微步在线
让安全没有边界

2022年
APT活动分析报告

The APT activity analysis report in 2022

01

概述

2022 年是国际局势趋向紧张的一年，特别是俄乌战争对全球政治和经济走向造成了深远影响，地缘政治的冲突也为网络攻击带来了新的方向和话题，以俄乌为焦点的 APT 攻击活动达到空前规模。而我国作为网络攻击的主要受害者，仍然承受着来自周边国家和地区背景 APT 组织的轮番攻击，微步基于自研的黑客画像、威胁狩猎和追踪溯源系统，实现了对全球数十个活跃 APT 组织的持续追踪，发现了上百起针对国内的攻击活动，并积极配合监管机关和相关企业客户对威胁事件进行了应急处置。本报告以微步视角对主流 APT 组织在 2022 年期间的活动情况进行了分析总结，主要内容包括：

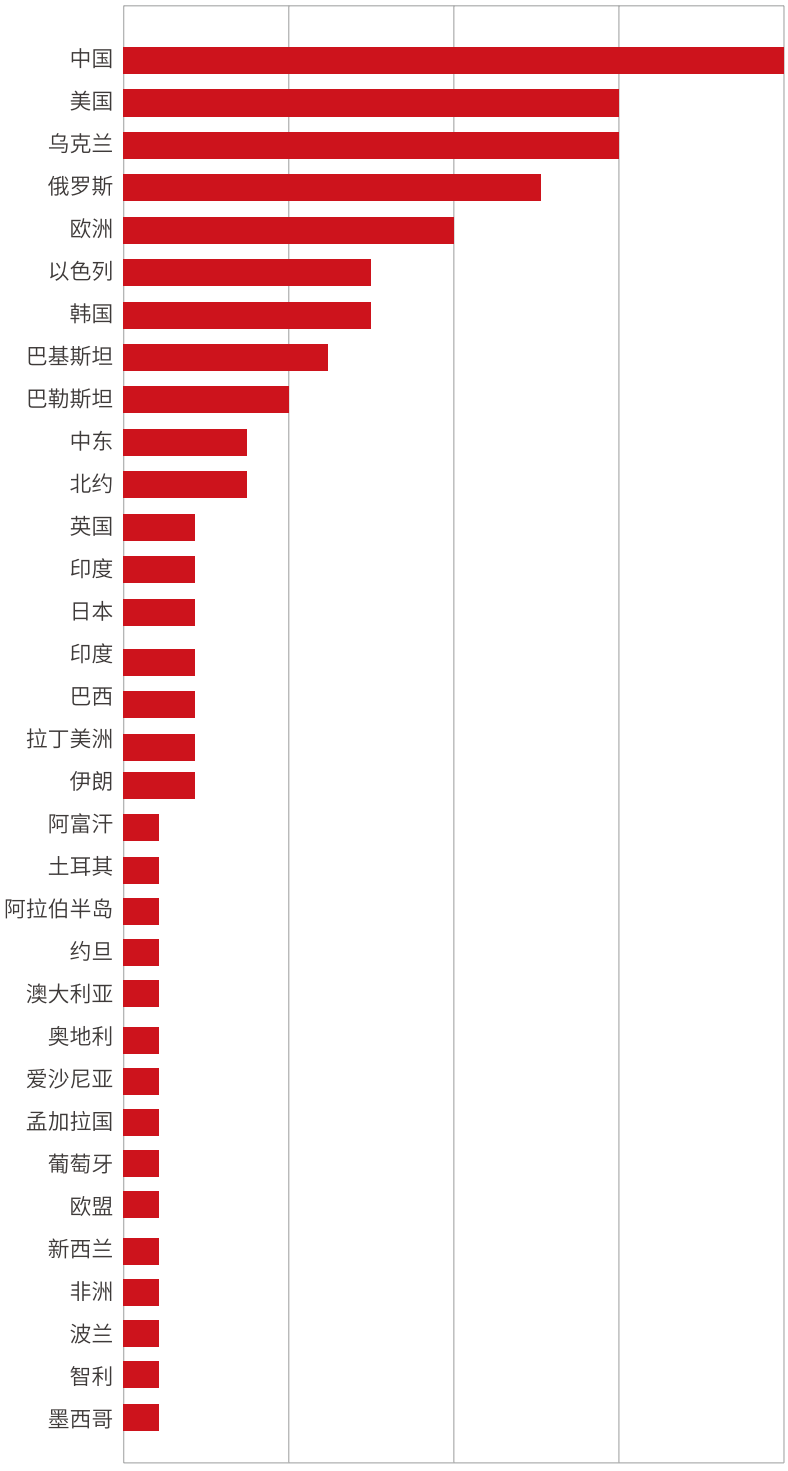
- 基于微步黑客画像系统统计发现，2022 年，受到 APT 组织影响的地区包括中国、美国、乌克兰、俄罗斯、韩国和巴基斯坦等，政府、金融、外交、军事、能源行业成为威胁行为组织瞄准的主要目标。
- 微步通过分析研究和应急响应，捕获了大量来自越南、印度、中国台湾以及部分未知地区的 APT 组织攻击活动，通过分析此类攻击活动总结出对我攻击的手法特征。
- 除针对我国的网络攻击活动外，俄对乌克攻击活动、Lazarus 投毒安全人员以及 Lapsus$ 团伙入侵知名企业等典型事件也给网络安全从业人员带来了更多启示。
- 最后以地域维度对 2022 年期间来自南亚、东南亚、东亚、东欧以及中东地区的 20 多个活动 APT 组织进行了较为全面的总结刻画。

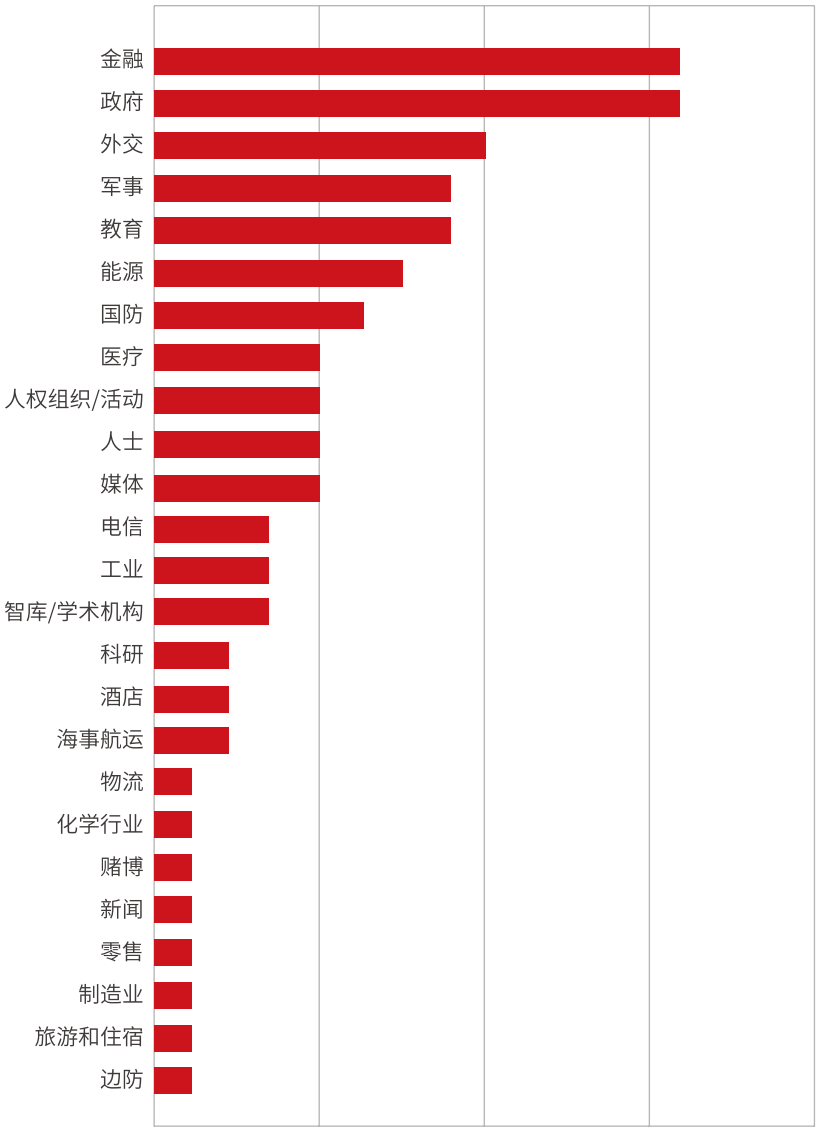
目录
CONTENTS

02

整体情况

基于微步在线黑客画像系统统计发现，2022 年期间被公开曝光的 APT 事件 150 余起，涉及 80 余个国家和地区遭受了不同程度的 APT 攻击。2022 年，受到 APT 组织影响的地区包括中国、美国、乌克兰、俄罗斯、韩国和巴基斯坦等，政府、金融、外交、军事、能源行业成为威胁行为组织瞄准的主要目标。而威胁行为组织主要来源于俄罗斯、南亚、朝鲜半岛和中东地区。




金融
政府
外交
军事
教育
能源
国防
医疗
人权组织/活动
人士
媒体
电信
工业
智库/学术机构
科研
酒店
海事航运
物流
化学行业
赌博
新闻
零售
制造业
旅游和住宿
边防

03

典型攻击团伙

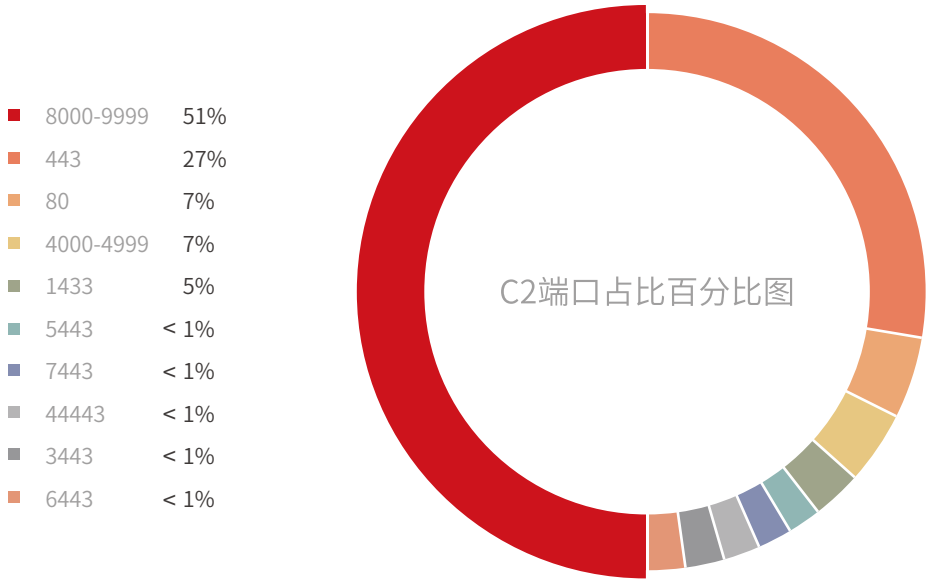
2022 年期间，微步情报局团队持续跟踪境内外的 APT 攻击活动，捕获了来自越南、印度、中国台湾以及部分尚未归因国家背景的 APT 组织对我发起的大量攻击活动，配合国内监管部门应急响应数十次，本章节以微步独立研究发现的多个典型 APT 组织特点为例子，展示当前境外 APT 组织对我攻击的手法特征。

海莲花

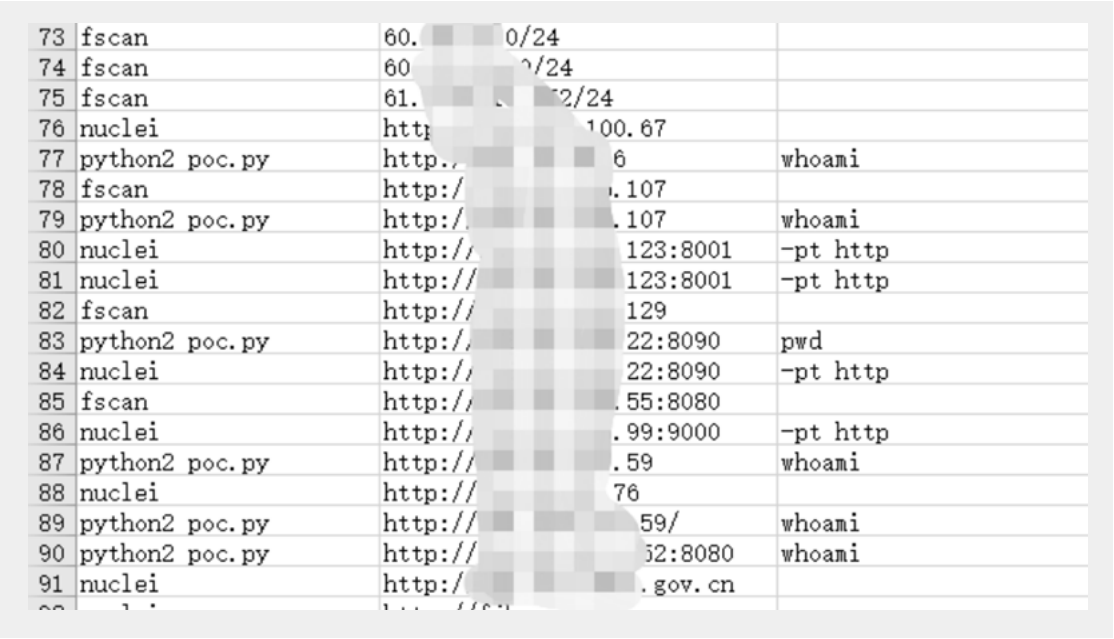
2022 年，微步情报局监测到疑似越南背景海莲花对国内的攻击活动高度活跃，研究人员通过资产同源、主动探测和样本狩猎等方式，掌握了海莲花组织的上百个 IP 资产，这些 IP 资产为发现海莲花组织针对国内的攻击活动提供了失陷检测能力。

在观察到的资产中，有许多 IP 地址位于中国境内、中国台湾和中国香港。这些 IP 地址对应机器已经被海莲花组织的攻击者攻陷，并被用作攻击跳板或流量代理设备，失陷的主机类型包括 Windows 和 Linux 系统，以及许多 IoT 设备，如 * 捷网关、*igor、*raytek、*vtech 和 * 星路由器。根据取得的证据，攻击者在去年三月就已经成功入侵了大量锐捷网关的主机，并将它们用于定向攻击。（为防止对部分品牌造成损害，在此处出现的品牌名称已经脱敏。）

在 APT 组织狩猎的过程中，一定会涉及到对资产的研究。根据微步情报局掌握的资产信息，海莲花组织的攻击者惯用端口统计如下图：



在具备海莲花组织失陷检测能力的基础上，微步情报局参与了多起关于海莲花组织攻击活动的重点取证事件，涉及行业包括政府机构、能源机构、海事机构、数据服务提供商和 IT 服务提供商。总体调查结果表明，海莲花的攻击者主要利用 Github 平台上的各种工具来实施外围打点，例如 nmap、fscan、nuclei、revsocks 和 Python 类型的漏洞利用脚本，利用特有木马、CobaltStrike、SSH、WebShell 的等方式来管理失陷机器。

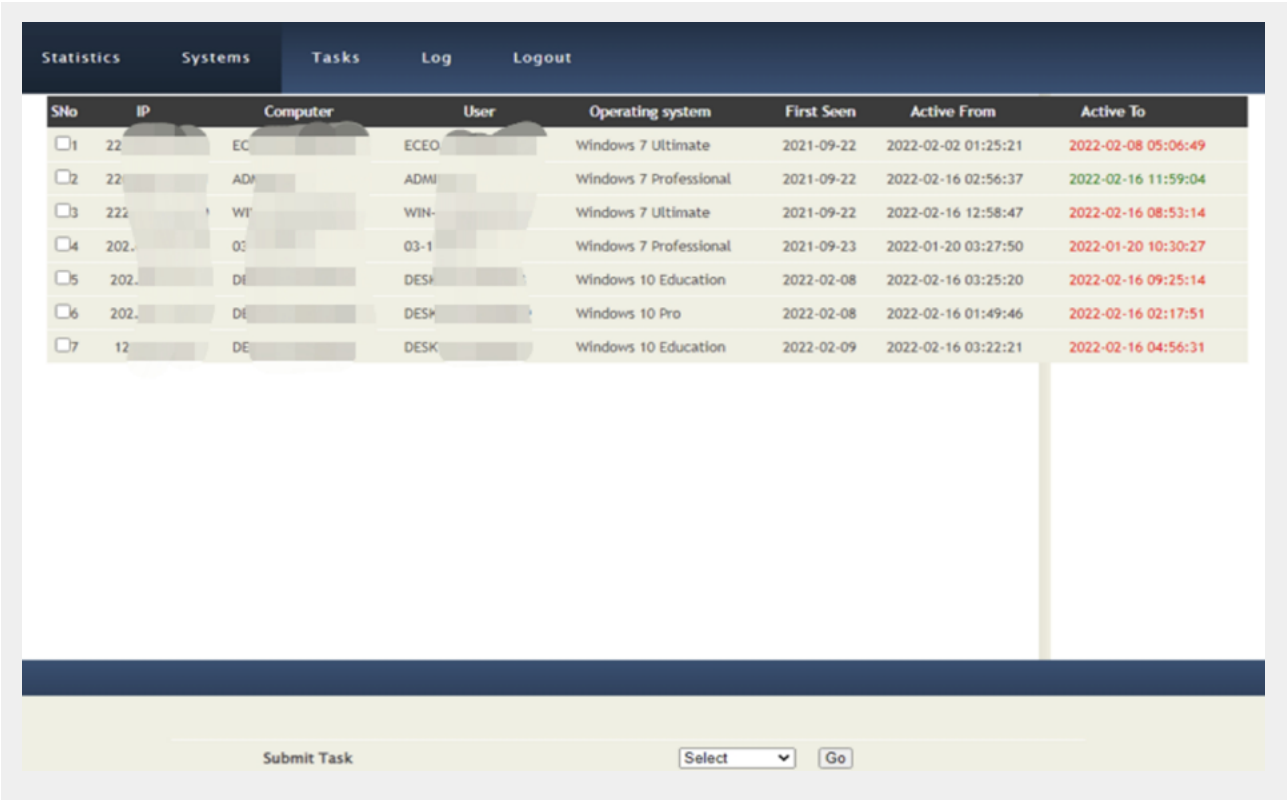


73	fscan	60. 0/24	
74	fscan	60 /24	
75	fscan	61. 2/24	
76	nuclei	htt 100.67	
77	python2 poc.py	http. 6	whoami
78	fscan	http:/ .107	
79	python2 poc.py	http:/ .107	whoami
80	nuclei	http:/ 123:8001	-pt http
81	nuclei	http:// 123:8001	-pt http
82	fscan	http:/ 129	
83	python2 poc.py	http:/ 22:8090	pwd
84	nuclei	http:/ 22:8090	-pt http
85	fscan	http:/ .55:8080	
86	nuclei	http:/ .99:9000	-pt http
87	python2 poc.py	http:// .59	whoami
88	nuclei	http:// 76	
89	python2 poc.py	http:// 59/	whoami
90	python2 poc.py	http:// 52:8080	whoami
91	nuclei	http:/ .gov.cn	

此外，在调查过程中，还发现用于实施攻击活动的跳板机器存在与海莲花组织关联的痕迹，例如越南语、海莲花组织的关联资产、关联木马等。

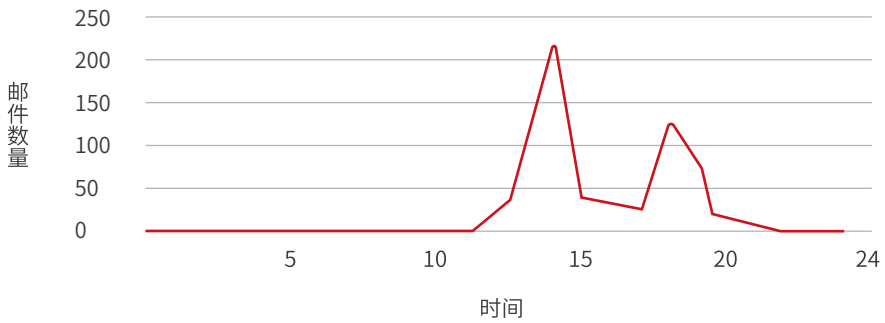
蔓灵花

在今年对南亚方向的持续追踪过程中，我们发现蔓灵花组织依然在使用与往年相同的 C&C 后台，且在其中发现了部分已经被控的主机，其中有来自孟加拉国、尼泊尔、中国的受害者，并且对攻击者对后台存放的木马进行分析后发现，攻击者存在着对老木马进行重开发迹象，在对这些重开发的木马进行持续追踪过程中，发现这批次木马被投递到我国重点行业的部分主机上。



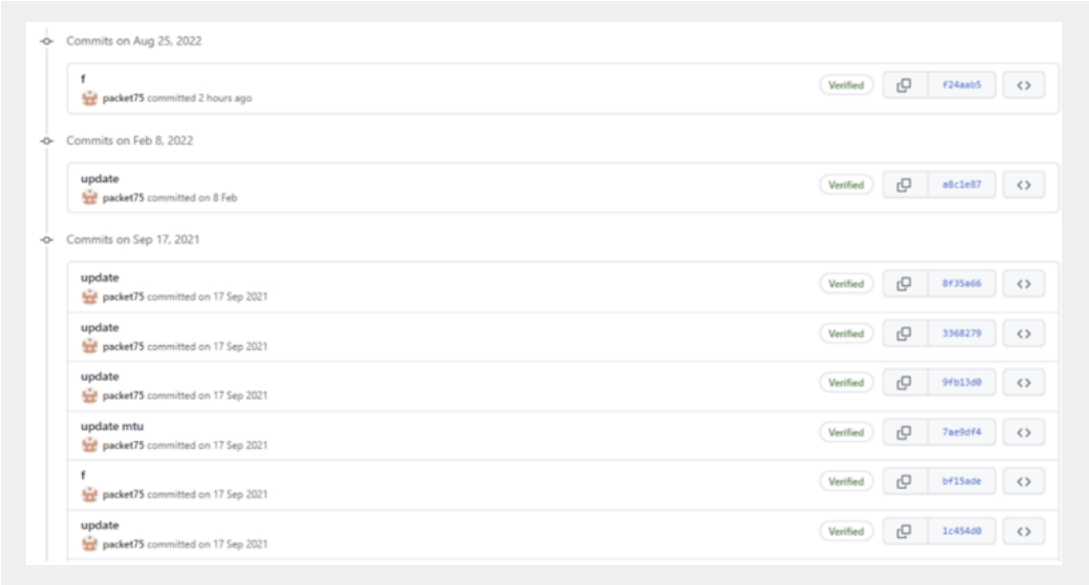
蔓灵花组织的后台

除此外，我们通过整理蔓灵花组织发送的大量钓鱼邮件，发现攻击者发送邮件时间段主要集中在北京时间的中午十二点到晚上八点，换算到印度时间为早上九点半至下午五点半，较为符合印度的工作作息时间，且其攻击目标主要集中在工业、航空航天、政府组织等行业。



白象

白象组织今年仍使用高仿钓鱼站对我国重点行业及单位发起攻击，且主要托管在公开平台 Netlify 中，利用“文件下载”、“邮箱登录”等话题作为诱饵发起钓鱼攻击。除了钓鱼攻击外，我们还发现该组织在今年多次利用 Github 仓库存放后续通信的 C2 地址，且在代码中使用多个 Github 仓库，当一个失效时，还会有其他几个作为替补，从攻击者所拥有的 Github 仓库的 Commit 记录来看，攻击者应该是将多个 C2 地址轮流使用。



Github仓库的Commit历史

绿斑

绿斑组织持续对我政府、科研、军工、航天、高校等单位的高频攻击，跟踪发现，该组织今年钓鱼链接有变化，直接访问域名无法打开钓鱼页面，需在后面加入指定后缀。在某次钓鱼活动中，攻击者使用了数字变量控制攻击目标，通过遍历该参数，我们识别出钓鱼网站后台存放目标邮箱地址超过 700 个。

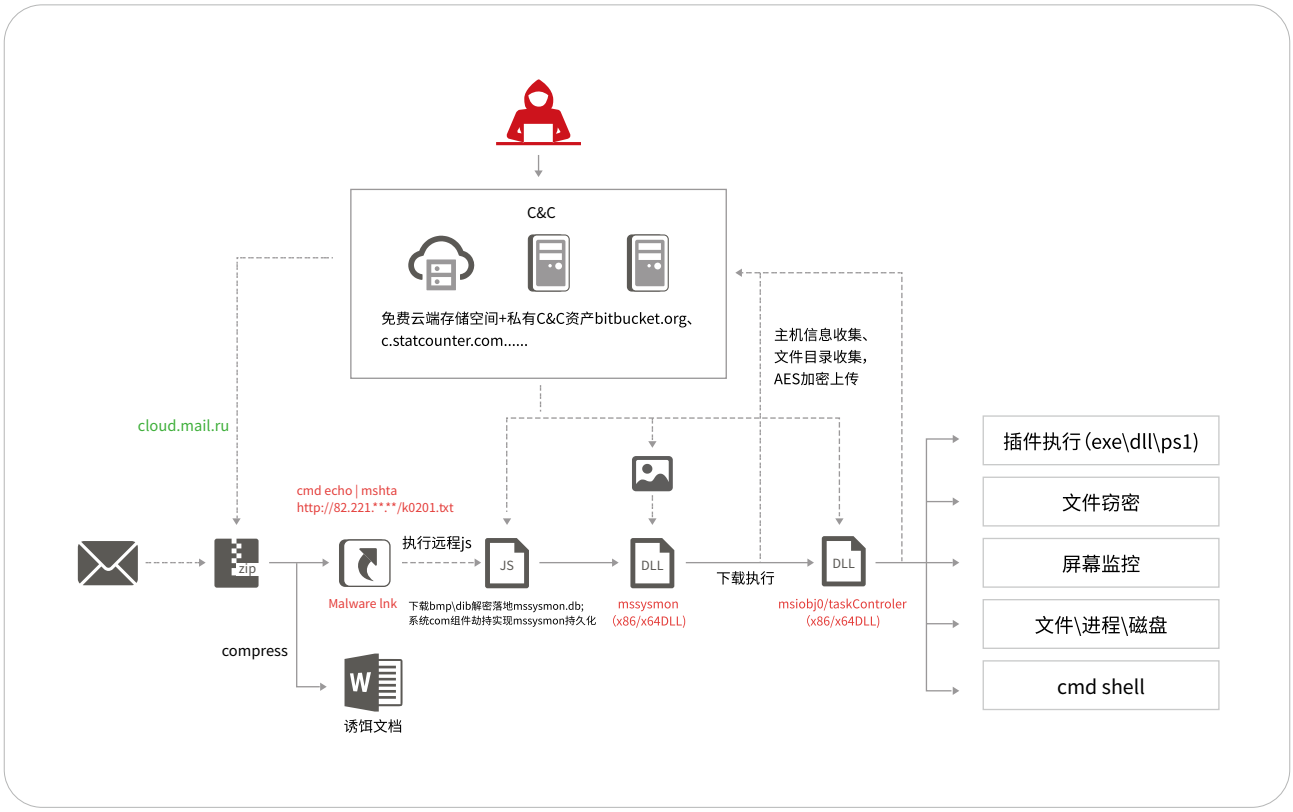
此外，由于目录权限设置错误，我们还发现了其钓鱼网站的部分日志，网站早期的访问 IP 地址均属于中国台湾地区，判断属于攻击者测试：

IP	运营商
1.1xx.xx.152	中华电信股份有限公司
36.2xx.xx.43	中华电信股份有限公司
36.2xx.xx.234	中华电信股份有限公司
111.2xx.xx8.94	中华电信股份有限公司
122.1xx.xx.19	中华电信股份有限公司

其他

在今年发现的 APT 攻击活动中，除上述较为频繁的组织外，还有一些针对性更强的低频 APT 攻击活动。这些攻击活动部分归属有些是已知 APT 组织例如 “伪猎者”，也有些未知 APT 组织例如“礼物陷阱”。

伪猎者 APT 组织于 2021 年由国内安全厂商披露，据悉，其最早攻击时间可以追溯到 2018 年，历史攻击目标为包含中国在内的人力资源和贸易相关机构。该组织从 2021 年 12 月份至今依然活跃，在今年上半年中，我们通过 APT 狩猎系统高危样本流程，捕获到该组织对韩国境内目标发起定向攻击活动样本，分别为 2022 年 2 月上旬针对 2022 平昌和平论坛相关人士的攻击和 2022 年 6 月中旬对 BernhardSeliger 博士的定向攻击。均为鱼叉邮件类型的攻击。从下载落地的压缩文件开始，落地载荷可分为三部分：具备恶意下载的 Lnk 文件，具备文件信息收集以及下载执行的下载器木马（mssysmon.db），具备文件窃密、插件加载、shell 功能的远控木马（TaskControler.dll）。本次样本与之前发现伪猎者攻击事件中落地载荷执行流程基本一致，第三阶段组件 TaskControler.dll 与历史事件具有相同导出函数、代码行为和通信过程基本一致。



“礼物陷阱”组织于 2022 年被微步情报局首次发现并命名，该组织擅长使用鱼叉邮件方式针对我国政府部门、互联网行业进行网络攻击。该组织使用精心伪装的钓鱼邮件，习惯在攻击前几天内注册高仿恶意域名，诱使受害者点击钓鱼连接或者打开恶意附件，通过注册计划任务下载后续攻击样本。整个攻击流程使用多个阶段脚本，最终恶意木马为开源项目 Poshc2。

微步在线通过 APT 狩猎系统高危域名情报生产流程发现部分可疑域名，感知到该组织发起的一起针对性攻击活动，此次活动中以伪装软件升级和伪造组织交流等邮件主题对国内用户进行攻击，在发现攻击样本后迅速帮助受害者进行排查，并且通过 APT 狩猎同源资产拓线流程系统发现更多相关线索、攻击样本和目标，同时帮助受害者阻断后续攻击。此次攻击活动中，该组织注册使用国内互联网大厂相关域名且契合邮件主题字段的钓鱼域名，且后续多阶段会错开受害者工作时间进行分发攻击，该组织样本免杀能力较弱且没有自研武器库能力。

通过 APT 狩猎同源画像系统，对这些低频 APT 组织进行溯源归因，大多数攻击活动会和已知 APT 组织有强归因，但还是存在部分组织和已有 APT 组织重叠性较差即弱归因，由于这些低频 APT 组织曝光时间较新，相关报告和情报较少，一旦出现 TTPS 较大更新，也难以归因。所以针对部分未知 APT 组织归因可信性较低，但我们仍为其创建新的组织命名，还同时建立详细画像规则，加入 APT 狩猎系统中，以便在后续发现和进行更深度的溯源归因。

04

典型攻击事件

除了针对我国的网络攻击活动外，另有一些典型的 APT 活动也需要引起网络安全从业人员的高度重视：

俄乌战争

2022 年 2 月中下旬，乌克兰东部局势恶化，其地方民间武装力量与乌政府的武装冲突因政治立场进一步升级成俄罗斯与乌克兰之间的国家级军事冲突。在此背景下，全球范围内借助战事热点的 APT 攻击活动达到空前规模。

从俄乌战争当事国之间的网络较量来看，公开披露的攻击事件主要为俄对乌的定向攻击，其中以 SandWorm、APT28、APT29、Turla 等为代表的俄背景全系 APT 组织对乌政府军工等目标单位发动了全方位的网络攻击，攻击方式包括 DDos 攻击、网络系统爆破、钓鱼攻击、窃密攻击、恶意主机数据擦除销毁以及针对 ICS 工控系统攻击。

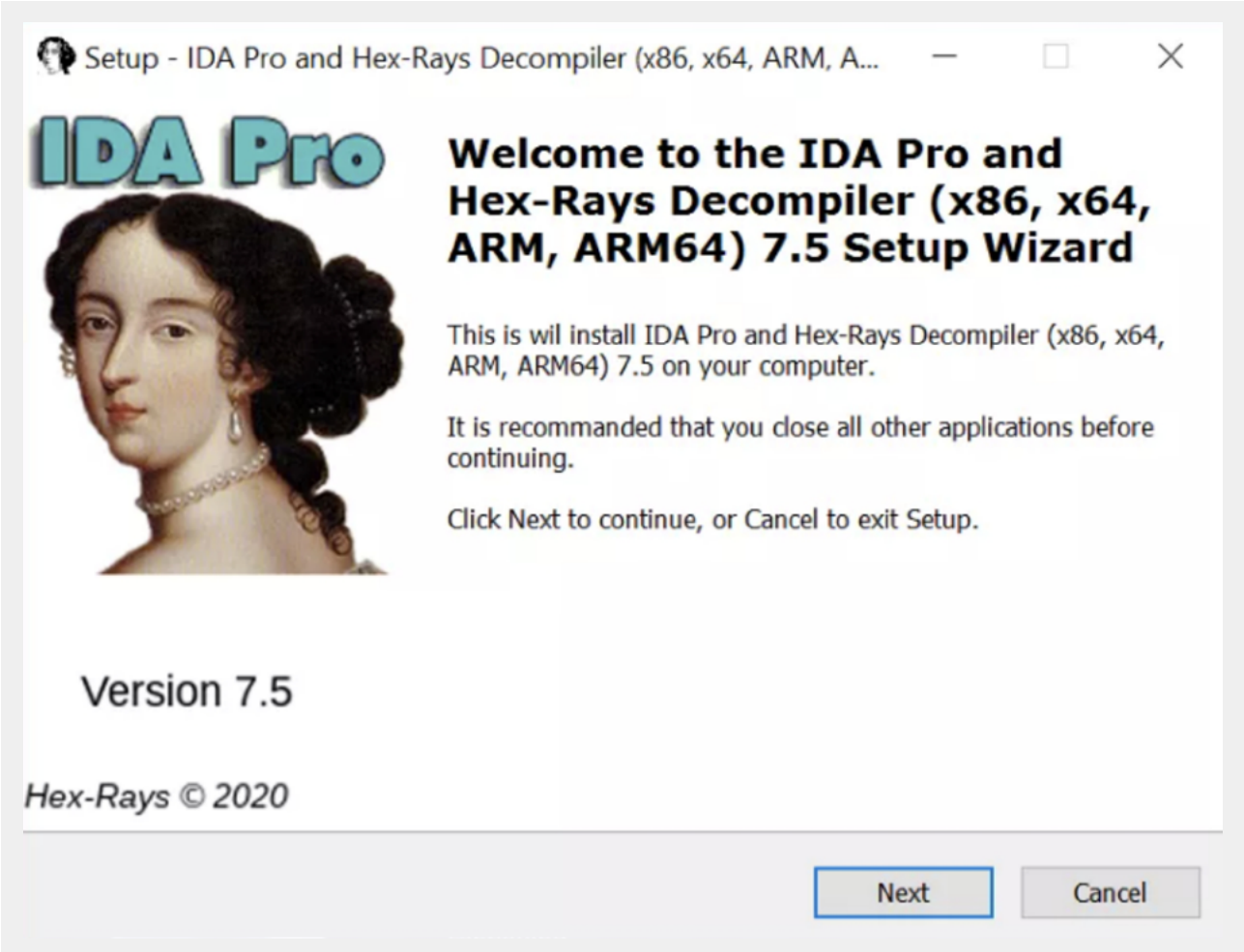
从检测及防守角度来看，后两类攻击值得警惕：恶意数据擦除销毁、针对 ICS 工控系统攻击。FoxBlade wiper、CaddyWiper 等类型数据擦除器是出于战争目的而生产使用的最直接网络武器，传统的 NDR 设备对此较为鸡肋，该类武器一旦投递成功，终端的安全对抗即成为最后防线。同样由 SandWorm 组织使用的针对 ICS 工控网络攻击乌电力系统的 Industroyer2 木马也值得引起注意，从震网病毒至今，对工控系统的攻击事件绝大多数是发生在特定军事冲突背景下的网络战，这种无须后续网络通信就可以完成既定破坏任务的武器值得我们重新探索工控领域中的安全防守底线。

Lazarus 利用 IDA 投毒事件

与去年发现的 Lazarus 组织攻击漏洞安全研究员相同，该组织在 2022 年期间依然将安全研究人员纳入攻击视线，利用反编译工具 IDA PRO 7.5 投毒对安全研究员发起攻击。

IDA Pro 是 Hex-Rays 公司的旗舰产品，意为交互式反汇编器专业版，是最流行的静态反编译软件之一，用户大多是安全研究人员，而由于其售价昂贵，部分用户下载使用盗版。而 Lazarus 组织则利用这一点发布捆绑恶意软件的盗版 IDA PRO 软件，推测其目的依旧为窃取安全研究人员手中的高价值 0Day 漏洞，用以扩充该组织军火库。

在木马中，Lazarus 组织使用恶意的 dll 替换了 IDA Pro 安装包的内部组件 win_fw.dll，通过其创建计划任务并启动另一恶意 dll 文件“idahelper.dll”，最终在 dll“idahelper.dll”中通过亦或解密出攻击者的 C2 地址并实现远程下载后续攻击载荷执行。



Lapsus$ 入侵十余家大型企事业机构

2022 年 3 月，一个名为 Lapsus$ 黑客组织异军突起，接连攻陷了英伟达、三星、育碧甚至微软等一系列科技巨头企业，成为本年度最具有话题性的网络安全事件。而通过对入侵事件的分析复盘发现，与其他靠技术吃饭黑客组织不同，Lapsus$ 主要将社会工程与目标企业内部人员价值发挥到最大，攻击成功后不会部署勒索软件，也因此很难被检出，更无法查杀，整体具有技术水平低、影响范围大的特点。

针对目标企业，Lapsus$ 主要是提前在论坛或者社交软件 Telegram 上，用葡萄牙语或英语发布招募贴，通过付费购买某目标企业员工或企业合作伙伴的登录凭证，但要求对方不仅要提供凭证，还需同意登录时多因素身份验证（MFA）的提示，或者让其在公司的工作站安装 Anydesk 或其他远程管理软件。为了实现对目标企业关键账户的访问，Lapsus$ 还用到了 SIM 卡调换这种欺骗性手段。过程中，攻击者主要是通过贿赂或欺骗通讯运营商企业员工，从而将目标账户的手机号码转移到攻击者自有设备。通过这种手段，攻击者可以拦截任何基于短信或电话发送给受害者的验证码，也可以通过短信重置线上账号密码。另外，Lapsus$ 还会利用已泄露在互联网中的登录账号密码或会话令牌，访问开放在互联网中的系统和应用，主要包括虚拟专用网络（VPN）、远程桌面协议 (RDP) 以及包括 ctrix 在内的虚拟桌面基础架构（VDI），甚至是 Azure Active Directory、Okta 等身份识别供应商系统。一旦通过失陷账户进入目标网络后，Lapsus$ 会利用多种策略发现更多的凭证或者入侵点，从而扩大其访问权限，主要包括利用 JIRA、Gitlab 和 Confluence 等内部可访问的服务器上未修补漏洞，或者搜索代码存储库、协作平台，获取公开的更高特权的账户或是访问其他敏感信息。

很多企业在进行安全防御投入的精力与成本，可能远不及攻击者的用心程度。一旦遇到这类轻技术、重社工的攻击，等到事发时往往为时已晚。

05

团伙详情

本章节以地域维度对 2022 年期间主流 APT 组织进行了较为全面的刻画，具体内容如下：

南亚

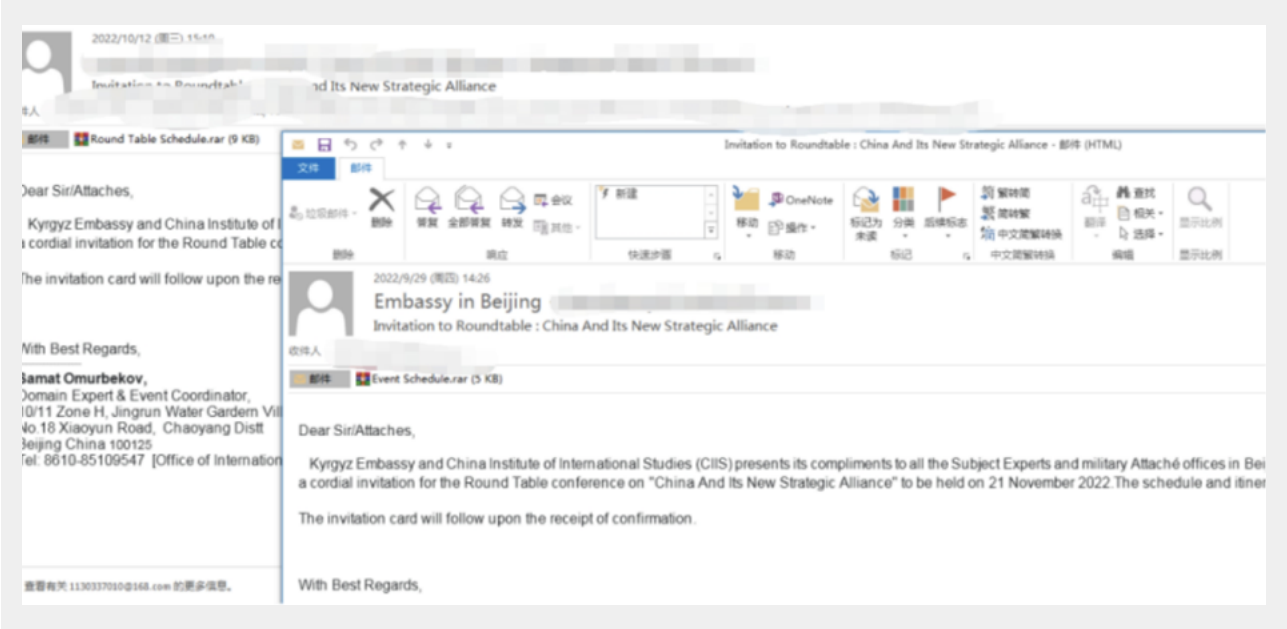
今年，在地缘、政治等多重因素影响下，印度黑客组织可谓异常活跃，针对周边国家的攻击活动频繁，包括中国、巴基斯坦、斯里兰卡、孟加拉国、尼泊尔、等邻国，攻击目标涵盖各国的政府、军队、医疗、航天、高校、科研等多行业。由于网络攻击具备双向性，所以疑似具有巴基斯坦背景的黑客组织透明部落和假旗部落，同样针对印度发起多次网络攻击。

印度攻击事件：

1. 蔓灵花

蔓灵花，又名 Bitter，是一个长期针对中国、巴基斯坦、蒙古、阿拉伯、土耳其等周边国家的政府、军工、航空等重点单位开展网络攻击的 APT 组织，其主要攻击目的为窃取敏感资料，具有较强的政治军事目的，该组织最早在 2016 年由美国安全公司 Forcepoint 进行了披露，其后，国内各大安全厂商持续对其网络攻击活动进行追踪曝光。

在 2022 年间，蔓灵花组织依然是南亚方向对我国发起攻击活动频次最高的组织之一，其攻击主要以窃取目标用户邮箱账号密码以及主机信息等为目的。在攻击方式上，蔓灵花组织使用的方式依然与往年相同，向目标发送带有恶意载荷的钓鱼邮件，钓鱼邮件中的恶意载荷包含有 .chm 的帮助文本格式、使用多个空白字符伪装为文档的 .exe 可执行程序，以及自解压程序。



蔓灵花的钓鱼邮件

2. 白象

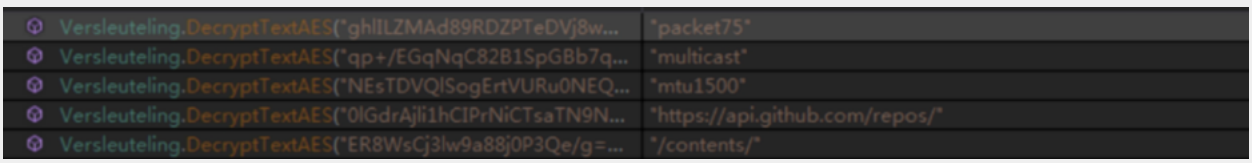
白象组织，又名“摩诃草”、“Patchwork”、“The Dropping Elephant”，是一个疑似具有印度国家背景的 APT 组织，该组织最早由 Norman 安全公司于 2013 年曝光，主要针对中国、巴基斯坦等亚洲地区国家进行网络间谍活动，其中以窃取敏感信息为主，相关攻击活动最早可以追溯到 2009 年 11 月。

2022 年，白象依然对中国保持着高频次的攻击，除了中国外，孟加拉国、尼泊尔等周边国家也遭受到不同程度的网络攻击。白象的攻击方式主要分为两类，一类是通过钓鱼站点达到窃取邮箱的目的，一类是通过种植恶意木马达到远控窃密的目的。

白象所使用的钓鱼站点依然多为公开服务例如 netlify 搭建钓鱼页面，通过仿冒官方网址引诱用户输入账号密码，以往利用 Github Page 发布钓鱼页面的攻击方式在今年有所减少。

在恶意载荷方面，白象组织使用的载荷中加解密、混淆、免杀等对抗手段有了提升，使用基于 BADNEWS 木马重开发的 Ragnatela。在今年发现的木马中，主要利用读取指定 Github 仓库解密 C2，通过自定义加解密，从仓库中的指定字段中解密出 C2 地址，给分析上带来一定困难。除此外，据 MalwareBytes 披露，在白象攻击者的 C2 服务器上，发现了攻击者主控端的屏幕截图，从其中可以发现攻击者使用印度语，并且在 Vmware 与 VirtualBox 测试木马，使用 VPN Secure 以及 CyberGhost 隐藏自己的 IP 地址，从攻击者的屏幕截图中还发现攻击者登陆了巴基斯坦某政府单位的邮箱。

针对中国的钓鱼站点



解密的 Github 仓库地址

3. 响尾蛇

响尾蛇 APT 组织（SideWinder）是一支疑似具有印度政府背景的黑客组织，最早活跃可追溯到 2012 年。其攻击目标主要为中国、巴基斯坦、孟加拉国等国家的军工、外交、科研等相关敏感单位。

今年，响尾蛇的攻击目标同样集中在中国及巴基斯坦等周边国家，攻击方式上并没有太大变化，依然使用钓鱼邮件投递载荷，利用恶意 .lnk 或文档类型文件远程下载执行后续载荷。响尾蛇的多阶段恶意载荷分别部署在不同 C2 服务器中，多阶段执行后下载最后阶段的木马对目标实现远控。

在资产上，该组织的资产特点依然与往年相同，在域名上仿冒正常网址，例如在针对巴基斯坦的攻击中就仿冒巴基斯坦官方的网址，而在针对中国的攻击中，则仿冒阿里云、新浪等官方域名。


邮件 未命名的附件 00006.zip (1 KB)

公共管理学院关于11月22日起工作安排调整的通知

当前北京市疫情正处于快速增长期，校园面临严峻挑战。为坚决遏制疫情向校园扩散蔓延，全力维护校园安全，根据北京市和[redacted]关于疫情防控要求和学院实际，对近期工作调整通知如下：

1. 按防控政策有居家要求的教职工，近期不到校，配合属地要求做好疫情防控，实行居家办公、线上授课；请居住在校内家属区的人员减少流动，不前往教学办公区；请在校学生不前往校内家属区；其他教职工非必要不到校、灵活办公，建议尽量居家办公、线上授课。

2. 学院安排领导每天带班，各办公室根据近期工作计划安排部分人员到岗（见附件名单），确因工作需要进校的教职工，请保持学校与家两点一线原则，尽量避免与学生有时空交集。

响尾蛇组织发送的邮件


RESTRICTED

GOVERNMENT OF
PAKISTAN
MINISTRY OF INTERIOR

VERIFICATION FORM

This form is the light of directions issued through policy of Ministry of Interior vide M/O/Interior's U.O. No 1193/2011-JS (A/S), dated 04.03.2011 and SOP Issued by the District Magistrate Islamabad vide No.1467/2018 dated 02 May 2018

CNIC / License No

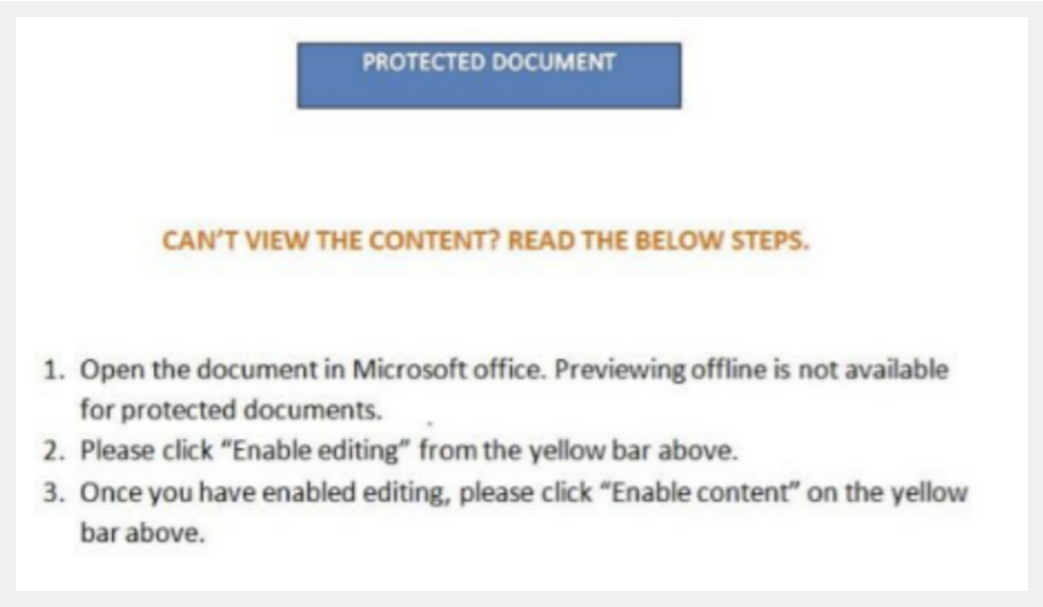
响尾蛇组织诱饵文件

4. 肚脑虫

肚脑虫（Donot）是一个疑似印度背景的 APT 组织，主要针对巴基斯坦、孟加拉国等南亚地区国家进行网络间谍活动，除此外今年还发现了针对泰国、斯里兰卡等地的攻击活动，该组织主要针对政府机构、重点企业等领域进行攻击，其中以窃取敏感信息为主。其攻击活动可以追溯到 2016 年至今。

肚脑虫组织的攻击目标主要集中在巴基斯坦、孟加拉国、斯里兰卡等国家的政府、军工等行业，该组织拥有 PC 端与移动端双平台攻击能力。在今年发现的攻击中，肚脑虫组织常依然使用恶意文档进行攻击，包括模板注入的 .rtf 文件以及附带宏代码的 Office 文档。肚脑虫组织的对抗手段也在今年有所改进，该组织的木马在发起 C2 请求时会使用特定的字段的特定内容，当 C2 服务器判断指定字段的对应内容符合预期时才会继续下发后续恶意载荷。而在后续 PE 文件中 Donot 组织除了使用 Sleep 函数进行休眠对抗调试，还会利用系统时间来进行判断，在加解密方面，该组织依然使用简单的亦或和加减进行加解密。

在资产方面，肚脑虫组织的资产特点依然明显，不过唯一有所不同的是在今年常用的顶级域名变为了 .buzz，其他测绘等重要的特征依然没有改变。



肚脑虫组织恶意文档

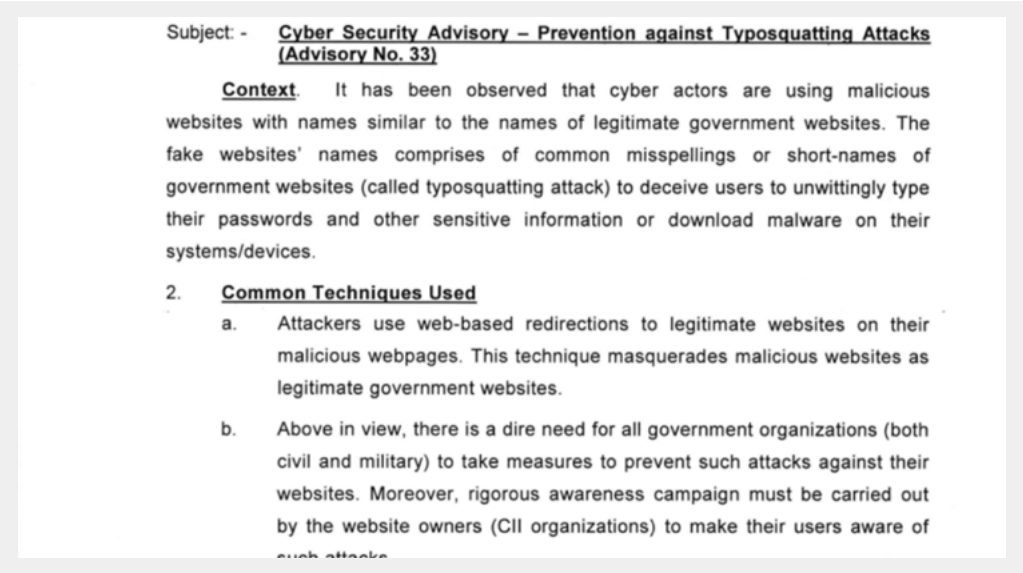
肚脑虫组织的计划任务

5.GroupA21

GroupA21 组织，又名“BabyElephant”、“幼象”，疑似是一个来自具有印度背景的 APT 组织，该组织最早的攻击活动可以追溯到 2017 年 7 月，其主要攻击目标为巴基斯坦、斯里兰卡、孟加拉国等国的政府、军队等单位，在 2021 年首次发现针对中国的攻击活动。

今年发现的攻击活动中，GroupA21 组织使用钓鱼邮件投递恶意压缩包，恶意压缩包通常由诱饵文件、恶意木马、.lnk 木马三项组成，而诱饵文件通常来自正常官方网站的 .pdf 文件。在后续攻击载荷方面，GroupA21 组织依然尝试用公开的商业木马或开源木马，例如 Cobalt Strike、Sliver、Netwire 等木马，除此外我们还发现 GroupA21 组织在今年自研的一款被称为“Warhawk”的木马，木马包含下载执行、命令执行、文件管理、文件上传多种功能。

在资产方面，GroupA21 组织依然模仿响尾蛇组织的特征，使用“-”、“gov”等作为关键词，仿冒正常网址。



Subject: - **Cyber Security Advisory – Prevention against Typosquatting Attacks (Advisory No. 33)**

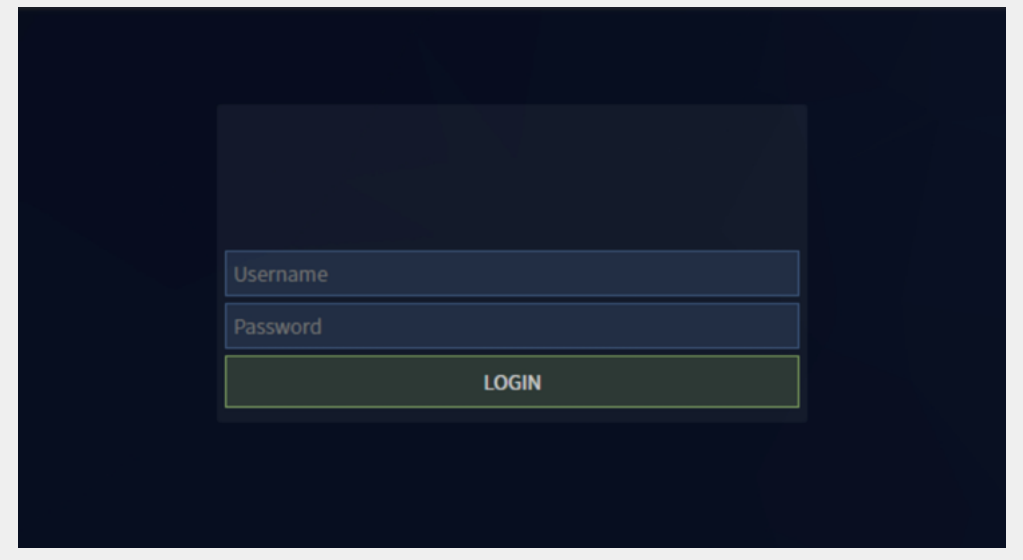
Context. It has been observed that cyber actors are using malicious websites with names similar to the names of legitimate government websites. The fake websites' names comprises of common misspellings or short-names of government websites (called typosquatting attack) to deceive users to unwittingly type their passwords and other sensitive information or download malware on their systems/devices.

2. **Common Techniques Used**

a. Attackers use web-based redirections to legitimate websites on their malicious webpages. This technique masquerades malicious websites as legitimate government websites.

b. Above in view, there is a dire need for all government organizations (both civil and military) to take measures to prevent such attacks against their websites. Moreover, rigorous awareness campaign must be carried out by the website owners (CII organizations) to make their users aware of

GroupA21 组织诱饵文件



Warhawk 木马后台页面

6. 孔夫子

孔夫子（Confucius）组织是一个疑似印度背景的 APT 组织，自 2013 年开始活跃，主要针对巴基斯坦等南亚各国的政府、军事等行业目标进行攻击。该组织早期攻击活动中的恶意代码和基础设施与白象 APT 组织存在较大重合，但目标侧重有所不同，所以孔夫子组织曾一度被认为是白象 APT 组织的某个分支机构。

今年攻击活动中，攻击活动都集中在印度周边国家，针对中国的攻击活动较少，在攻击手法上变化不大，唯一有所改变的是在诱饵文档中添加了密码保护，而密码会随钓鱼邮件一同发送给目标，由于文档有密码保护，导致许多杀软不能检测出恶意行为。

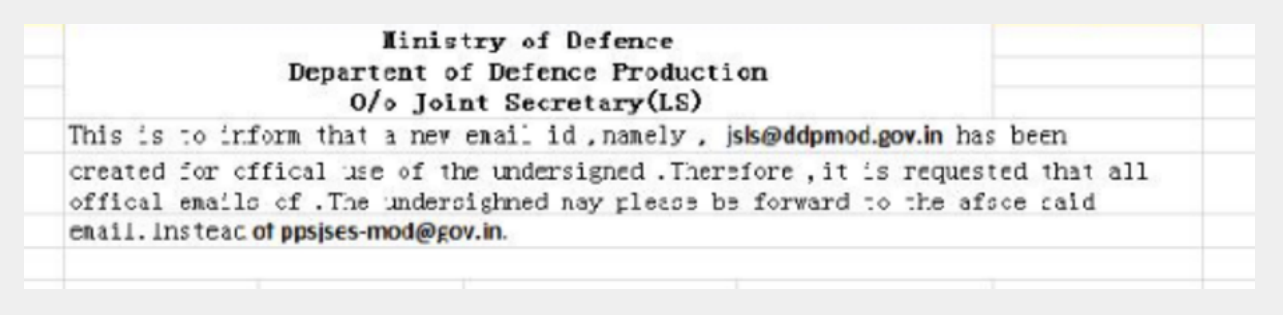
孔夫子组织诱饵文档

孔夫子组织诱饵文档

7. 透明部落

透明部落又称 APT36、ProjectM、C-Major，疑似是具有巴基斯坦背景的黑客组织，其活动可以追溯到 2013 年。该组织主要使用鱼叉式网络钓鱼和水坑攻击，长期针对印度的政治、军事进行定向攻击活动，针对印度的政府、公共部门、各行各业包括但不限于医疗、电力、金融、制造业等进行攻击和信息窥探。在涉及到的攻击目标中基本事关国家安全、稳健发展的职能或研究单位 / 部门，具备极高的国家战略价值。常使用一种称为 Crimson RAT 的 .NET RAT 作为主要控制木马。还曾被发现广泛传播 USB 蠕虫、使用基于 Python 开发的 RAT-Peppy 作为武器。

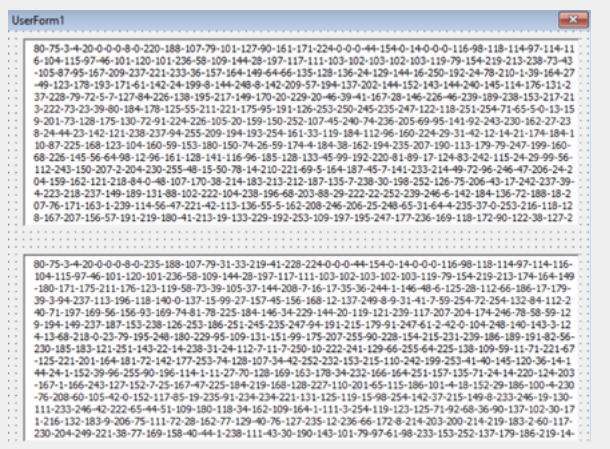
该组织具备 Windows 和安卓双平台能力，Android 平台攻击使用商业间谍软件 SpyNote 和 SonicSpy，以及开源间谍软件 AhMyth 和 Metasploit；该组织在针对 Windows 的攻击过程中常使用带有嵌入宏的恶意文档。使用诱人的文档和文件名（通常称为蜜陷阱）来诱骗受害者在其端点上执行恶意内容。


Ministry of Defence
Departent of Defence Production
O/o Joint Secretary(LS)
This is to inform that a new emai. id ,namely , jsls@ddpmod.gov.in has been created for offical use of the undersigned .Therefore ,it is requested that all offical emails of .The undersighned nay please be forward to the afore said email. Insteac of ppsjses-mod@gov.in.

透明部落使用的武器特征如下:

1、USB 蠕虫

通过木马部署一个模块来感染 USB 设备。感染 USB 设备中的文档文件，在这些文档被嵌入恶意 VBA 代码，通过 USB 设备横移后，传播这些感染的文档，当新的受害者打开感染文档后会释放包含恶意负载的编码 ZIP 文件。



该宏将 ZIP 文件放入在 %ALLUSERPROFILE% 下创建的新目录中，并在同一位置提取存档内容。目录名称可以不同，具体取决于示例:

%ALLUSERSPROFILE%\ 媒体列表 \tbvrarthsa.zip
%ALLUSERSPROFILE%\Media-List\tbvrarthsa.exe

2、Crimson RAT

Crimson RAT 在 2016 年被首次披露，是一种基于 .NET 编写的专有 RAT，作为该组织进行网络间谍活动的首选恶意软件并沿用至今，允许攻击者获取有关受感染机器的基本信息、收集屏幕截图、操纵文件系统以及下载或上传任意文件。

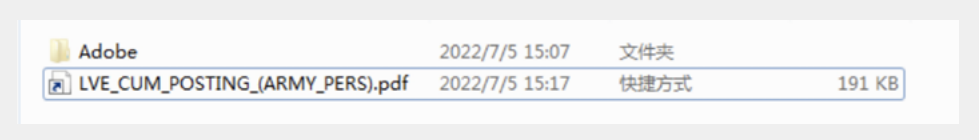
Crimson 依赖于额外的模块负载来进一步丰富其特性集。这些模块包括键盘记录、浏览器凭证窃取、自动搜索和窃取可移动驱动器上的文件，以及两个不同的有效载荷更新模块。该组织的 C2 大都属于 Contabo GmbH 托管服务提供商，该托管服务器在南亚地区的威胁组织中较受青睐。

透明部落一直以来针对军事和外交使用广泛的基础设施来支持他们的行动并不断更新他们的武器库。该组织持续不断的开发 Crimson RAT、USBWorm、基于 Pyinstaller 打包的 EXE 等，以执行情报活动和监视敏感目标。

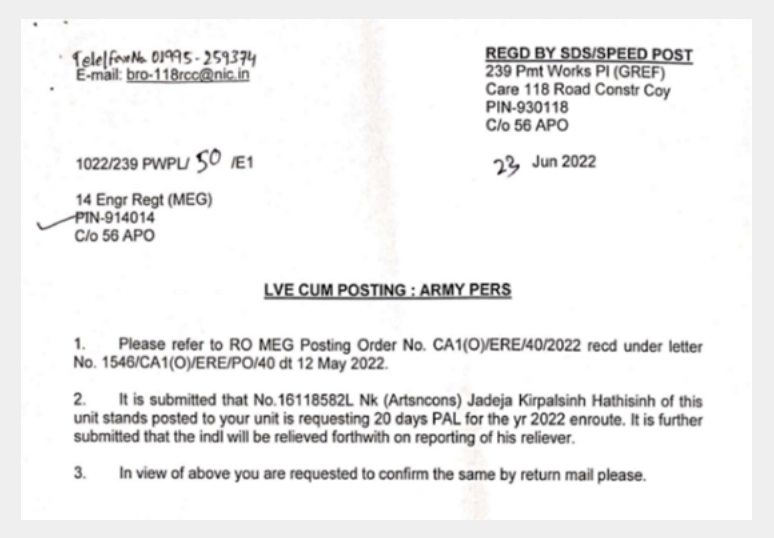
8. 假旗部落

假旗部落组织，又称 sidecopy、FalseFlager。至少自 2019 年开始活动，主要针对印度开展网络间谍活动。该组织善于向受害者发送时政和军事等目标相关信息制作的钓鱼邮件和诱饵文档，通过远程模板攻击的方式访问挂载了诱饵文档和恶意软件的失陷网站，以获取电子邮件凭据。在元数据、漏洞利用代码、文件名称和白利用程序等多个关键点模仿来自印度的肚脑虫、响尾蛇 等 APT 组织。

假旗部落喜欢使用公开的代码及工具，如: CetaRAT、ReverseRAT、MargulasRAT（自有远控软件）、AllakoreRAT、Bella RAT（mac os 平台）等，以及多款 C# 插件。在某些感染链中 SideCopy 使用了 Python 远程访问工具 BackNet。

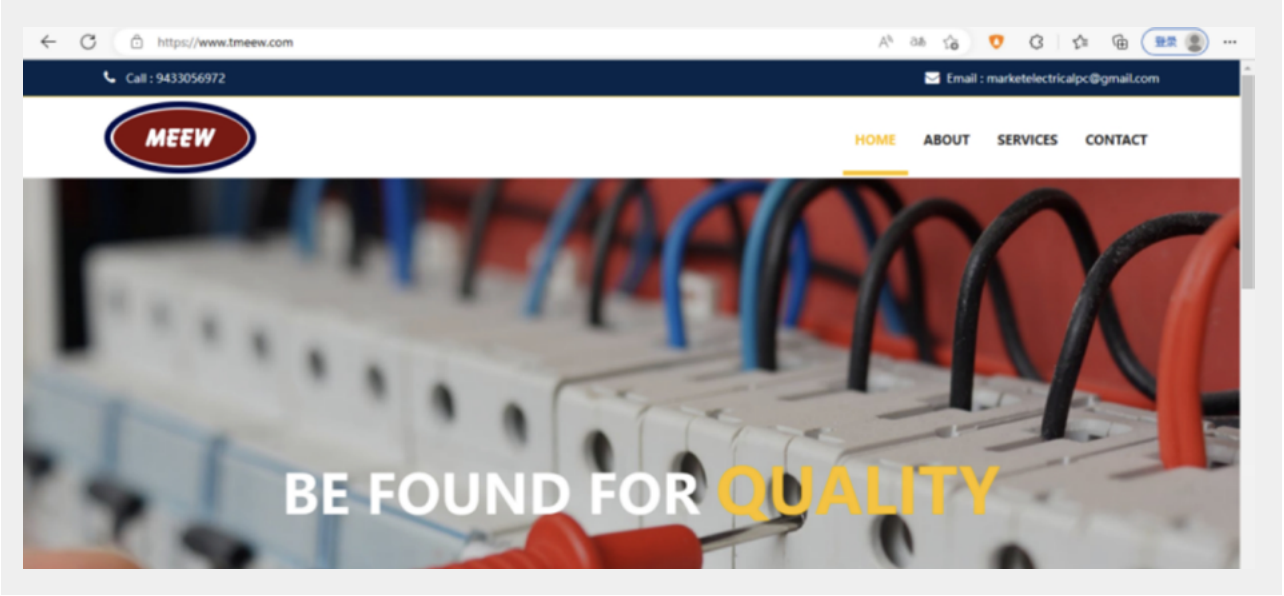


伪装成 pdf 的诱饵文档



假旗部落诱饵文档

LNK 文件中执行的链接



失陷网站

连接到失陷网站“https://tmeew.com/assets/carousel/files/LVE_CUM_POSTING_(ARMY_PERS)/jspxtoolkit/jqueryxmlcss.hta”并下载“.hta”恶意文件。

东南亚

东南亚地区最活跃的 APT 组织当属“海莲花”。2022 年，微步情报局的 APT 狩猎系统捕获到该组织的上百个攻击资产，其中大量 IP 属于被利用的失陷设备。除了“海莲花”组织之外，研究人员还发现了一类使用 Glitch 平台作为 C2 托管的鱼叉式钓鱼邮件。大多数样本上传地址为越南地区，这些样本的代码混淆、花指令、DLL 侧加载的手法与历史上“海莲花”组织使用的技术高度相似，可以合理怀疑“海莲花”存在人员变动等因素。

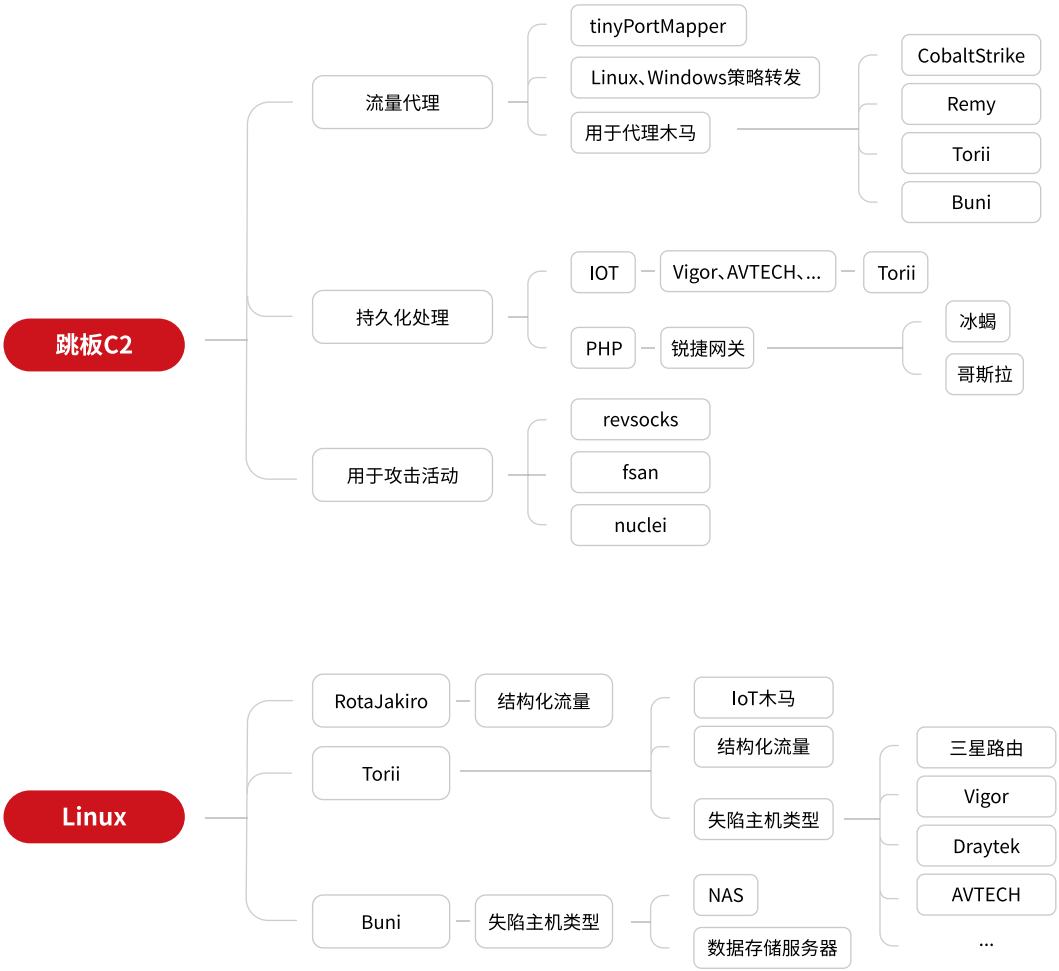
1. 海莲花

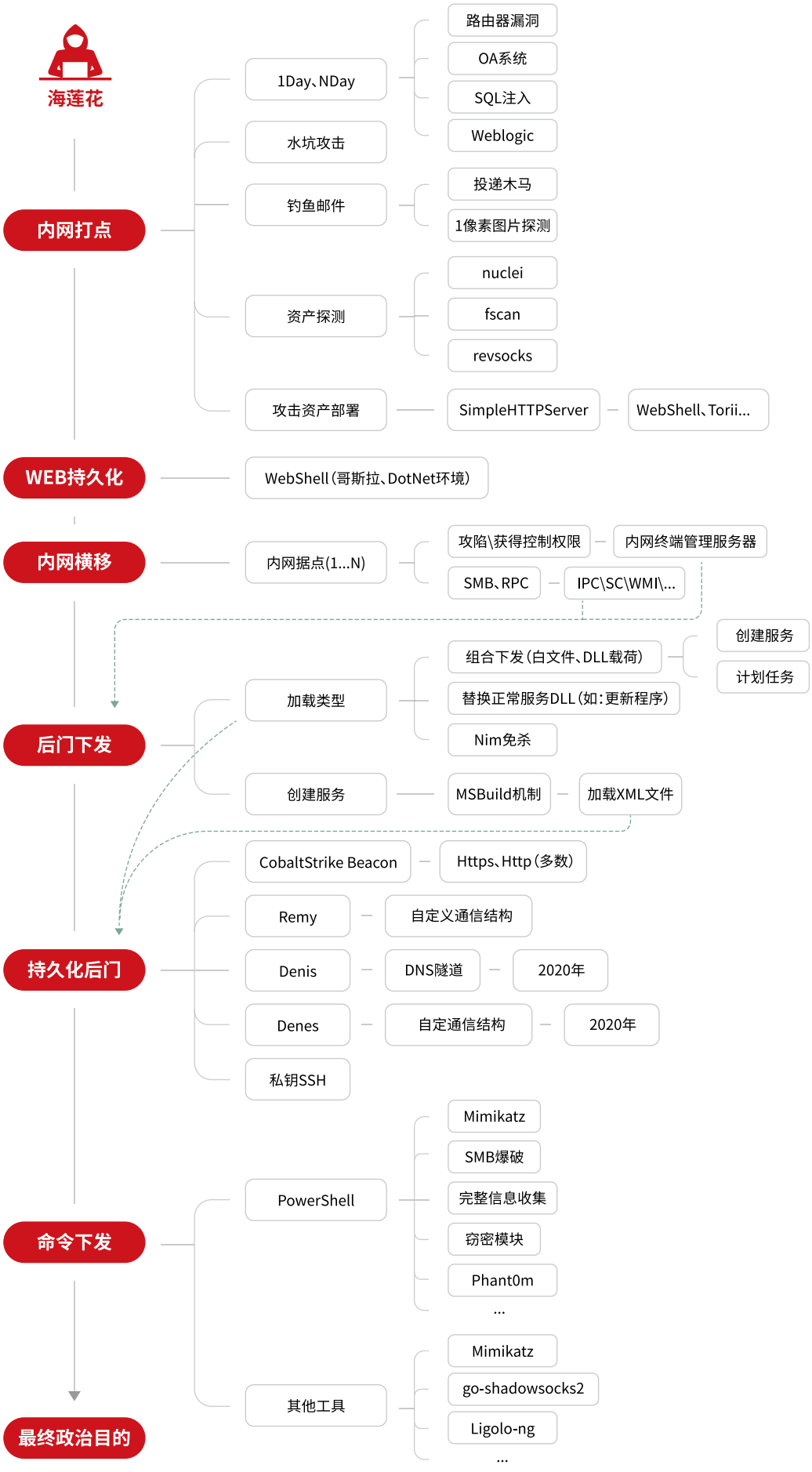
“海莲花”，也称为 APT32 和 OceanLotus，疑似具备越南政府背景的黑客组织，该组织至少从 2012 年开始活跃，是目前东南亚地区最活跃的 APT 组织之一。

通过多维度的分析，包括资产和样本，微步情报局发现了今年该组织针对中国地区进行的大量网络间谍活动。活动涉及政府机构、能源机构、海事机构、数据服务提供商、IT 服务提供商和许多暴露在互联网上的物联网设备。

APT32 攻击者惯用去年流行的攻击方法，主要以漏洞利用为主。近两年的取证痕迹表明，APT32 组织在渗透初始阶段投入了更多的资源。容易成为目标的系统类型包括 OA 系统、物联网设备、数据库服务器、Weblogic 服务器等。

APT32 组织画像大致如下：

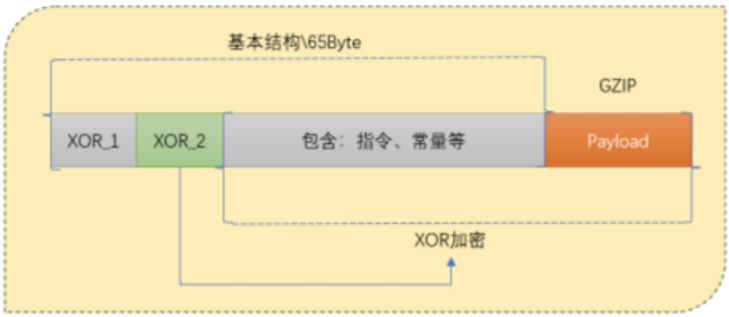



海莲花
内网打点
1Day、NDay
路由器漏洞
OA系统
SQL注入
Weblogic
水坑攻击
钓鱼邮件
投递木马
1像素图片探测
资产探测
nuclei
fscan
revsocks
攻击资产部署
SimpleHTTPServer
WebShell、Torii...
WEB持久化
WebShell（哥斯拉、DotNet环境）
内网横移
内网据点(1...N)
攻陷\获得控制权限
内网终端管理服务器
SMB、RPC
IPC\SC\WMI\...
后门下发
加载类型
组合下发（白文件、DLL载荷）
创建服务
计划任务
替换正常服务DLL（如：更新程序）
Nim免杀
创建服务
MSBuild机制
加载XML文件
持久化后门
CobaltStrike Beacon
Https、Http（多数）
Remy
自定义通信结构
Denis
DNS隧道
2020年
Denes
自定通信结构
2020年
私钥SSH
命令下发
PowerShell
Mimikatz
SMB爆破
完整信息收集
窃密模块
Phant0m
...
其他工具
Mimikatz
go-shadowsocks2
Ligolo-ng
...
最终政治目的

在 Windows 平台上，通过在内网主机中植入持久化后门（如 CobaltStrike 和 Remy），并使用多种手段（如 DLL 侧加载、“一机一码”和小众的 Nim 语言编译）来免杀和规避沙箱，攻击者可以更有效地侵入内网。在内网作战工具方面，攻击者主要使用开源项目，如 PassHashes、go-shadowsocks2、Phant0m 和 Mimikatz 等。

在 Linux 平台中，微步情报局首次披露了 APT32 组织使用的 Buni 家族木马。Buni 与“双头龙”在单一进程实例、信息收集、C2 编码、结构化通信流量等技术特点几乎一致，但流量加密方式和指令类型有所不同，研究人员在数据服务供应商的服务器中提取了该木马。

```
struct packet_format
{
  char dec_xor[2];
  char unknow1[4];
  char constant_1;
  char random_32[32];
  char command_type[2];
  char unknow2[4];
  char error_status[2];
  char payload_length[4];
  char command_sub_type;
  char unknow3[4];
  char unknow4[4];
  char unknow5[4];
  char has_payload;
  char payload[payload_length];
};
```




```
# 1 or 0
# 4c 57 a7
```

此外，微步情报局还首次证实“海莲花”组织是 Torii 僵尸网络的运营者，在取证中发现 Torii 后门用于控制 APT32 攻击活动中的流量跳板设备。Torii 家族具有结构化流量的特点，与 Buni 和“双头龙”两个家族有相似之处。它的交叉编译方式可以覆盖多种架构的 IoT 设备和 PC 主机，包括 ARM、x86、x64、MIPS、SuperH 等。在通信资产层面，APT32 组织一直在致力于隐藏和代理 CobaltStrike C2 通信流量。他们入侵了大量路由器、摄像头、安全网关等 IoT 设备，用于 CobaltStrike 木马控制和命令服务器的流量中转。APT32 利用失陷机器流量转发的方式包括：iptables、tinyPortMapper 和 Gost，被代理流量的木马类型包括 CobaltStrike、Buni、Torii 和 Remy 等。

东亚

1. 拉撒路

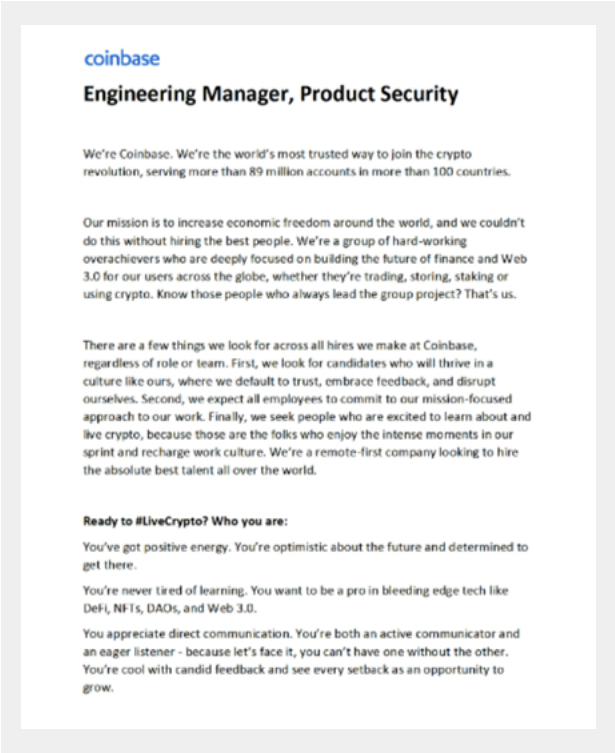
拉撒路（Lazarus）组织为朝鲜半岛地区大型 APT 组织，是当前活跃度最高的 APT 组织之一，该组织整体攻击水平较高，攻击活动涵盖政府、国防、教育、研究中心、金融、能源、航空航天、运输、医疗、加密货币等诸多具有高经济价值的行业领域。

在今年观察到的活动中，拉撒路组织的攻击涵盖了全球范围，包括德国、巴西、印度、意大利、墨西哥、瑞士、土耳其等国家。在攻击手法上，拉撒路组织擅长针对不同行业实施精准的社会工程学攻击，例如使用“工作机会”相关的话题针对洛克希德马丁公司、BAE 系统公司的求职人员，此类社会工程学的手法被用在 Windows 和 MacOS 双平台的活动中。

在后门方面，拉撒路组织使用 Github 托管方式进行 C2 地址指令下发，以及使用以往的老旧木马“DTrack”对外发起攻击，在白加黑方面拉撒路组织也有所创新，与常见的将白文件与黑文件放在同一目录下直接加载不同，拉撒路组织使用白文件加载系统恶意“dui70.dll”，再通过系统 dll 加载恶意 dll 文件，与常见的白加黑相比多了一个环节，推测是为了干扰分析。

此外，微步情报局还在今年发现拉撒路组织通过修改开源项目 SumatraPDF 阅读器进行攻击的活动，拉撒路组织以往也有类似的攻击活动，但以往都是使用“诱饵 .PDF”的方式直接执行恶意代码，而今年却通过修改开源项目代码，将恶意代码写入阅读器代码中，只有当通过阅读器启动指定 hash 的文件时，才会执行恶意代码，这在一定程度上可以规避杀软查杀和逃避沙箱检测。

在针对密币行业方面，拉撒路组织除了使用钓鱼站点对 NFT 相关人员发起钓鱼攻击外，还会通过克隆交易所的官方页面，仿冒出交易所站点，并在其中托管恶意攻击载荷，利用 .msi 安装包仿冒交易所客户端在目标主机中运行远控木马。



coinbase

Engineering Manager, Product Security

We're Coinbase. We're the world's most trusted way to join the crypto revolution, serving more than 89 million accounts in more than 100 countries.

Our mission is to increase economic freedom around the world, and we couldn't do this without hiring the best people. We're a group of hard-working overachievers who are deeply focused on building the future of finance and Web 3.0 for our users across the globe, whether they're trading, storing, staking or using crypto. Know those people who always lead the group project? That's us.

There are a few things we look for across all hires we make at Coinbase, regardless of role or team. First, we look for candidates who will thrive in a culture like ours, where we default to trust, embrace feedback, and disrupt ourselves. Second, we expect all employees to commit to our mission-focused approach to our work. Finally, we seek people who are excited to learn about and live crypto, because those are the folks who enjoy the intense moments in our sprint and recharge work culture. We're a remote-first company looking to hire the absolute best talent all over the world.

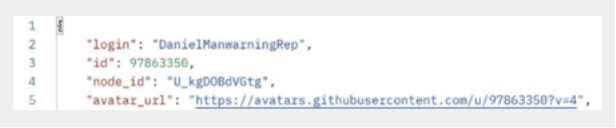
Ready to #LiveCrypto? Who you are:

You've got positive energy. You're optimistic about the future and determined to get there.

You're never tired of learning. You want to be a pro in bleeding edge tech like DeFi, NFTs, DAOs, and Web 3.0.

You appreciate direct communication. You're both an active communicator and an eager listener - because let's face it, you can't have one without the other. You're cool with candid feedback and see every setback as an opportunity to grow.

拉撒路针对 MacOS 的诱饵文件



```
{
  "login": "DanielManwarningRep",
  "id": 97863350,
  "node_id": "U_kgDOBdVGtg",
  "avatar_url": "https://avatars.githubusercontent.com/u/97863350?v=4",
```

拉撒路组织使用 Github 作为 C2

2. Kimsuky

Kimsuky 是疑似具备朝鲜政府背景的 APT 组织，该组织长期针对韩国政府、军工、新闻、医疗、金融等机构进行攻击活动，经常以政府相关热点事件为诱饵进行定向攻击，窃取高价值情报是其主要攻击目的。

在今年该组织曾以“金正恩执政 10 年共歌和 2022 年朝鲜局势展望”、“·韩国核武装相关专家在线坐舰会”、“kima- 2020-04-4 新政府外交安保展望”、“2022 年亚洲领袖会议”的议程、“酬金请求的形式和澳大利亚外交官的简历”等相关主题为诱饵针对韩国地区的媒体和智库人员进行攻击，且部分诱饵文档为该地区常用的 HWP 格式，具有非常明显的针对性。

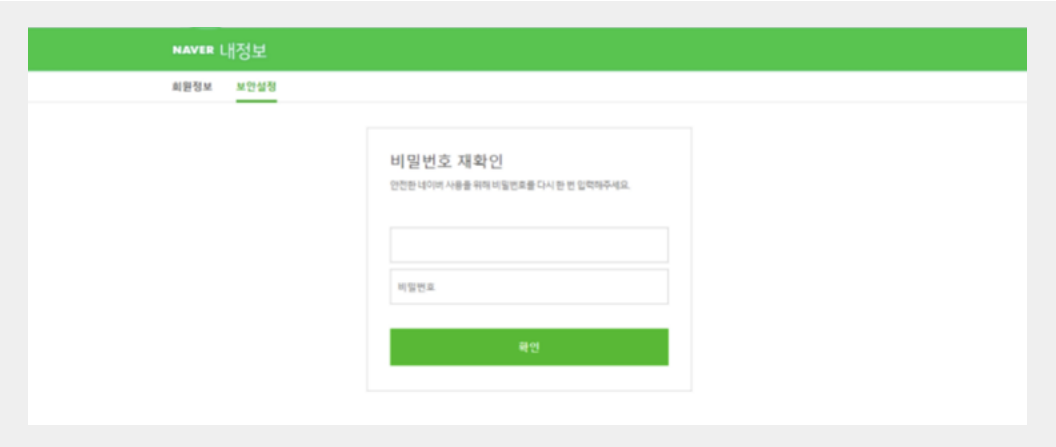
2022년 ALC 회계

[사례비 지급을 위한 개인정보 기입 요청서]

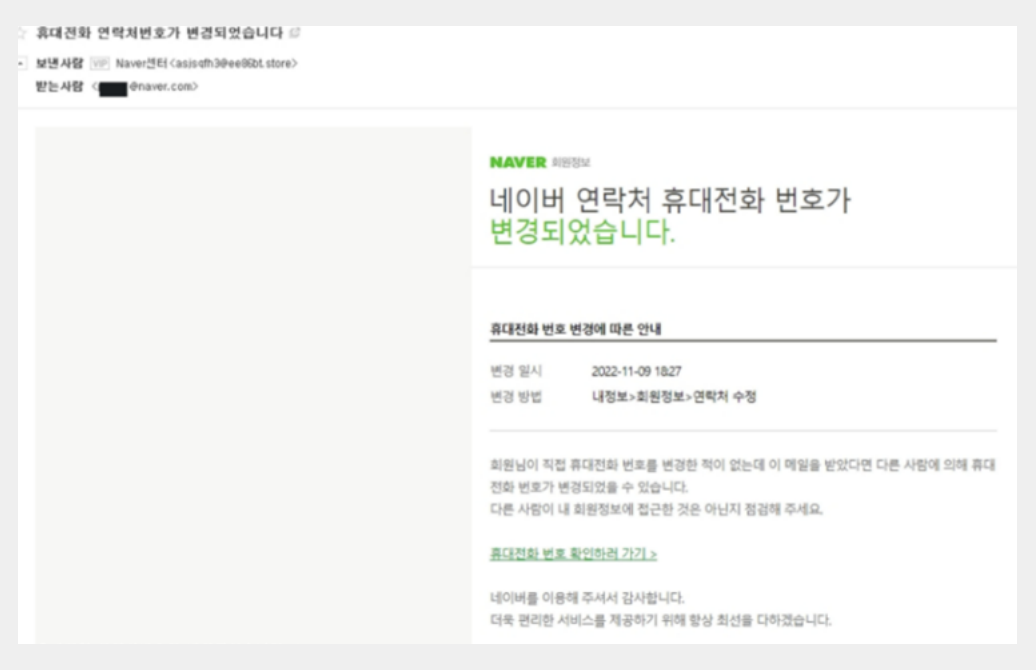
이름	
주민등록번호	
주소	
연락처	
은행명	
계좌번호	
예금주 주소	

在钓鱼网站方面，Kimsuky 通过注册大量仿冒域名对外发起钓鱼攻击，主要使用的顶级域名多为 n-e.k、p-e.kr、r-e.kr、o-r.kr、kro.k，基础设施复用的情况较为普遍。受害者收到的钓鱼邮件通常会包含一个链接，该链接将受害者带到第一阶段的 C2 服务器，该服务器在传递恶意文档之前检查并验证一些参数，如果访问者与目标列表不匹配，则会向他们提供一份无害的文件或弹出报错信息，否则受害者的 ip 地址将作为参数传递给第二阶段的服务器。根据卡巴斯基披露的信息，受害者大多为韩国的政治家、外交官、大学教授和记者。

例 1：钓鱼站点仿冒韩国 naver 网站登陆页面。



例 2：仿冒 naver 中心向用户发送钓鱼邮件，欺骗用户登录凭据，在某些钓鱼链接中会下载恶意 apk 文件用于语音网络钓鱼。



此外，Kimsuky 还在多次攻击活动中使用 blogspot 搭建博客站点并托管恶意载荷，为了逃避检测以及避免被溯源归因。

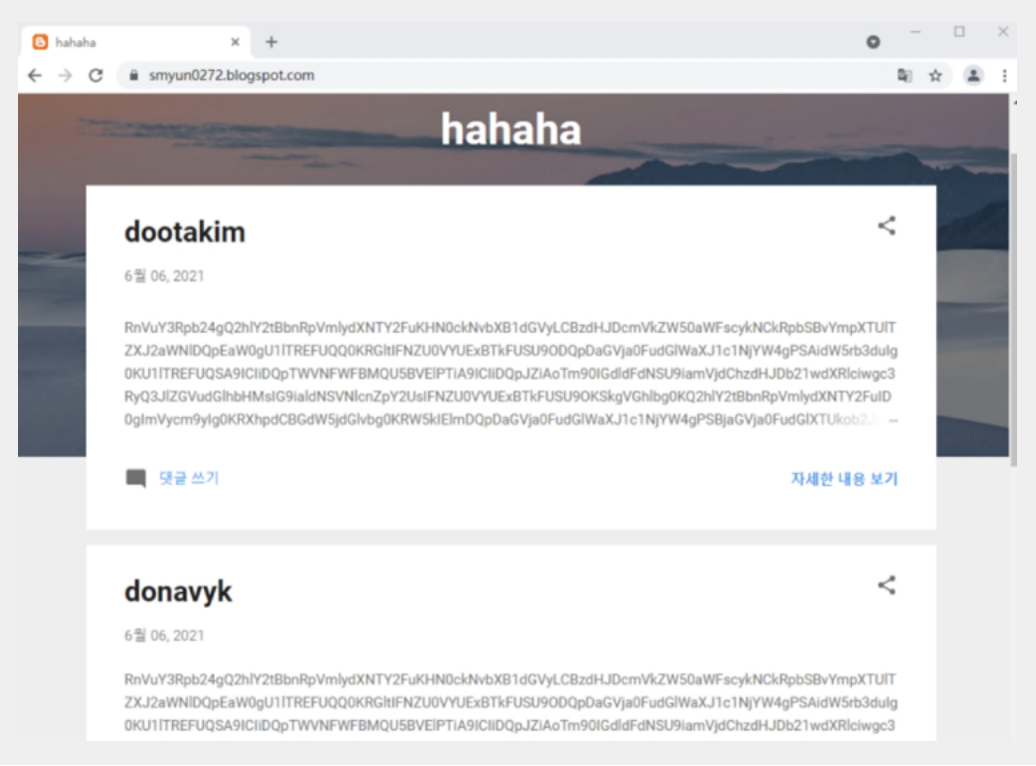


图 Kimsuky 用于托管恶意载荷的博客站点

在后门投递方面，Kimsuky 通过专属安装程序安装（installer_sk5621.com.co.exe）从攻击者的服务器下载以 Gzip 文件形式压缩的 Gold Dragon，将其解压缩为“以 [随机 4 个数字] 的形式”，安装程序还会添加新的注册表项，为恶意软件有效负载建立持久化，通过 rundll32.exe、powershell.exe、iexplore.exe 或 svchost.exe 等系统程序执行。在 Kimsuky 最新的活动中还出现使用 xRAT 对韩国实体进行有针对性的攻击，也使用相同的投递方式和持久化技术。

恶意程序持久化

Kimsuky 组织作为境外 APT 组织，一直保持着很高的活跃程度，其对热点事件特别是政府相关事件保持很高的关注度，该组织在攻击过程中体现出轻量化、多阶段脚本载荷的特点，善于使用各种反取证和反分析技术，近些年 Kimsuky 致力于新的工具开发以及历史工具的迭代更新，使用多种漏洞针对特定机构进行定向攻击，积极参与相关情报收集活动，让半岛地区的网络安全态势变得愈发复杂。

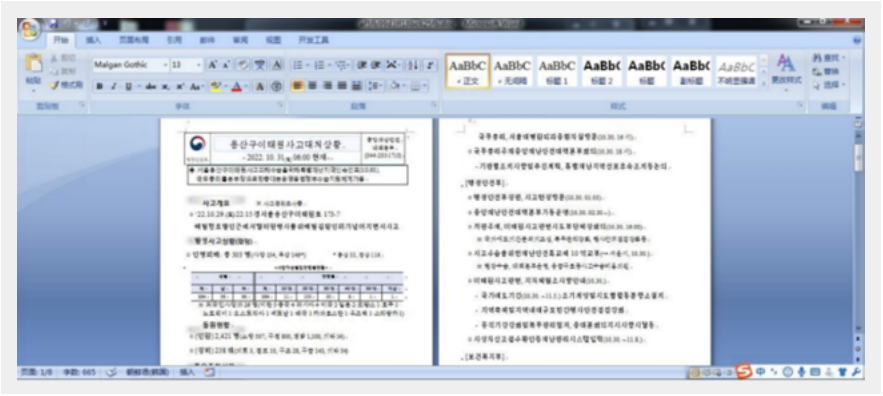
3. Group123

Group123 又 称 APT37、InkySquid、ScarCruft、Ricochet Chollima 等，其至少从 2012 年以来一直活跃，该组织以监视与朝鲜有关的个人而闻名，例如记者、叛逃者、人权活动家、外交官、政府雇员等，该组织试图攻击这些目标来获取机密信息。与公司单位不同的是，这些目标通常没有足够的安全工具来防御和响应高度熟练的监视攻击。

Group123 的部署复杂而多样，前期通常使用鱼叉式钓鱼邮件方式向目标投递携带恶意宏的诱饵文档，一旦用户启用文档的宏代码便会执行恶意代码。在执行时 powershell 脚本启动并打开一个诱饵文档以分散注意力，同时在后台解码第二个脚本。第二个脚本下载并执行后门程序 Goldbackdoor，用以接受远程命令并窃取数据。

除此，还有利用远程模版注入技巧窃取账号密码的手法，例如在今年 11 月份捕捉到该组织利用话题“首尔龙山梨泰院事故”针对韩国发起鱼叉式钓鱼攻击，诱导用户输入凭据：

在目标人员输入凭据后，将凭据发送到“https://ms-xxxxxxx.com:443/templates-xxx-word/download?id=TYV6YAYWOPEKI61Y”，随后下载富文本文档并展示给受害人员，根据公开的信息，Group123 还在上述攻击中的后续阶段使用了针对 Internet Explorer 浏览器的 CVE-2022-41128 漏洞。



根据以往观察到的活动，该组织通常使用支持键盘记录、剪贴板监控、窃取浏览器隐私信息、上传文件、下载 / 执行进一步有效载荷的后门程序，例如 ROKRAT，BLUELIGHT。这些后门程序滥用云存储服务，特别是 Google Drive 来进行 C&C 通信。

另外值得一提的是，研究人员在今年披露了 Group123 组织使用的一个新后门，并将其命名为 Dolphin，该后门具有广泛的间谍功能，具备包括监控驱动器、便携式设备以及文件窃取、键盘记录、屏幕截图以及从浏览器窃取凭据的功能，研究人员已经观察到多个版本的 Dolphin，这说明攻击者不断的改进后门功能并试图逃避检测。

Group123 善于使用云服务进行命令和控制，使得基于网络的检测变得更加困难，且使用 Ruby 和 Python 等脚本语言，巧妙的用来混淆实际的恶意软件，这些技术可以有效的加载恶意软件以逃避检测，可以预见的是，在未来的时间里 Group123 使用的攻击组件将会持续迭代更新。

4. 绿斑

“绿斑”组织是疑似具备台湾地区政治背景且长期针对大陆境内目标的 APT 组织，根据微步情报局监测发现，其网络攻击活动涉及的行业包括政府、国防军工、航空航天、国家智库、医疗疫苗、高新科研、能源、贸易等领域。虽然整体攻击手法较为单一，但涉及到的攻击目标中基本事关国家安全、稳健发展的职能或研究单位 / 部门，具备极高的国家战略价值。

“绿斑”的攻击人员在初期会针对其攻击目标大范围采集邮箱登陆凭证信息，然后将采集到的登录凭证信息进行高价值行业和对象筛选，用于后期的高信誉鱼叉式钓鱼攻击。在相关的攻击中，“绿斑”会根据攻击目标定位的精准度、对象需求和切合度等评估投放钓鱼内容，旨在窃取邮箱账密和进行情报收集。

在今年的攻击活动中，“绿斑”“曾以与科研相关的可持续发展的亚洲与世界 2022 年度报告”、“2022 一带一路暨金砖大赛之金融科技综合能力赛项选拔赛的通知”和“基金评议通知－面上项目－请于 10 月 11 日前提交”等主题为诱饵，仿冒高校邮箱登陆页面针对中国大陆高校进行定向攻击；还以“加快广东省制造业数字化转型研究”、“二十大代表选举名册”等主题的诱饵文件，仿冒腾讯和 163 邮箱的登陆页面针对科研机构和政府单位发起钓鱼攻击。

向筛选到的高价值目标发送钓鱼邮件：

诱导受害者修改密码以获取新密码：

随着绿斑组织的钓鱼手法迭代更新，除了仿冒攻击对象的官方登陆平台与网易云邮箱、qq 中转站、新浪邮箱进行钓鱼攻击外，今年还发现绿斑组织在 url 方面也有了变化，在钓鱼域名后新增了 uri，只有拼接正确的 uri 才能打开钓鱼链接。

1、没有 uri 的钓鱼链接

绿斑使用了一贯的钓鱼链接，钓鱼页面仿照真实的网站进行部署，向目标群体发送带有钓鱼链接的邮件，当用户成功输入用户名和密码之后将数据发送到本地的“xxx.php”进行保存（如：“.copy.php”、“login.php”、“login2.php”等），随后跳转到正常网站或下载无毒文档。下面是部分案例：

国家无线电检测中心：

2、有 uri 的钓鱼链接

以闽台乡建乡创融合为话题发起钓鱼攻击：

从目前检测到的攻击情报上分析判断，台湾地区情报机构无论目的是采集邮箱情报信息还是投放窃密木马，都是依托钓鱼邮件方式将采集邮箱信息的钓鱼链接投送到攻击目标。

在微步情报局今年捕获到的”绿斑”钓鱼链接中有 54.6% 没有具备明显的定向性， 55.4% 的钓鱼链接中根据行业进行划分，攻击范围从地域或行业领域上划分广泛，攻击对象排名首位的是高校，占比 24.4%，其次是军工单位，占比为 17.0%。

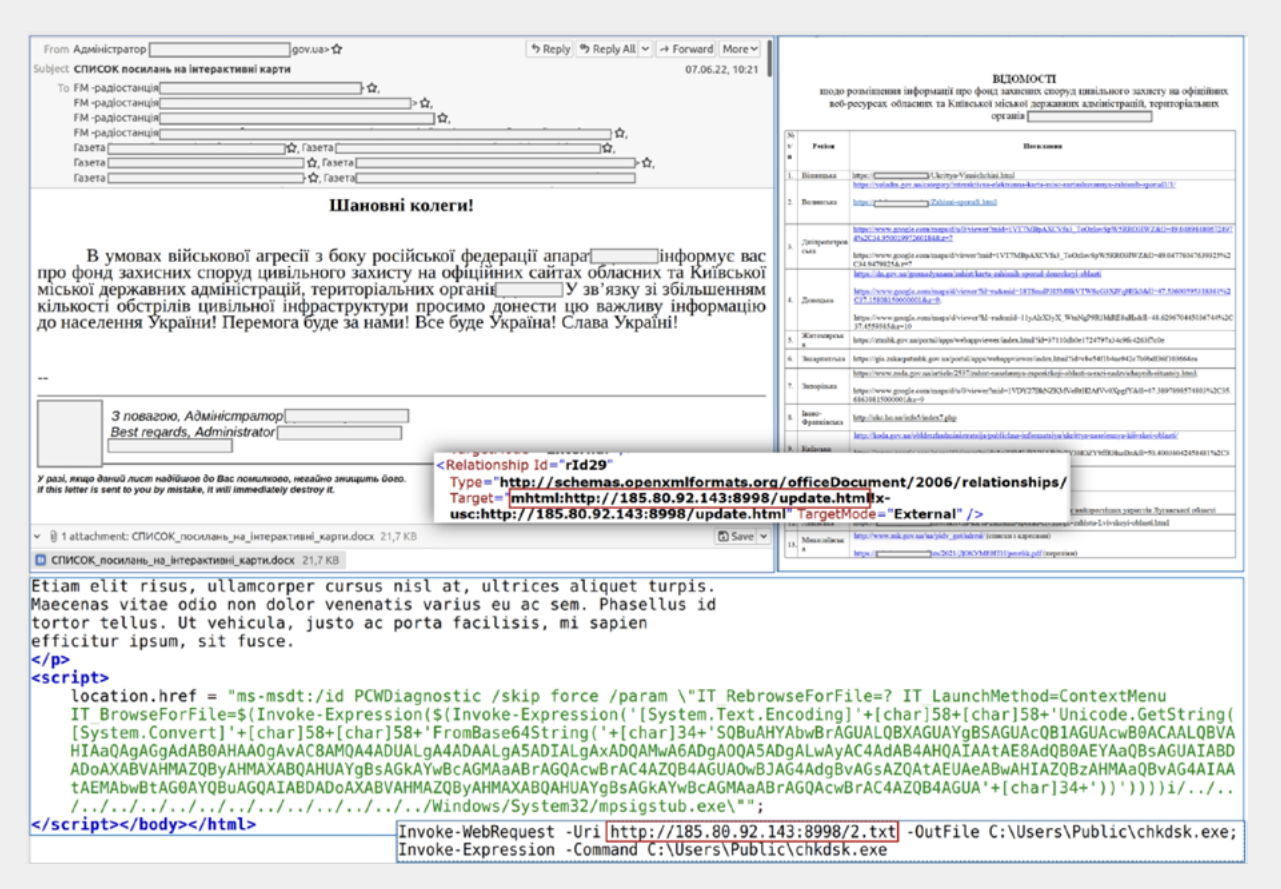
东欧

2022 年，在俄乌战争背景加持下，俄语系 APT 组织频繁发起各类网络攻击活动。较往年攻击活动而言，2022 年俄语系 APT 组织攻击目标更加专注、攻击手法及目的更趋近于网络战属性。以 SandWorm、APT28、APT29、Turla、Gamaredon、SaintBear 为代表的俄语系 APT 组织攻击目标主要集中在战争敌对国乌克兰以及政治立场敌对的各北约成员国，在对乌攻击活动中，诸如数据擦除器、ICS 工控系统定制木马等特种武器的使用均有别于传统 APT 攻击事件体现出用于打击报复目标网络系统的军事目的。此外，从捕获披露的各攻击事件来看，俄语系 APT 组织逐渐青睐于使用 CobaltStrike、BruteRatel 等成熟的红队渗透工具，基于此类工具开展高频次的网络间谍活动。

1. SandWorm

SandWorm 是一个疑似具有俄罗斯总参部 GRU 情报局旗下 74455 部队背景的 APT 组织，该组织最早于 2009 年开始活跃，主要攻击目标为北约国家的政府、军工、能源等机构，具备工控系统、IOT 设备等多系统的网络攻击能力。从 2019 年开始，该组织一度低调隐匿，直到 2022 年俄乌战争开始，SandWorm 才重新回归网络攻击战场。

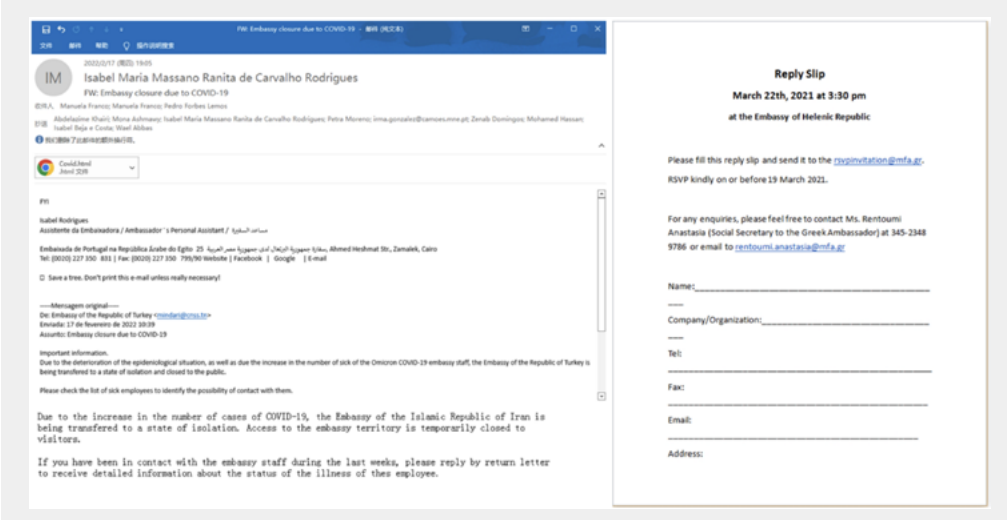
据国内外安全机构披露，大众广为关注的 Hermetic Wiper、FoxBlade Wiper、CaddyWiper、Industroyer2 等系列特种网络战武器均出自 SandWorm 组织。在对乌特定目标攻击活动中，当 SandWorm 渗入目标系统即会释放此类武器库木马，通过覆写目标主机磁盘系统或精准操控目标工控系统最终对目标主机实现不可逆的攻击破坏。SandWorm 是一支极具代表性的基于网络通道执行军事打击任务的 APT 组织。



2. APT29

APT29，疑似归属于俄罗斯联邦对外情报局（SVR），2015 年由 FireEye 披露，最早活动时间可追溯至 2008 年。其攻击目标覆盖全球较多地区和国家，主要攻击目标为包含美国、英国等在内的北约成员国以及欧洲地域邻近国家，具体攻击行业目标为政府实体、科研机构、智库、军工单位、高技术企业、教育机构、医疗机构、通信基础设施供应商等。

2022 年，APT29 对希腊、土耳其等国家政府部门发起多次鱼叉邮件攻击，攻击者习惯使用 html 走私技术投递 ISO 或 IMG 类攻击载荷，攻击载荷多为打包的白利用套件，最终内存加载 CobaltStrike 或 BruteRatelC4 渗透木马实现初步落地侦察目的。

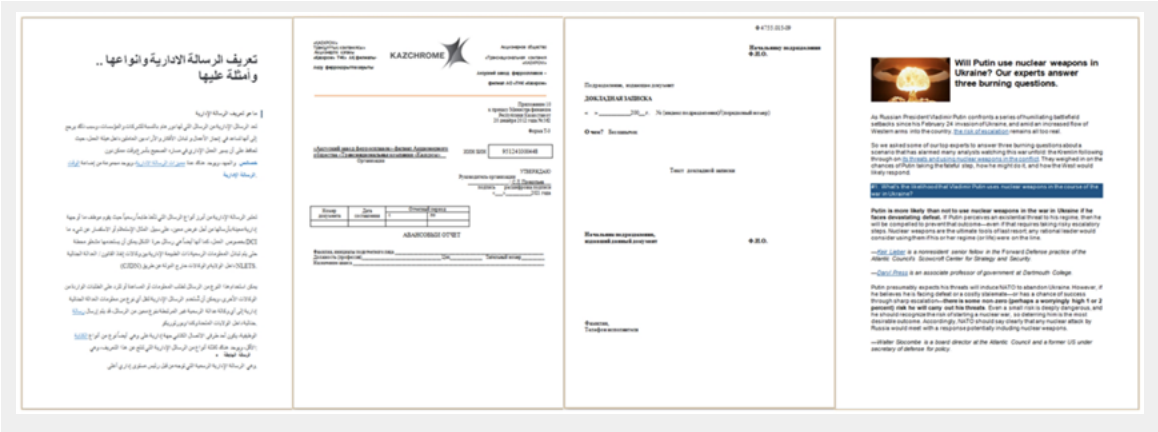


此外，2022 年曝光的 APT29 后渗透攻击组件 MagicWeb 可针对性绕过 AD FS 服务器并窃用高权限令牌实施后续恶意渗透行为。

3. APT28

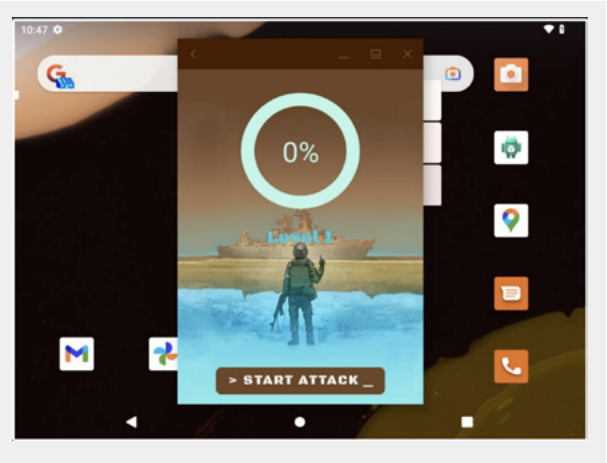
APT28 疑似具备俄罗斯背景，至少自 2004 年开始活跃至今。其攻击目标基本与 APT29、Turla 重合，侧重于发动政治情报间谍攻击活动。

较 2021 年而言，APT28 攻击活动有所收敛。2022 年，APT28 对战争敌对国乌克兰以及巴勒斯坦等地缘国家发起多次鱼叉邮件攻击，攻击者开始使用攻击失陷站点作为 C&C 服务器。在 2022 年的攻击活动中，APT28 还投入一款使用 .Net 开发名为 DocumentSaver 的窃密木马组件，使用前期窃取的邮箱作为 C&C 回传收集的中马侧主机的浏览器 cookie、登录凭据等敏感信息。



4. Turla

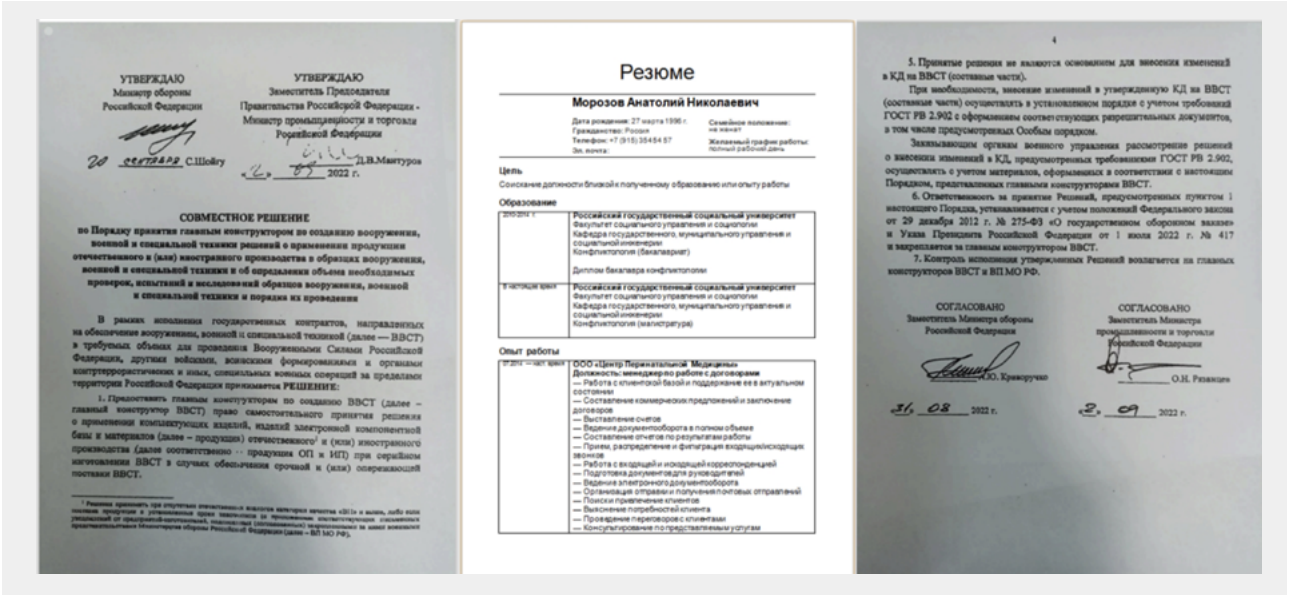
Turla，也被称为 Snake，Venomous Bear、WhiteBear Waterbug、Uroboros 等，是一个疑似具有俄罗斯政府背景的 APT 组织，该组织疑似归属于俄罗斯联邦安全局 FSB，最早活动时间约为 2004 年。自活动至今，Turla 组织发起的攻击活动中的受害者涉及地域已超过 45 个国家，其攻击目标包括政府机构、大使馆、国际组织、军队、高等教育机构、科研机构、制药公司等等。其最终攻击目的为情报刺探，通过一系列网络间谍活动窃取目标单位敏感情报信息。



2022 年，Turla 组织对奥地利经济商会、北约电子学习平台以及波罗的海国防学院等东欧实体机构开展网络间谍活动。攻击者投入使用的钓鱼资产域名刻意模仿目标机构官方域名。此外，2022 年，安全机构首次披露 Turla 使用 CyberAzov、StopWar 等 Android 端间谍程序，移动端木马用于攻击乌克兰军队窃取军事情报。

5. Gamaredon

Gamaredon 是一个疑似具有俄罗斯背景的 APT 组织，至少自 2013 年以来一直活跃，其攻击目标主要为以乌克兰为主的俄罗斯欧洲地域邻国的政府机构。2022 年，在俄乌战争背景下，Gamaredon 继续保持高频次的攻击态势。区别于其他俄语系 APT 组织，Gamaredon 攻击方式单一且攻击能力较为一般，均为大批量的鱼叉邮件攻击，攻击者常使用 lnk、sfx 自解压类型的攻击载荷，初始落地攻击木马多为简单下载器或 VNC 远控工具。


УТВЕРЖДАЮ
Министр обороны
Российской Федерации

УТВЕРЖДАЮ
Заместитель Председателя
Правительства Российской Федерации -
Министр промышленности и торговли
Российской Федерации

СОВМЕСТНОЕ РЕШЕНИЕ

Резюме

Морозов Анатолий Николаевич

Цель

Образование

Опыт работы

СОГЛАСОВАНО

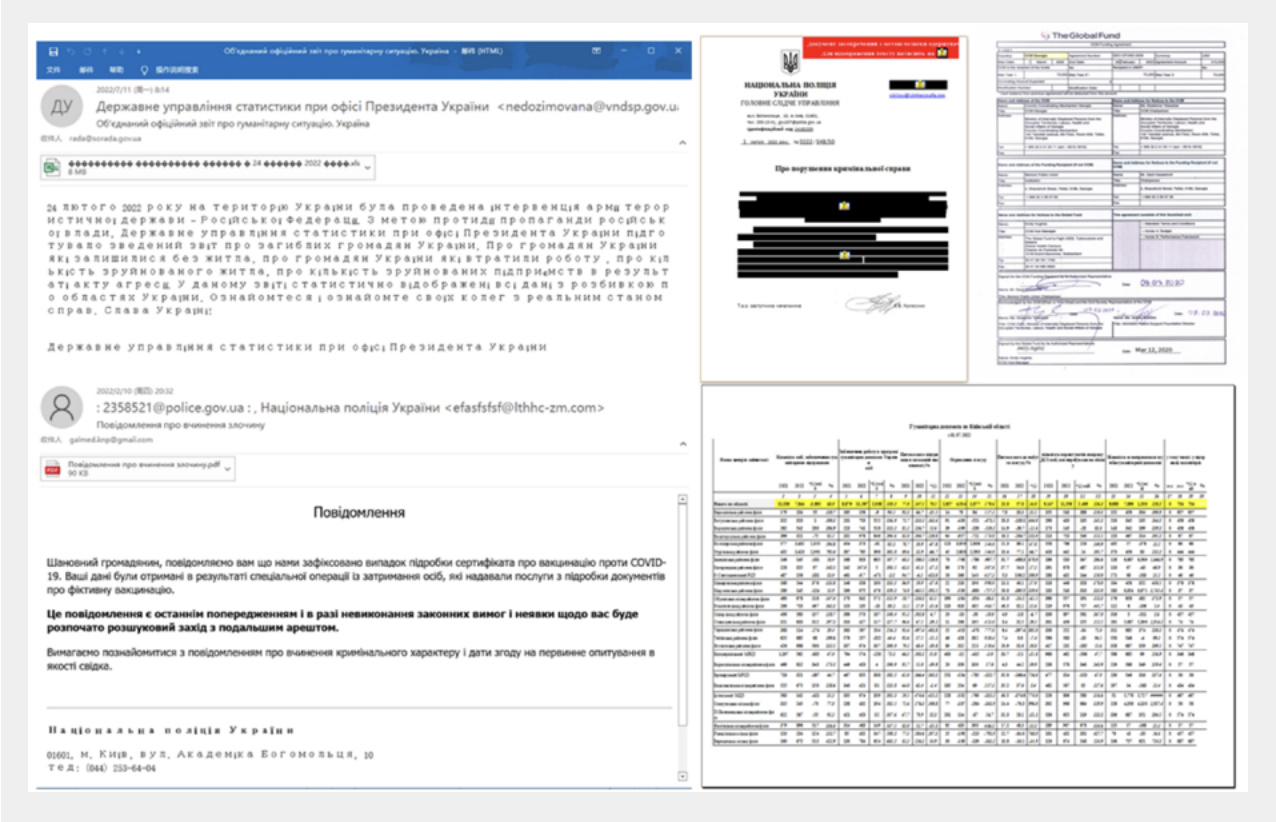
СОГЛАСОВАНО

基于我们掌握的丰富的 Gamaredon 攻击数据，该组织的定位偏向于是一支服务于其他俄语背景 APT 组织的基础分支机构，主要负责开展日常泛散的邮件渗透工作。

6. SaintBear

SaintBear APT 组织，疑似具有俄罗斯背景，2021 年 7 月由微步在线披露，最早活动时间可追溯至 2020 年 7 月。其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。

受俄乌战争影响，2022 年上半年，SaintBear 组织对乌克兰开展了大量鱼叉邮件攻击，攻击目标覆盖政府、军工、银行、教育、能源、乌克兰驻外使馆等各个行业领域。从投入使用的网络武器库来看，SaintBear 开发并使用 Go Elephant 框架木马插件，在部分网络间谍活动中，SaintBear 还投入使用了 CobaltStrike 渗透工具。



中东

近年来，中东地区的高层互访与首脑峰会不断增多，表明不同国家之间的外交活动越来越频繁。以色列与一些阿拉伯国家之间的建交，被视为中东局势缓和的重要标志。但是，这种缓和只是表面现象，并不意味着真正的稳定。美国与伊朗之间深层次的矛盾仍然存在，伊核谈判也迟迟未能取得实质性进展。尽管中东地区的局势表面上看起来有所缓和，但实际上这只是各方出于利益驱动而集体行动的结果。只有当各方完全放弃意识形态斗争和地缘政治对抗，才能为中东地区建立长久的和平基础。然而，这一过程将是艰难而漫长的。因此，中东局势很可能会愈加极化和脆弱，所以今年中东网络攻击活动仍然频繁，攻击方式和武器库也层出不穷，例如 APT35、双尾蝎、APT34、APT33 和 Muddywater 等所熟悉的中东 APT 组织。

1. APT35

APT35 是疑似伊朗国家支持的 APT 组织，又名 Charming Kitten、TA453 或 Phosphorus，已经活跃了近 10 年，以欧洲、中东、美国和其他国家 / 地区的能源、政府和技术部门的组织为目标，曾涉嫌参与干涉美国总统大选、针对北美和中东的组织官员的网络攻击活动。在披露核弹级漏洞 Log4j 仅四天，就被研究人员发现 APT35 使用 Log4j 漏洞分化新的攻击模块，这也不是 APT35 第一次使用漏洞进行攻击，在去年曾披露过 APT35 使用 Exchange 漏洞和 Fortinet 漏洞进行攻击，使用 bitlocker 加密网络设备，今年 APT35 依旧使用更多漏洞组合进行攻击，在漏洞攻击成功后，利用恶意样本在失陷服务器上创建新的用户账户，使用 RDP 访问，释放相关脚本下载反向代理工具 FRPC 修改版，通过配置信息连接到攻击者服务器，并收集本地服务器和域控信息，采集登录存储凭据等。通过我们观察到的视野发现，今年 APT35 的攻击目标更为广泛，采用广撒网式漏洞攻击，包括部分国内服务器也遭受到 APT35 的攻击。

2. 双尾蝎

双尾蝎（APT-C-23）组织至少 2016 年 5 月起活跃至今，长期对巴勒斯坦教育机构、军事机构等重要领域展开有组织、有计划、有针对性的网络间谍活动，背后的攻击者疑似具备中东背景。攻击活动中至少涉及 Windows 与 Android 双平台，投递的诱饵主要伪装成文档、播放器、聊天软件以及一些特定领域常用软件，通过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。今年双尾蝎组织升级了相关武器库，并且依旧在 Windows 和 Android 双平台活跃，值得一提的是，以往双尾蝎的攻击活动似乎都是针对中东讲阿拉伯语的人群，但今年被发现针对以色列人进行新攻击活动，目标人员包括政府、军事和紧急服务工作的以色列个人。攻击者使用新恶意软件 Barbie 和 BarbWire Windows 后门和 VolatileVenom Android 变种升级版进行攻击，通过建立运营虚假的 Facebook 个人账号，这些账号大多数使用虚假的女性身份个人资料和关注喜欢一些以色列人熟知的 Facebook 群组、网站和政客等。在获取受害者信任后，会由 Facebook 转移到 WhatsApp，并诱导受害者下载色情 App 或者软件，实际上为相关平台木马后门。

06

附录

团队简介
微步情报局

Team Introduction

微步情报局，即微步在线研究响应团队，负责微步在线安全分析与安全服务业务，主要研究内容包括威胁情报自动化研发、高级 APT 组织 & 黑产研究与追踪、恶意代码与自动化分析技术、重大事件应急响应等。

微步情报局由精通木马分析与取证技术、Web 攻击技术、溯源技术、大数据、AI 等安全技术的资深专家组成，并通过自动化情报生产系统、云沙箱、黑客画像系统、威胁狩猎系统、追踪溯源系统、威胁感知系统、大数据关联知识图谱等自主研发的系统，对微步在线每天新增的百万级样本文件、千万级 URL、PDNS、Whois 数据进行实时的自动化分析、同源分析及大数据关联分析。微步情报局自设立以来，累计率先发现了包括数十个境外高级 APT 组织针对我国关键基础设施和金融、能源、政府、高科技等行业的定向攻击行动，协助数百家各个行业头部客户处置了肆虐全球的 WannaCry 勒索事件、BlackTech 定向攻击我国证券和高科技事件、海莲花长期定向攻击我国海事 / 高科技 / 金融的攻击活动、OldFox 定向攻击全国上百家手机行业相关企业的事件。

关于微步

About ThreatBook

微步成立于 2015 年，是数字时代网络安全技术创新型企业，专注于精准、高效、智能的网络威胁发现和响应，开创并引领中国威胁情报行业的发展，提供“云 + 流量 + 端点”全方位威胁发现和响应产品及服务，帮助客户建立全生命周期的威胁监控体系和安全响应能力。

公司多次入选全球网络安全 500 强，是 2017-2021 年唯一连续四次入选 Gartner《全球威胁情报市场指南》的中国公司，并获“红鲱鱼亚洲 100 强”称号，2021 年获评国家级专精特新“小巨人”企业，2022 年获评沙利文《中国威胁情报市场报告》领导者象限增长指数第 1 名，并成为 Gartner《托管检测和响应服务市场指南》中国入选企业。

多次入选全球权威榜单

- 《威胁情报市场指南》中国唯一**连续四次入选**企业（Gartner，2017，2019-2021）
- 《**托管检测和响应服务**市场指南》中国入选企业（Gartner，2022）
- 中国安全运营推荐厂商（Gartner，2022）
- 《中国威胁情报市场报告》**领导者象限增长指数第1名**（沙利文，2022）
- 亚洲**100强**（红鲱鱼，2019）
- 全球网络安全**500强**（Cybersecurity Ventures，2017-2019）

屡获国家级资质及荣誉

- 国家级专精特新“**小巨人**”企业
- CCIA中国网安产业竞争力**50强**
- 中标国家某中心网络安全标准项目
- 工信部网络安全技术应用试点示范项目**网络安全威胁认定先进单位**
- 国家信息安全漏洞库（CNNVD）**二级技术支撑单位**
- 国家网络与信息安全信息通报机制技术支持单位

参与多项国家标准制定

- 《GB／T 34960.5-2018 数据治理规范》
- 《GB／T 37988-2019 信息安全技术数据安全能力成熟度模型》
- 《GB／T 28448-2019 信息安全技术网络安全等级保护测评要求》
- 《20210990-T-469 信息安全技术政务网络安全监测平台技术规范》

国家重大项目保障

Cybersecurity Vendor of Major Events

- **2017-2019**
  夏季达沃斯论坛
  特聘网络安保单位
- **2018-2021**
  中国国际进口博览会
  特聘网络安保单位
- **新中国成立70周年庆祝活动**
  网络安全保卫工作
  优秀技术支持单位
- **2020年联合国生物**
  多样性大会
  特聘网络安保单位
- **2022北京冬奥会**
  网络安全保障突出贡献奖

全方位产品和服务体系

Comprehensive Products & Services

“云+流量+端点”全方位威胁发现和响应

重塑新一代网络安全

流量检测

- TDP®威胁感知平台（XC版）
- TDP®威胁感知平台（监管版）
- TDP®威胁感知平台

服 务

- 安全评估类
- 高级情报类
- 安全分析类
- 威胁检测与响应类
- 攻防服务类
- 场景类服务

工 具

- X安全情报社区
- S云沙箱
- 河马SHELLPUB Webshel检测专家
- HFish®威胁诱捕与诱骗系统

威胁情报

- API 威胁情报检测与分析
- TIP 威胁情报管理平台

端点安全

- OneSEC 终端安全管理平台
- OneEDR® 主机威胁检测与响应平台

云上安全

- OneRisk 攻击面管理平台
- TDP 威胁感知平台（云版、虚拟化版）

安全边界

- OneSIG 安全情报网关
- OneDNS® 互联网安全接入服务

微步安全云

漏洞研究 | 威胁情报 | 高级威胁追踪 | 网络空间测绘 | 攻防研究

终端 | 服务器 | 虚拟机 | 数据中心 | 分支 | 公有云 | 私有云

让安全没有边界

微步在线

邮箱：contactus@threatbook.cn

电话：400-030-1051

北京：北京市海淀区苏州街49-3盈智大厦

上海：上海市杨浦区大连路588-688号宝地广场B座11层04

深圳：深圳市南山区科技南十二路曙光大厦701室

广州：广州市天河区体育东路116号财富广场东塔2401A

武汉：湖北省武汉市江夏区区高新大道438号宜科中心园区2栋12层1203

成都：成都市高新区吉泰五路118号3栋10层2号

南京：南京市江宁区东山街道金源路2号绿地之窗商务广场D1幢1206室