APT

全球高级持续性威胁（APT）活动
2019年中报告

奇安信威胁情报中心

2019年7月

序 言

奇安信威胁情报中心在 2018 年曾公开发布了两篇全球高级持续性威胁研究总结报告[参考链接：2 3]，其中总结了高级持续性威胁背后的攻击组织在过去一年中的攻击活动和战术技术特点。

如今，2019 年已经过去一半，我们在对历史活跃 APT 组织近半年的攻击活动情况的持续跟踪过程中，呈现地缘政治特征的国家背景黑客组织作为观察的重点，其实施的网络威胁活动始终穿插在现实的大国政治和军事博弈过程中，网络空间威胁或已成为各国情报机构和军事行动达到其情报获取或破坏目的所依赖的重要手段之一。

本报告主要分成两个部分，第一部分主要总结在 APT 威胁来源的地域特征下主要活跃的 APT 组织，以及其在 2019 年上半年的主要情况；第二部分基于近半年重要的全球高级持续性威胁事件，对整体威胁态势的总结。

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；外部的情报来源包括主要发布 APT 类情报 178 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。
- MITRE 组织总结的 ATT&CK 框架以及威胁组织、攻击工具列表[4]也是对研究 APT 组织及其战术技术特点的重要基础之一。
- 其他公开的 APT 组织及行动资料，包括 MISP 项目[5]，国外安全研究人员 Florian Roth 的 APT 组织和行动表格[6]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

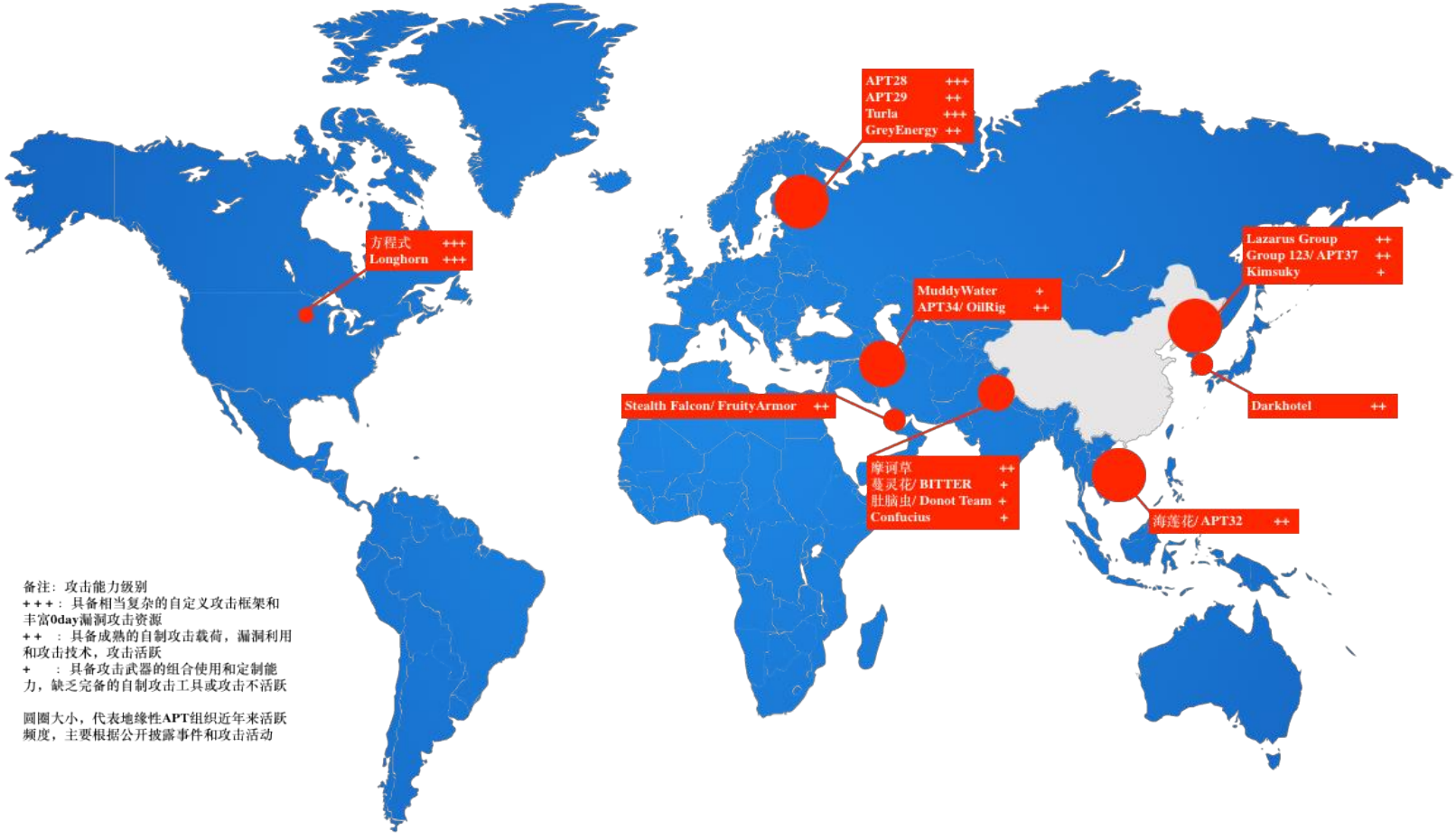
第一部分　地缘政治下的 APT 组织

自 2010 年震网事件被发现以来，网络攻击正在被各个国家、情报机构用作达到其政治、外交、军事等目的的重要手段之一。在过去对 APT 活动的追踪过程中，APT 攻击往往伴随着现实世界重大政治、外交活动或军事冲突的发生前夕和过程中，这也与 APT 攻击发起的动机和时机相符。

奇安信威胁情报中心结合公开情报中对 APT 组织归属的结论，按地缘特征对全球主要的 APT 组织和攻击能力进行评估，并对其在 2019 年最近半年的攻击活动的总结。

地域	主要组织	攻击能力
东亚	Lazarus Group	++
	Group 123/ APT37	++
	Kimsuky	+
	Darkhotel	++
东南亚	海莲花/ APT32	++
南亚次大陆	摩诃草	++
	蔓灵花/ BITTER	+
	肚脑虫/ Donot Team	+
	Confucius	+
东欧	APT28	+++
	APT29	++
	Turla	+++
	GreyEnergy	++
中东	MuddyWater	+
	APT34/ OilRig	++
	Stealth Falcon/ FruityArmor	++
北美	方程式	+++
	Longhorn	+++

表：地缘政治下的全球主要 APT 组织及能力



备注：攻击能力级别
+ + + ：具备相当复杂的自定义攻击框架和丰富**0day**漏洞攻击资源
+ + ：具备成熟的自制攻击载荷，漏洞利用和攻击技术，攻击活跃
+ ：具备攻击武器的组合使用和定制能力，缺乏完备的自制攻击工具或攻击不活跃

圆圈大小，代表地缘性**APT**组织近年来活跃频度，主要根据公开披露事件和攻击活动

一、 东亚

围绕东亚一直是全球 APT 威胁活动最为活跃的地域之一，最早在 2011 年曝光的 Lazarus Group 是历史上少数几个最为活跃的 APT 组织之一。

Lazarus Group，据公开披露被认为是朝鲜 Bureau 121 背景下的 APT 组织，历史曾攻击索尼娱乐，全球多家银行 SWIFT 系统以及和 Wannacry 勒索病毒有关。2018 年 9 月，美国 DoJ 和 FBI 联合公开指控朝鲜黑客 PARK JIN HYOK 及 Chosun Expo 机构与上述攻击事件有关，并指出其背后为朝鲜政府[7]。

我们注意到近年来针对 Lazarus 活动的披露有所减少，其攻击目标主要为金融和加密货币相关，推测其动机更倾向于获得经济利益。

我们总结了 Lazarus 组织在近半年的主要攻击活动，如图所示。

Lazarus 使用的攻击工具如下：

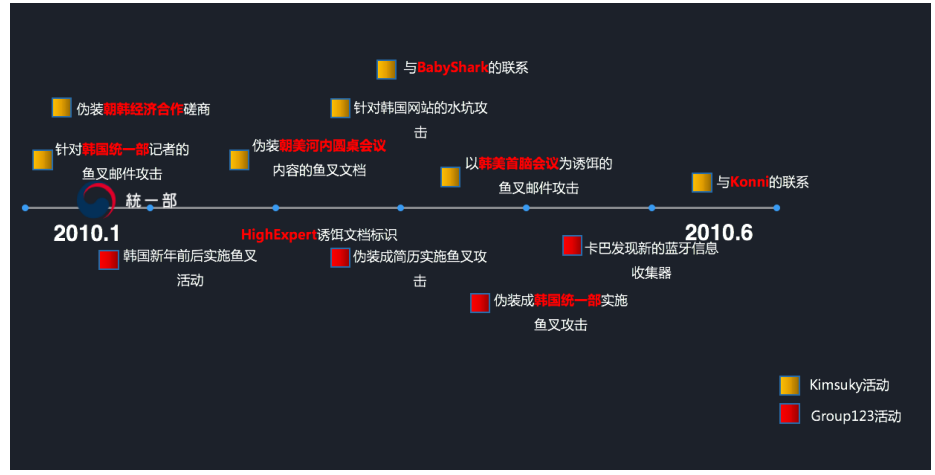
名称	说明
Rising Sun	第二阶段植入物，由 Duuzer 后门演化的新渗透框架
KEYMARBLE	RAT 工具，使用伪 TLS 通信
HOPLIGHT	木马，使用公共 SSL 证书进行安全通信
ELECTRICFISH	网络代理和隧道工具

除了 Lazarus，在近两年来，另外两个朝鲜语系的 APT 团伙表现出了异常的活跃，分别是 Group 123 和 Kimsuky。近年来，朝鲜半岛的政治局势日益趋向于缓和的局势，朝鲜政府也积极就朝核问题、朝韩双方关系与美国、韩国展开对话，但缓和的政治外交局势下，并不能掩盖东亚区域依然频繁的网络情报活动。

结合两个组织历史攻击活动，我们推测 Kimsuky 更关注于朝鲜半岛的政治外交问题，并通常结合相关热点事件用于诱饵文档内容；而 Group 123 则针对更广泛的网络情报获取。

	Lazarus Group	Group 123	Kimsuky
主要别名	Hidden Cobra	APT37	无
活动频度	中	高	高
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

两个组织近半年的主要攻击活动总结如下图[9 10]。



Group 123 和 Kimsuky 通常都利用向目标投递鱼叉邮件和诱饵文档，包括 Office 文档和 HWP 文档，诱导目标人员触发恶意宏代码或漏洞文档来建立攻击立足点。其也通过渗透韩国网站作为载荷分发和控制回传通道。

Group 123 还偏好使用云服务作为其窃取目标主机信息和资料的重要途径，其常用的 ROKRAT 后门就是基于云服务的实现，利用包括 Dropbox，Yandex，pCloud 等云服务。

二、 东南亚

海莲花组织是东南亚地区最为活跃的 APT 组织，其首次发现和公开披露是由奇安信威胁情报中心的红雨滴团队。

海莲花组织最初主要以中国政府、科研院所、海事机构等行业领域实施攻击，这也与当时的南海局势有关。但在近年来的攻击活动中，其目标地域延伸至柬埔寨、菲律宾、越南等东南亚其他国家，而其针对中国境内的 APT 攻击中，也出现了针对境内高校和金融投资机构的攻击活动。

海莲花组织是一个快速变化的 APT 组织，其擅长与将定制化的公开攻击工具和技术和自定制恶意代码相结合，例如 Cobalt Strike 和 fingerprintjs2 是其常用的攻击武器之一。

海莲花组织经过多年的发展，形成了非常成熟的攻击战术技术特征，并擅长于利用多层 shellcode 和脚本化语言混淆其攻击载荷来逃避终端威胁检测，往往能够达到比较好的攻击效果。

这里我们也总结了海莲花组织的常用 TTP 以便于更好的跟踪其技术特点的变化。

图 海莲花近半年攻击目标

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

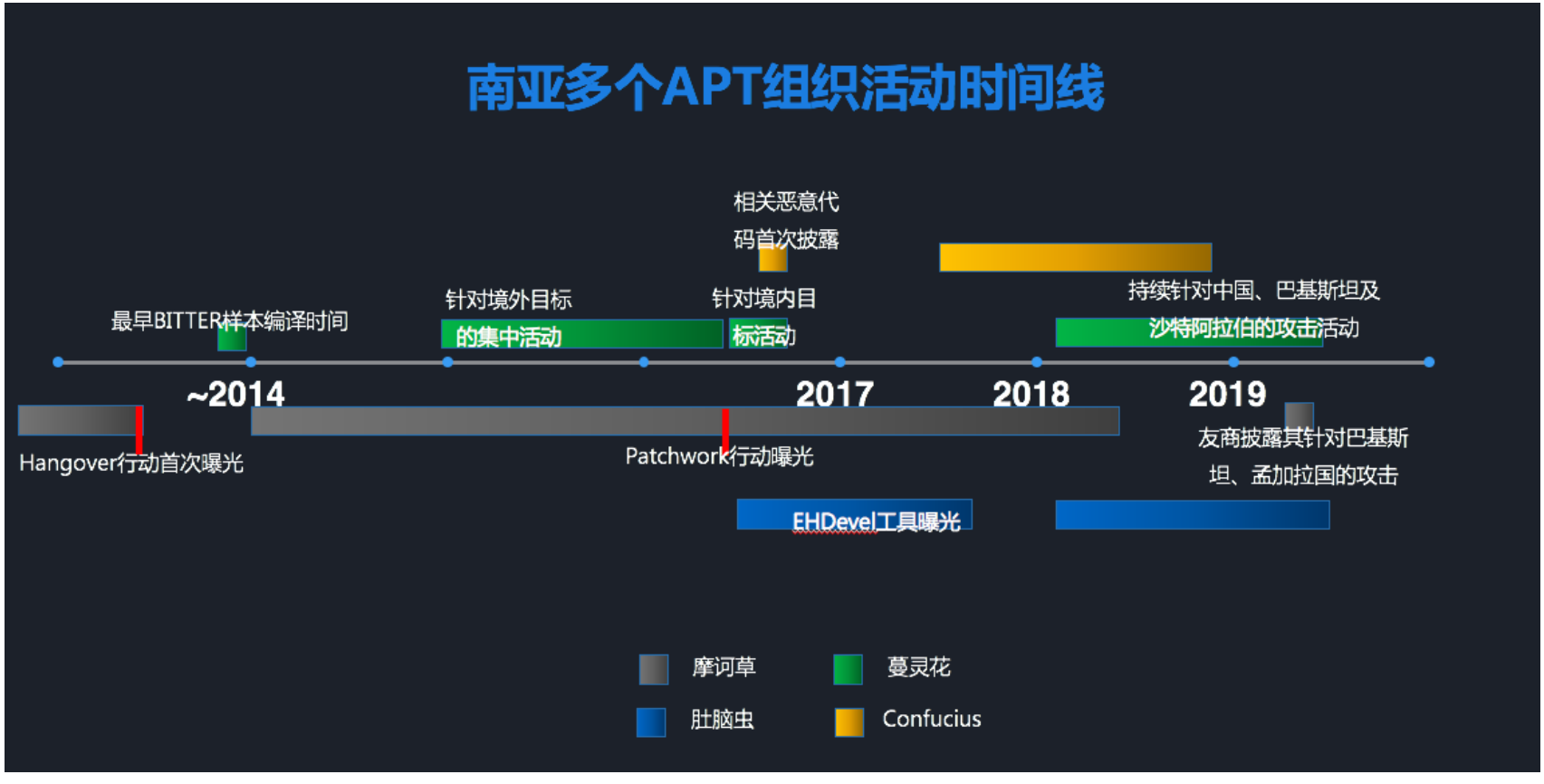
三、 南亚次大陆

南亚次大陆是另一个 APT 组织活动的热点区域，从 2013 年 5 月 Norman 安全公司披露 Hangover 行动（即摩诃草组织）以来，出现了多个不同命名的 APT 组织在该地域持续性的活跃，并且延伸出错综复杂的关联性[13]，包括摩诃草、蔓灵花、肚脑虫、Confucius，以及其他命名的攻击活动和攻击工具，包括 Sidewinder、Urpage、Bahamut、WindShift。

造成归属问题的主要因素是上述 APT 活动大多使用非特定的攻击载荷和工具，脚本化和多种语言开发的载荷往往干扰着归属分析判断，包括使用.Net、Delphi、AutoIt、Python 等。但从历史攻击活动来看，其也出现了一些共性：

- 同时具备攻击 PC 和智能手机平台能力；
- 巴基斯坦是主要的攻击目标，部分组织也会攻击中国境内；
- 政府、军事目标是其攻击的主要目标，并且投放的诱饵文档大多也围绕该类热点新闻，如克什米尔问题；

我们结合历史公开报告的披露时间制作了相关 APT 组织的活跃时间线，推测这些 APT 组织可能从 2015-2016 甚至更早出现了分化，并且趋向于形成多个规模不大的小型攻击团伙的趋势。


南亚多个APT组织活动时间线
相关恶意代码首次披露
最早BITTER样本编译时间
针对境外目标的集中活动
针对境内目标活动
持续针对中国、巴基斯坦及沙特阿拉伯的攻击活动
~2014
2017
2018
2019
Hangover行动首次曝光
Patchwork行动曝光
友商披露其针对巴基斯坦、孟加拉国的攻击
EHDevel工具曝光
摩诃草
蔓灵花
肚脑虫
Confucius

四、 东欧

APT28、APT29、Turla 作为东欧地区最为知名的 APT 组织一直广泛活跃。

美国 DHS 曾在 2016 年 12 月对 APT28，APT29 组织在同年针对 DNC 的攻击事件以及干扰美国大选活动发布了相关调查报告，并将其恶意攻击活动称为 GRIZZLY STEPPE，并直指俄罗斯情报部门。

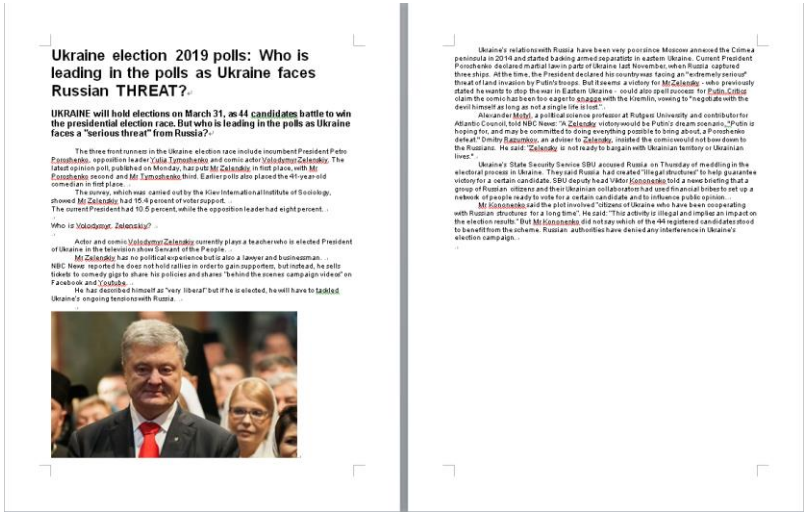
来自伦敦国王学院的安全研究人员在 SAS 2017 年会议上介绍了 Turla APT 组织的前身是 90 年代著名网络间谍组织 Moonlight Maze[16]。

国外安全厂商 ESET 在 2018 年披露了 BlackEnergy 的继任者，命名为 GreyEnergy[17]，一个专注于工业系统的 APT 组织。

	APT28	APT29	Turla	BlackEnergy
主要别名	Sofacy	Cozy Bear	Snake	无
目标行业	政府、外交、国防、军事等			工业、能源
目标地域	中东、美国、NATO、中亚等			乌克兰、波兰

从 2019 年上半年的公开披露情况来看，除了 APT28 以外，其他三个组织的公开披露活动有所减少。而 APT28 组织的主要活动似乎更多旨在干扰其目标国家的选举活动。

安全厂商披露在 3 月捕获的一份在野诱饵文档，其使用的内容以乌克兰总统竞选人 Volodymyr Zelenskiy 和乌俄问题为诱导，其正值乌克兰总统竞选时机[18]。



Ukraine election 2019 polls: Who is leading in the polls as Ukraine faces Russian THREAT?

UKRAINE will hold elections on March 31, as 44 candidates battle to win the presidential election race. But who is leading in the polls as Ukraine faces a "serious threat" from Russia?

The three front runners in the Ukraine election race include incumbent President Petro Poroshenko, opposition leader Yulia Tymoshenko and comic actor Volodymyr Zelenskiy. The latest opinion poll, published on Monday, has put Mr Zelenskiy in first place, with Mr Poroshenko second and Mr Tymoshenko third. Earlier polls also placed the 41-year-old comedian in first place.

The survey, which was carried out by the Kiev International Institute of Sociology, showed Mr Zelenskiy had 15.4 percent of voter support.

The current President had 10.5 percent, while the opposition leader had eight percent.

Who is Volodymyr Zelenskiy?

Actor and comic Volodymyr Zelenskiy currently plays a teacher who is elected President of Ukraine in the television show Servant of the People.

Mr Zelenskiy has no political experience but is also a lawyer and businessman.

NBC News reported he does not hold rallies in order to gain supporters, but instead, he sells tickets to comedy gigs to share his policies and shares "behind the scenes campaign videos" on Facebook and Youtube.

He has described himself as "very liberal" but if he is elected, he will have to tackle Ukraine's ongoing tensions with Russia.

Ukraine's relations with Russia have been very poor since Moscow annexed the Crimea peninsula in 2014 and started backing armed separatists in eastern Ukraine. Current President Poroshenko declared martial law in parts of Ukraine last November, when Russia captured three ships. At the time, the President declared his country was facing an "extremely serious" threat of land invasion by Putin's troops. But it seems a victory for Mr Zelenskiy - who previously stated he wants to stop the war in Eastern Ukraine - could also spell success for Putin. Critics claim the comic has been too eager to engage with the Kremlin, vowing to "negotiate with the devil himself as long as not a single life is lost".

Alexander Motyl, a political science professor at Rutgers University and contributor for Atlantic Council, told NBC News: "A Zelenskiy victory would be Putin's dream scenario." Putin is hoping for, and may be committed to doing everything possible to bring about, a Poroshenko defeat." Dmitry Razumkov, an adviser to Zelenskiy, insisted the comic would not bow down to the Russians. He said: "Zelenskiy is not ready to bargain with Ukrainian territory or Ukrainian lives."

Ukraine's State Security Service SBU accused Russia on Thursday of meddling in the electoral process in Ukraine. They said Russia had created "illegal structures" to help guarantee victory for a certain candidate. SBU deputy head Viktor Kononenko told a news briefing that a group of Russian citizens and their Ukrainian collaborators had used financial bribes to set up a network of people ready to vote for a certain candidate and to influence public opinion.

Mr Kononenko said the plot involved "citizens of Ukraine who have been cooperating with Russian structures for a long time". He said: "This activity is illegal and implies an impact on the election results." But Mr Kononenko did not say which of the 44 registered candidates stood to benefit from the scheme. Russian authorities have denied any interference in Ukraine's election campaign.

国外安全厂商也披露从 2018 年中以来，APT28 组织针对欧洲的网络间谍活动大幅增加，以及针对欧洲民主机构的攻击，其也可能与 2019 年的欧盟议会选举有关[19 20]。

从战术和技术角度来看，似乎从 2018 年起 APT28 更倾向于使用多种语言开发的 Zebrocy 攻击组件并用于鱼叉攻击后的第一阶段的载荷植入[21]。其模块可能由 Delphi，C#，Python，AutoIt 甚至至 Go。卡巴在最新的研究报告中将其作为独立的组织进行追踪。

而在 ESET 对 Turla 最新的研究报告中，其更倾向于基于定制化的开源项目（如 Posh-SecMod）和脚本，并加载其过去的自定义武器库。

我们并不认为这些改变是其攻击能力削弱的体现，在 2018 年曝光的 VPNFilter 事件和 Lojax rootkit 都被怀疑与东欧 APT 组织有关。我们推测攻击组织做出积极的改变旨在提高攻击的效率和效果，并着力于混淆和隐藏攻击活动的来源，以及对抗目标网络的防御机制。

五、 中东

中东地区，其拥有全球最为复杂的政治、外交和军事局势，多年以来，充斥着战乱、恐怖主义、军事行动以及频繁的网络间谍活动和情报活动。在此背景下，网络攻击活动往往作为刺探对手情报，监控人员舆论，配合间谍活动和情报活动甚至制造虚假言论和虚假新闻的最有效方式之一。而在中东地区，公开披露最多的属据称为伊朗政府背景的相关网络攻击活动，这也源于伊朗与以美国为首的西方国家的政治和外交关系相左的原因。

我们在这里列举了近半年来中东地区发生的一些重点事件：

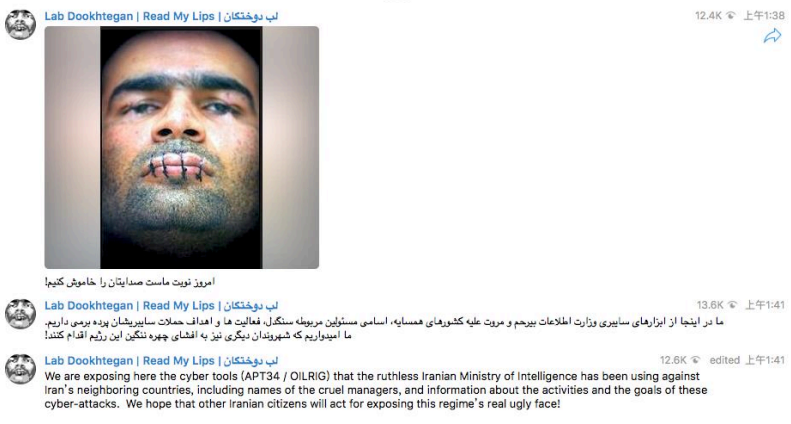
- 多家安全厂商披露大规模的 DNS 劫持活动，并称疑似与伊朗有关[26 27 28]；
- 卡巴多次披露 FruityArmor(又称 Stealth Falcon)使用的多个 Windows 提权 0day 漏洞 (CVE-2019-0797 、CVE-2018-8453、CVE-2018-8611、CVE-2018-8589)；
- 据称是伊朗背景的多个 APT 组织发生内部资料和网络武器泄露；
- 美、伊的外交形式急剧恶化，伊朗政府从情报活动、军事活动等多方面采取更加强硬的姿态，包括破坏 CIA 在其情报网络、击落无人机等，美国回应将对其采取网络军事行动。

我们在这里结合上半年泄露的据称是伊朗黑客组织的资料和网络武器对其近年来主要活跃的 APT 组织进行总结。

今年上半年发生了多起针对中东地区 APT 组织的相关资料泄露和拍卖事件，通过泄露资料，再一次帮助我们将虚拟的 APT 组织与现实世界的人员、机构及国家联系到一起。

APT34，又称 OilRig，一个最早从 2014 年起就开始活跃的 APT 组织，其被公开披露声称与伊朗情报与国家安全部(Iranian Ministry of Intelligence)有关。在过去，其主要活跃地

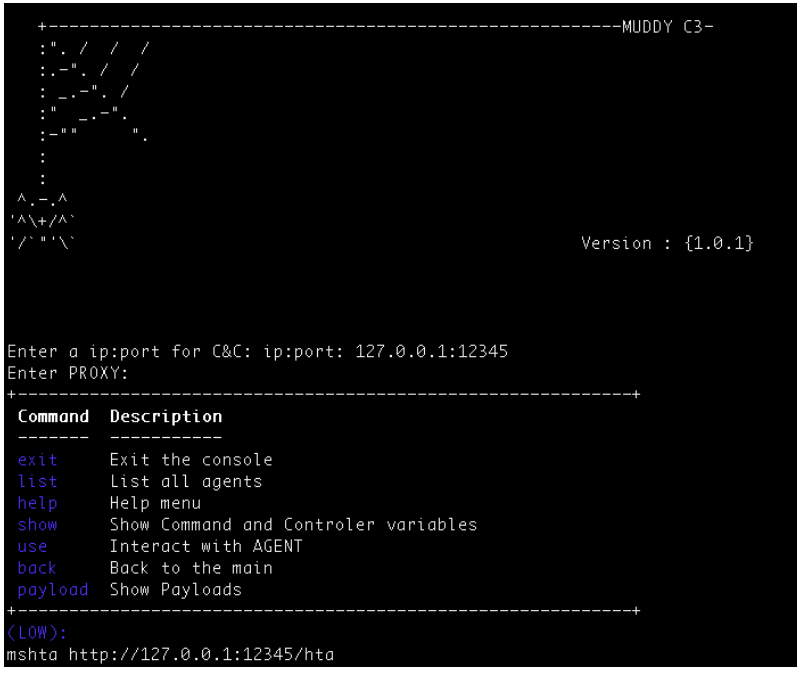
区为中东，并针对如金融，政府，能源，化学和电信等多个行业实施攻击[29]。



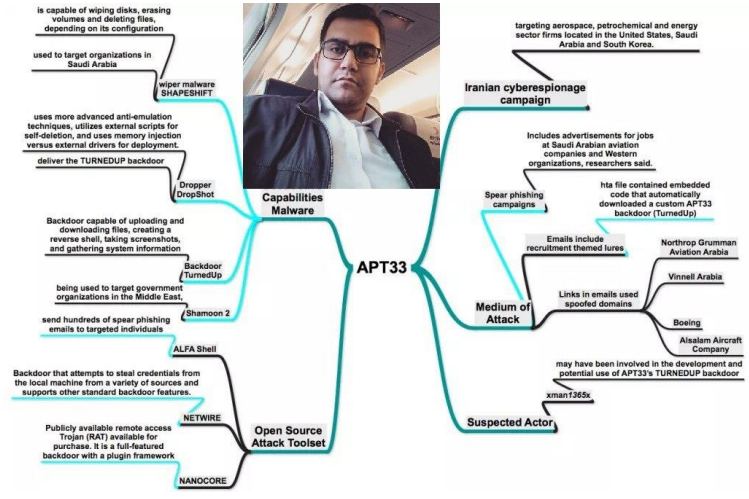
泄露的网络武器库：

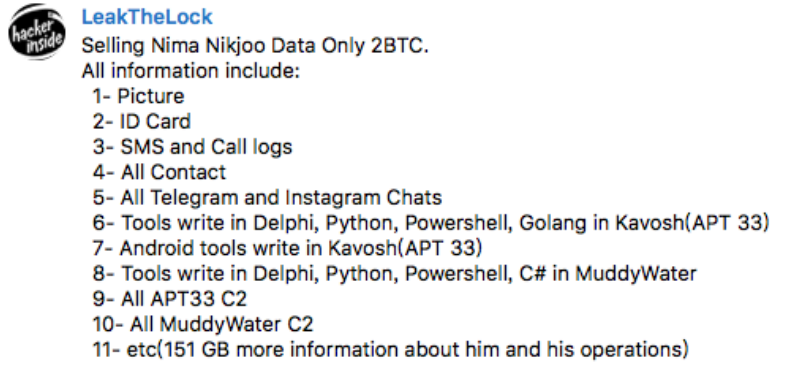
名称	说明
Poison Frog	Powershell 后门，通过 DNS 和 HTTP 通信，也称为 BONDUPDATER[30]
Glimpse	Powershell 后门，通过 DNS 通信，也称为 Updated BONDUPDATER[30]
多个 Webshell	FoxPanel222、HighShell、HyperShell、Minion
webmask	Python 实现的 DNS 劫持和中间人攻击工具，Cisco Talos 也称为 DNSpionage[31]
Jason	Exchange 密码爆破工具

另一个被公开认为和伊朗有关的 APT 组织 MuddyWater，最早由 Palo Alto Networks Unit 42 于 2017 年 11 月发现并命名[32]，并迅速成为中东地区非常活跃的 APT 组织之一，其主要使用 Powershell 后门 POWERSTATS，以及名为 MuddyC3 的控制后台[33]。



有黑客成员公开声称 MuddyWater 和另一个 APT 组织 APT33 关联到同一个名为 Nima Nikjoo 的人员，并将其相关资料进行拍卖[34]。

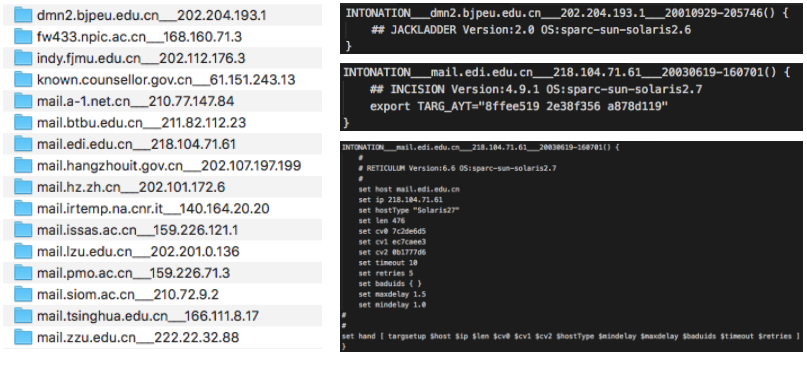




六、 北美

结合公开披露资料，作为网络空间能力的强国，历史曝光的震网事件，方程式组织都被认为与北美情报机构有关[22 23]。

从 2013 年以来，相关情报机构的多次泄密事件展示了其完备的网络空间攻击体系和自动化攻击武器，并暴露了其将中国作为其实施全球网络间谍活动的重要目标之一的相关证据。



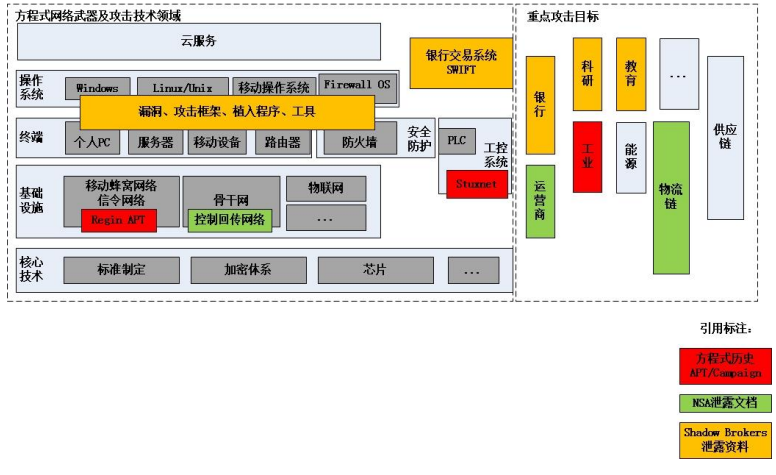
在 2018 和 2019 年的美国国防部网络战略情报报告中，都将中国和俄罗斯作为其重要的战略对手[24]。

在 2018 年的网络空间战略摘要中提到了“Defend forward”概念，旨在从源头上破坏或制止恶意网络空间活动，并且同年美国政府取消了第 20 号总统政策指令，取消了针对美国对手的进攻性网络攻击批准程序的一些限制。这些都表明美国作为超级网络强国正在积极进入网络空间的备战状态。而在近期纽约时报也报道了美国正在加强针对俄罗斯电网的网络入侵[25]，展示了其在网络空间攻防中采取了更加主动积极的姿态。

We are engaged in a long-term strategic competition with China and Russia. These States have expanded that competition to include persistent campaigns in and through cyberspace that pose long-term strategic risk to the Nation as well as to our allies and partners. China is eroding U.S. military overmatch and the Nation's economic vitality by persistently exfiltrating sensitive information from U.S. public and private sector institutions. Russia has used cyber-enabled information operations to

The Department must take action in cyberspace during day-to-day competition to preserve U.S. military advantages and to defend U.S. interests. Our focus will be on the States that can pose strategic threats to U.S. prosperity and security, particularly China and Russia. We will conduct cyberspace operations to collect intelligence and prepare military cyber capabilities to be used in the event of crisis or conflict. We will defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict. We will strengthen the security and resilience of networks and systems that contribute to current and future U.S. military advantages. We will collaborate with our interagency, industry, and international partners to advance our mutual interests.

从历史泄露的方程式资料分析，其具备的网络攻击能力是全方位的，下图是我们根据泄露 NSA 资料和公开情报整理的其网络武器及攻击技术所覆盖的领域和目标。



第二部分　上半年全球 APT 威胁态势

一、　APT 组织采用的供应链攻击

供应链攻击往往是网络攻击中最容易忽视的一类，在 MITRE ATT&CK 中也将供应链攻击作为获取初始访问的一项攻击技术(T1195 Supply Chain Compromise)。而在 APT 活动中，供应链攻击也是时常发生，这里列举了近半年的 APT 类供应链攻击活动。

- ESET 披露新的针对游戏行业的供应链攻击，并疑似与 Winnti Group 有关[35];
- 卡巴披露针对华硕的供应链攻击行动 ShadowHammer，并且通过匹配用户 mac 地址实施针对特定目标的攻击[36]；
- ESET 披露 BlackTech 组织通过合法证书签名的样本，并疑似通过供应链攻击华硕 WebStorage[37]。

我们认为 APT 组织使用供应链攻击通常有着特殊的意图，其通常可以作为攻击目标人员或组织的一种“曲线攻击”路径，通过对目标相关的供应商或服务商的攻击作为达到最终目标的重要途径。

二、　国家公共基础设施或将成为网络战的重点

自 2010 年伊朗震网事件和 2015 年乌克兰电网攻击事件，针对国家公共基础设施(包括电力、工业、能源、医疗等)的网络攻击活动会对城市和民众日常生活造成极为严重的破坏。

在 2019 年上半年，南美地区发生多起异常停电事件，由于尚不明确造成停电的原因，也被国外新闻媒体联想到是否与网络攻击或演习有关，而针对公共基础设施领域的网络攻击也逐渐作为国与国之间进行战略性打击和威慑的重要手段。

这里我们也将上半年相关事件时间线进行总结：

- 3 月 6 日，委内瑞拉全境出现大面积断电，委内瑞拉政府指责是美国蓄意破坏；
- 6 月 14 日，连线网披露美国 E-ISAC 发现 Triton 针对美国境内电网的探测活动[38]；
- 6 月 15 日，纽约时报披露美政府加强对俄电网的数字入侵，而针对其电网控制系统的探测和侦查早在 2012 年就开始了[25]；
- 6 月 16 日，南美多个国家出现停电事件，主要由于阿根廷和乌拉圭的互联电网发生大规模故障；
- 6 月 22 日，伊朗击落美国无人机，美声明将对其采取网络攻击[39]。

三、 APT 组织网络武器库的泄露与扩散

网络武器库和相关资料泄露在过去一直时有发生，这些网络武器库通常由知名 APT 组织或网络军火商制作和使用。

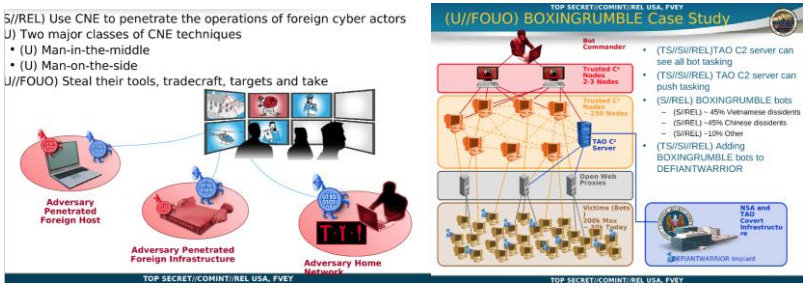
- 2014 年 8 月 4 日，网络军火商 Gamma 40GB 资料泄露；
- 2015 年 7 月 5 日，网络军火商 Hacking Team 400GB 数据泄露，包括电子邮件、文件和源代码；
- 2016 年 8 月 13 日，黑客组织 The Shadow Brokers 公开泄露和拍卖 NSA 网络武器库，包括针对防火墙、Linux/类 Unix、Windows 和 SWIFT 平台攻击武器；
- 2017 年 3 月 7 日，维基解密网络曝光 CIA CCI 部门的 8761 份机密性文档，涉及其内部针对多个平台网络武器开发的资料；
- 2019 年 3 月 27 日，有黑客成员通过 Telegram 渠道披露 APT34 组织的网络武器和相关信息；
- 2019 年 5 月 7 日，有黑客成员通过 Telegram 渠道披露 MuddyWater 组织相关资料，并进行公开拍卖。

网络武器库的泄露向我们展示了 APT 组织为了实施网络攻击活动以及为达到其目的进行了长期的攻击能力和技术的积累和筹备，而数字武器泄露造成扩散的副作用也是无穷的。

四、 APT 组织间的“黑吃黑”游戏

2019 年 6 月 21 日，赛门铁克披露了一份 Turla 组织最新的报告[40]，其中最为有意思的是其发现 Turla 对 APT34 组织基础设施的劫持并用于自身的攻击活动。

类似于上述这种 APT 组织间的“黑吃黑”行为在斯诺登泄露的 NSA 机密文档中也曾出现类似的项目[41]。通过采用中间人攻击或旁观者攻击的方式对其他攻击组织进行攻击，并窃取其使用的工具、获取的情报甚至接管攻击的目标。



我们更倾向于这类行为在未来的 APT 攻击活动中还会发生，并且更有可能出现在拥有更高技术能力的 APT 组织。这种行为往往能够更好的隐蔽真实的攻击来源和意图，而对被攻击的受害主体评估其影响和损失造成了迷惑性。

五、 APT 狩猎下的中国威胁论

在过去的 APT 研究中，公开声称归属中国 APT 组织的报告也是层出不穷，甚至有北美安全厂商以 Panda 作为其认为的归属为中国的 APT 组织命名，而在历史的公开 APT 组织列表中，被认为归属为中国和伊朗的 APT 组织数量最为众多。

近日，一家国外安全厂商披露了一项以全球电信运营商和蜂窝网络为目标的 APT 行动，其中也将攻击来源归属指向疑似中国来源的 APT 组织[42]，而随后部分外媒和国外安全研究人员更倾向于将其归属指向 APT10 的结论。

In 2018, the Cybereason Nocturnus team identified an advanced, persistent attack targeting global telecommunications providers carried out by a threat actor using tools and techniques commonly associated with Chinese-affiliated threat actors, such as APT10. This multi-wave attacks focused on obtaining data of specific, high-value targets and resulted in a complete takeover of the network.

在大多数的相关研究报告中，出现以下攻击技术特征通常会被归属到疑似和中国黑客组织有关：

- 使用中国菜刀(China Chopper) Webshell；
- 将 Poison Ivy RAT 或其变种作为攻击载荷或后门程序；
- 控制基础设施地理位置在中国境内。

然而，China Chopper 和 Poison Ivy 都是作为公开的攻击工具，而中国也是历来 APT 活动的主要受害者之一。

我们认为在当前的 APT 活动中，APT 组织在更加注重攻击归属的隐藏的同时，也积极引入假旗标志(False Flag)和模仿其他攻击组织的战术技术特点。APT 攻击活动的归属问题变得更加困难，也依赖于更加严密的分析判断和负责任的披露。

总　结

2019 年上半年是不平静的半年，全球的政治局势变得更加风云变幻，在冲突和博弈之下，网络空间对抗的格局也变得尤为凸显，国家背景的 APT 活动似乎由过去的隐蔽战线部分转向更加明显的网络战争对抗的趋势。与现实战争不同的是，现代战争可能因为某些导火索而一触即发，而网络战争更依赖于对战略性对手的早期侦查和探测，并实施长期的渗透和潜伏。

我们在此份报告中再次围绕地缘政治博弈主导下的网络空间 APT 组织的主题，对全球主要的 APT 组织近年来的情况进行总结和介绍，并结合了其在上半年的活动情况，APT 已然是国家和情报机构在网络空间领域的战略手段。

奇安信威胁情报中心和红雨滴研究团队也将持续致力于最新 APT 活动的跟踪和研究，以及披露相关 APT 组织、技术能力和网络武器的情况。

附录1 奇安信威胁情报中心

奇安信威胁情报中心是北京奇安信科技有限公司（奇安信集团）旗下的威胁情报整合专业机构。该中心以业界领先的安全大数据资源为基础，基于奇安信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，通过强大的大数据能力，实现全网威胁情报的即时、全面、深入的整合与分析，为企业和机构提供安全管理与防护的网络威胁预警与情报。

奇安信威胁情报中心对外服务平台网址为 https://ti.qianxin.com/。服务平台以海量多维度网络空间安全数据为基础，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。

微信公众号：奇安信威胁情报中心

附录2 红雨滴团队（RedDrip Team）

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。

团队 LOGO：

关注二维码：

附录 参考链接

1.https://ti.qianxin.com/blog/

2.https://ti.qianxin.com/uploads/2018/08/01/c437f2e1f3eba14802924e26fc2318fb.pdf

3.https://ti.qianxin.com/uploads/2019/01/02/56e5630023fe905b2a8f511e24d9b84a.pdf

4.https://attack.mitre.org/

5.https://www.misp-project.org/galaxy.html

6.https://docs.google.com/spreadsheets/u/0/d/1H9_xaxQHpWaa4O_Son4Gx0YOIzlcBWMsdvePFX68EKU/pubhtml#

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

8. https://www.cyberscoop.com/apt32-ocean-lotus-vietnam-car-companies-hacked/

9. https://blog.alyac.co.kr/

10. https://securelist.com/scarcruft-continues-to-evolve-introduces-bluetooth-harvester/90729/

11. https://s.tencent.com/research/report/711.html

12. https://www.freebuf.com/articles/paper/120002.html

13. https://www.first.org/resources/papers/tallinn2019/Linking_South_Asian_cyber_espionnage_groups-to-publish.pdf

14. https://labs.bitdefender.com/2017/09/ehdevel-the-story-of-a-continuously-improving-advanced-threat-creation-toolkit/

15. https://www.arbornetworks.com/blog/asert/donot-team-leverages-new-modular-malware-framework-south-asia/

16. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180251/Penquins_Moonlit_Maze_PDF_eng.pdf

17. https://www.welivesecurity.com/wp-content/uploads/2018/10/ESET_GreyEnergy.pdf

18. https://blog.yoroi.company/research/apt28-and-upcoming-elections-possible-interference-signals/

19. https://securityaffairs.co/wordpress/82772/apt/russian-apt-groups-may-elections.html

20. https://securityaffairs.co/wordpress/81445/apt/apt28-institutions-europe.html

21. https://securelist.com/zebrocys-multilanguage-malware-salad/90680/

22. https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

23. https://securelist.com/equation-the-death-star-of-malware-galaxy/68750/

24. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

25. https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html

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

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

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

29. https://www.fireeye.com/blog/threat-research/2017/12/targeted-attack-in-middle-east-by-apt34.html

30. https://unit42.paloaltonetworks.com/behind-the-scenes-with-oilrig/

31. https://blog.talosintelligence.com/2019/04/dnspionage-brings-out-karkoff.html

32. https://unit42.paloaltonetworks.com/unit42-muddying-the-water-targeted-attacks-in-the-middle-east/

33. https://ti.qianxin.com/blog/articles/apt-organization-muddywater-new-weapon-muddyc3-code-leak-and-analysis

34. https://hack2interesting.com/iranian-cyber-espionage-apt33/

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

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

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

38. https://www.wired.com/story/triton-hackers-scan-us-power-grid/

39. https://www.nytimes.com/2019/06/22/us/politics/us-iran-cyber-attacks.html

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

41. https://www.eff.org/files/2015/01/27/20150117-spiegel-overview_of_methods_for_nsa_integrated_cyber_operations_0.pdf

42. https://www.cybereason.com/blog/operation-soft-cell-a-worldwide-campaign-against-telecommunications-providers