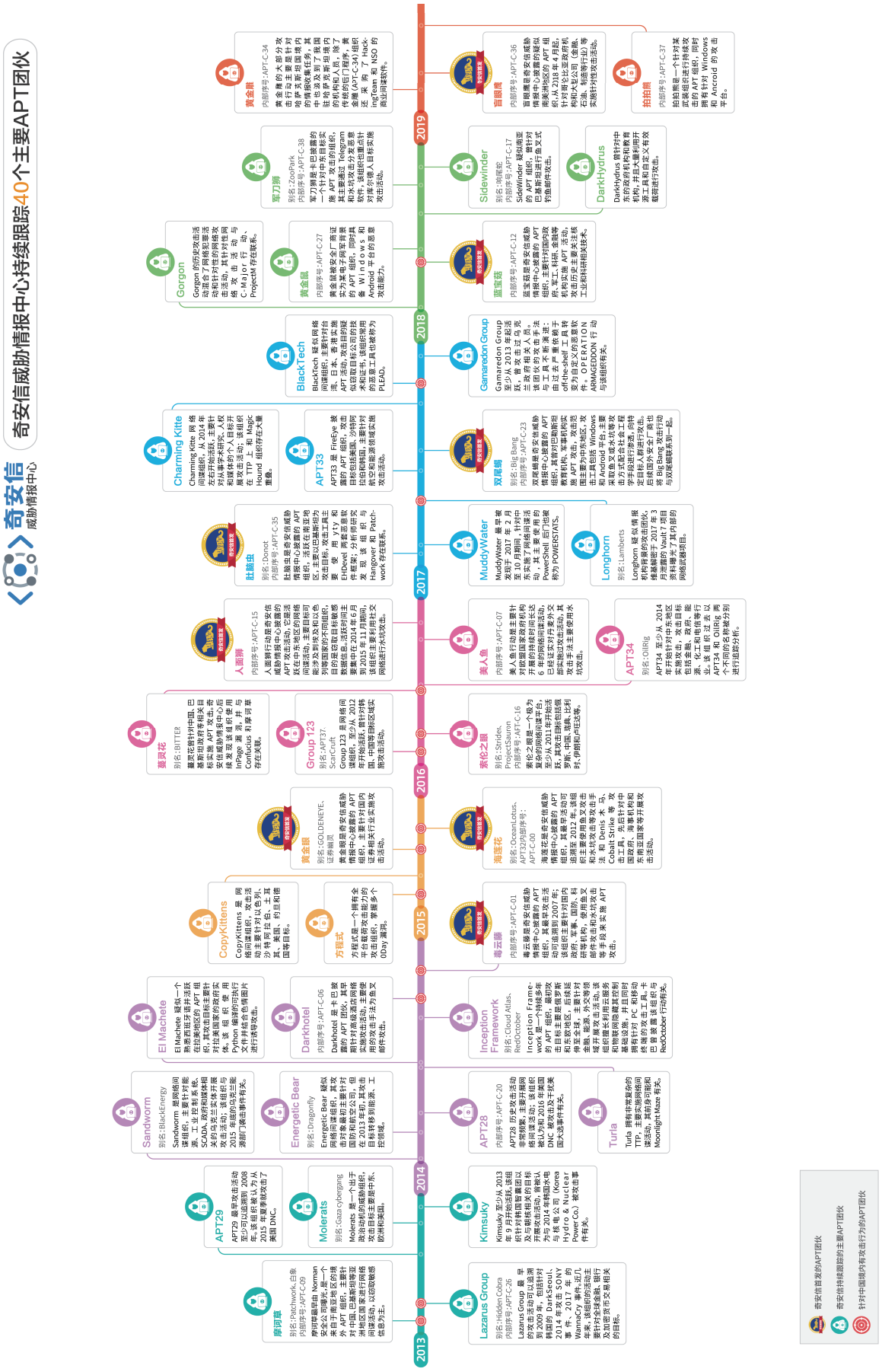
65. https://www.secureworks.com/blog/lyceum-takes-center-stage-in-middle-east-campaign

66. https://github.com/RedDrip7/APT_Digital_Weapon

67. https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/

68. https://www.justice.gov/opa/press-release/file/1092091/download

附录4　全球主要APT组织列表



奇安信 | 奇安信
威胁情报中心