“伏特台风”

—— 美国情报机构针对美国国会和纳税人的合谋欺诈行动

〔**内容摘要：**根据美方发布的及其他公开技术信息分析，“伏特台风”黑客组织具有“中国政府支持背景”证据不足。相反，“伏特台风”与勒索病毒等网络犯罪团伙关联程度更为明显；美网络安全机构在向美国会申请预算的关键时间点发布相关虚假信息旨在申请预算拨款，微软等相关网络安全企业也借机获得美政府大额合同；美政府抹黑中国形象旨在遏制和打压中国发展；“伏特台风”的真相是美国把网络攻击溯源当成政治游戏，当成打压中国的工具，当成为自身谋取经济利益的抓手，也彻底暴露了美“歇斯底里”和“无底线”的对华政策，以及美国政客、高官和企业家勾连腐败的真相。〕

一、引言

北京时间2024年2月1日零时（美国东部时间1月31日12时），美国国会众议院中国问题特别委员会在华盛顿众议院办公楼举行了“中共对美国国土和国家安全的网络威胁”听证会[1]，会议由美国国会众议院中国问题特别委员会主席，共和党人麦克·加拉格尔（Mike Gallgher）主持。美国网络安全机构中的“四大金刚”负责人参加会议并接受了国会议员的质询，包括时任美国网络司令部司令兼美国国家安全局（NSA）局长中曾根（Paul Nakasong），美国国土安全部下属网络安全与基础设施安全局（CISA）局长简·伊斯特利

[1] http://selectcommitteeontheccp.house.gov/committee-activity/hearings/hearing-notice-ccp-cyber-threat-american-homeland-and-national-security

（Jen Easterly），美国联邦调查局（FBI）局长克里斯托弗·雷（Christopher Wray）和美国国家网络总监办公室（ONCD）主任哈里·库克（Harry Coker,Jr）。此次会议上，麦克·加拉格尔一开场就声称，2023 年 5 月被美国微软公司披露的名为“伏特台风”（Volt Typhoon）且所谓“具有中国政府支持背景”的黑客组织对美国关键基础设施发动了网络攻击并试图进一步实施破坏，给美国国家安全造成严重威胁。随后，四位接受质询的高官进一步“添油加醋”，把中国描绘成随时可以通过网络攻击颠覆美国政权甚至通过破坏关键基础设施将美国民众置之于死地的“恶魔”。尽管我们早已对美国政府“贼喊捉贼”的低级表演习以为常，但如此大的阵仗也不多见，不禁让人好奇，“伏特台风”是何方神圣？其与中国政府的关联证据何在？既然去年 5 月就已经披露了攻击活动，美国政客为何时隔 8 个月旧事重提，再次向中国发难？本文将就上述问题进行探究，以求廓清真相、正本清源、以正视听。

二、“伏特台风”简史

2023 年 5 月 24 日，“五眼联盟”国家（美国、英国、加拿大、澳大利亚、新西兰）的网络安全主管部门联合发布了名为《中华人民共和国国家支持背景的黑客正在使用逃避检测技术》的预警通报[2]，预警通报称名为“伏特台风”的黑

[2] https://media.defense.gov/2023/May/24/2003229517/-1/-1/0/CSA_PRC_State_Sponsored_Cyber_Living_off_the_Land_v1.1.PDF

客组织针对美国关键基础设施单位实施了网络间谍活动。该预警通报直接引用了微软公司于同日发布的《“伏特台风”组织利用逃避检测技术针对美国关键基础设施发动攻击》[3]的技术分析报告和溯源分析结果。微软公司技术分析报告中将攻击者按照微软公司的内部规则命名为“伏特台风”，并直接指出该组织是所谓“总部位于中国且由国家政权支持的网络攻击行为主体”。该技术报告重点介绍了该组织的攻击技战术，即：首先通过入侵小型商用或家用路由器、防火墙等网络设备进入目标内部网络，然后采用“Living_off_the_Land”逃避检测技术进一步渗透窃密。“Living_off_the_Land”直译为“离地生活”，网络安全行业又称其为“无文件攻击”或“少文件攻击”，在这种攻击技战术中，攻击者主要使用非定制化恶意程序或攻击工具，如：受害主机系统中原生内置的系统工具和第三方开源攻击工具等，攻击者将恶意代码以多种方式直接加载或注入到内存进程中直接执行，完全不在本地磁盘中留存文件或仅留存很少且无可溯源特征的文件，以实现逃避检测的目的。虽然“五眼联盟”的预警通报和微软公司的技术报告详细介绍了攻击者的技战术特征和感染指标（IoC）等，但没有给出具体的溯源分析过程，而是直接给“伏特台风”打上了“中国政府支持背景黑客组织”的标签。该预警通报一经发布就被路透社、华尔街日报、纽

[3] https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/

约时报等各大主流新闻媒体大量转载，纽约时报还报道称美国情报机构在2023年2月发现关岛和美国部分地区的电信网络遭到入侵，并将上述攻击与相关预警通报联系起来[4]。

时间来到2023年12月13日，美国流明科技（Lumen Technologies, Inc）公司（美国仅次于AT&T和Verizon的第三大固网电信公司）旗下网络安全研究机构“黑莲花实验室”（BLACKLOTUS Labs）发布了一篇名为《在开放的防火墙上烧烤路由器：KV僵尸网络调查》（Routers Roasting On An Open Firewall）的报告[5]，报告中再次提及“伏特台风”组织，并认为该组织在攻击活动中利用被命名为“KV僵尸网络”（KV-Botnet）的物联网僵尸网络作为跳板，其溯源理由是KV僵尸网络在2022年7月使用了美国网件公司（NetGear）ProSAFE防火墙作为网络中继节点并与位于关岛的IP地址存在关联，而根据微软公司的报告，“伏特台风”利用包括美国网件公司在内的多个品牌小型商用和家用网络设备作为跳板攻击了关岛的电信运营商。美国流明科技公司的报告一经发布，再次引发美国政府的高度关注，特别是在2024年1月31日，美国政府突然密集采取了一系列动作，美国司法部网站公开发布名为《美国政府破坏了中华人民共和国用来掩盖针对美国关键基础设施实施网络攻击的僵尸网络》

[4] https://www.nytimes.com/2023/05/24/us/politics/china-guam-malware-cyber-microsoft.html?searchResultPosition=1

[5] https://blog.lumen.com/routers-roasting-on-an-open-firewall-the-kv-botnet-investigation/

的通报[6]，通报称 2023 年 12 月，经法院授权，美国司法部开展专项行动，成功从美国全国数百台路由器上清除了 KV 僵尸网络程序。同日，美国网络安全与基础设施安全局（CISA）和联邦调查局联合发布关于《改善小型商用和家用网络设备网络安全状况的指导意见》[7]，声称鉴于包括中国政府支持的“伏特台风”组织在内的黑客组织正在针对小型商用和家用网络设备进行攻击，美国政府敦促所有相关设备生产商应加强网络安全设计并及时修复漏洞。而就在同一天，美国国会众议院中国问题特别委员会在华盛顿众议院办公楼举行了“中共对美国国土和国家安全的网络威胁”听证会（详见本文第一部分）。

这里补充一点，“伏特台风”组织的命名是源自微软公司 2023 年 4 月公布的该公司黑客组织命名规则[8]，其中将以所谓具有“中国政府支持背景”的黑客组织冠以“台风”作为姓氏，其他国家也被分配了相应的姓氏[9]，如图 1 所示。当然其中不会出现“五眼联盟”国家。

---

[6] https://www.justice.gov/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical

[7] https://www.cisa.gov/resources-tools/resources/secure-design-alert-security-design-improvements-soho-device-manufacturers?utm_source=FBI&utm_medium=press_release&utm_campaign=SbD_SOHO

[8] https://www.microsoft.com/en-us/security/blog/2023/04/18/microsoft-shifts-to-a-new-threat-actor-naming-taxonomy/

[9] https://learn.microsoft.com/zh-cn/microsoft-365/security/defender/microsoft-threat-actor-naming?view=o365-worldwide

参与者类别	类型	姓氏
Nation-state	中国 伊朗 黎巴嫩 朝鲜 俄罗斯 韩国 土耳其 越南	台风 沙尘暴 雨 雨夹雪 暴雪 冰雹 灰尘 气旋
出于财务动机	出于财务动机	暴风雨
私营部门攻击性行动者	PSOA	海啸
影响操作	影响操作	洪水
正在开发中的组	正在开发中的组	风暴

图 1 微软公司的黑客组织命名规则（来自微软官方网站）

综合上述情况，我们不难看出，关于“伏特台风”组织以及该组织的归属，美国政府、网络安全企业和新闻媒体的最主要参考依据就是微软公司的技术分析报告和“五眼联盟”发布的联合预警通报。

三、“伏特台风”真的具有国家支持背景吗？

前文提到，“伏特台风”这一名称和归因都源自美国微软公司的技术分析报告和“五眼联盟”发布的联合预警通报，但微软公司并没有给出详细的归因分析过程和根据，而且微软公司在报告中也提到，由于黑客使用了逃避检测技术，给取证和溯源工作带来较大困难。不过，在两份报告的末尾部分都给出了相关攻击活动的技术特征，即 IoC，按照行业惯例，我们可以使用这些技术特征尝试进行溯源分析。

首先，我们对两份报告的技术特征部分给出的样本信息

进行了统计，去除重复项后，总计29个恶意程序样本，如表1所示。

表 1 “伏特台风”相关恶意程序样本

序号	样本 SHA256	来源
1	baeffeb5fdef2f42a752c65c2d2a52e84fb57efc906d981f89dd518c314e231c	微软公司报告
2	b4f7c5e3f14fb57be8b5f020377b993618b6e3532a4e1eb1eae9976d4130cc74	微软公司报告
3	4b0c4170601d6e922cf23b1caf096bba2fade3dfcf92f0ab895a5f0b9a310349	微软公司报告
4	c0fc29a52ec3202f71f6378d9f7f9a8a3a10eb19acb8765152d758aded98c76d	微软公司报告
5	d6ab36cb58c6c8c3527e788fc9239d8dcc97468b6999cf9ccd8a815c8b4a80af	微软公司报告
6	9dd101caee49c692e5df193b236f8d52a07a2030eed9bd858ed3aaccb406401a	微软公司报告
7	450437d49a7e5530c6fb04df2e56c3ab1553ada3712fab02bd1eeb1f1adbc267	微软公司报告
8	93ce3b6d2a18829c0212542751b309dacbdc8c1d950611efe2319aa715f3a066	微软公司报告
9	7939f67375e6b14dfa45ec70356e91823d12f28bbd84278992b99e0d2c12ace5	微软公司报告
10	389a497f27e1dd7484325e8e02bbdf656d53d5cf2601514e9b8d8974befddf61	微软公司报告
11	c4b185dbca490a7f93bc96eefb9a597684fdf532d5a04aa4d9b4d4b1552c283b	微软公司报告
12	e453e6efc5a002709057d8648dbe9998a49b9a12291dee390bb61c98a58b6e95	微软公司报告
13	6036390a2c81301a23c9452288e39cb34e577483d121711b6ba6230b29a3c9ff	微软公司报告
14	cd69e8a25a07318b153e01bba74a1ae60f8fc28eb3d56078f448461400baa984	微软公司报告
15	17506c2246551d401c43726bdaec800f8d41595d01311cf38a19140ad32da2f4	微软公司报告
16	8fa3e8fdbaa6ab5a9c44720de4514f19182adc0c9c6001c19cf159b79c0ae9c2	微软公司报告
17	d17317e1d5716b09cee904b8463a203dc6900d78ee2053276cc948e4f41c8295	微软公司报告

序号	样本 SHA256	来源
18	472ccfb865c81704562ea95870f60c08ef00bcd2ca1d7f09352398c05be5d05d	微软公司报告、五眼联盟报告
19	3e9fc13fab3f8d8120bd01604ee50ff65a40121955a4150a6d2c007d34807642	微软公司报告
20	f4dd44bc19c19056794d29151a5b1bb76afd502388622e24c863a8494af147dd	五眼联盟报告
21	ef09b8ff86c276e9b475a6ae6b54f08ed77e09e169f7fc0872eb1d427ee27d31	五眼联盟报告
22	d6ebde42457fe4b2a927ce53fc36f465f0000da931cfab9b79a36083e914ceca	五眼联盟报告
23	66a19f7d2547a8a85cee7a62d0b6114fd31afdee090bd43f36b89470238393d7	五眼联盟报告
24	3c2fe308c0a563e06263bbacf793bbe9b2259d795fcc36b953793a7e499e7f71	五眼联盟报告
25	41e5181b9553bbe33d91ee204fe1d2ca321ac123f9147bb475c0ed32f9488597	五眼联盟报告
26	c7fee7a3ffaf0732f42d89c4399cbff219459ae04a81fc6eff7050d53bd69b99	五眼联盟报告
27	3a9d8bb85fbcfe92bae79d5ab18e4bca9eaf36cea70086e8d1ab85336c83945f	五眼联盟报告
28	fe95a382b4f879830e2666473d662a24b34fccf34b6b3505ee1b62b32adafa15	五眼联盟报告
29	ee8df354503a56c62719656fae71b3502acf9f87951c55ffd955feec90a11484	五眼联盟报告

然后，我们使用美国谷歌公司的 VirusTotal 多引擎病毒文件分析平台[10]（以下简称：VT 平台）对这些样本进行了逐一检索，发现只能查到 13 个样本的信息，而且每个样本都与多个 IP 地址存在关联，以第一个样本为例，检索结果如图 2 所示。

[10] https://www.virustotal.com/

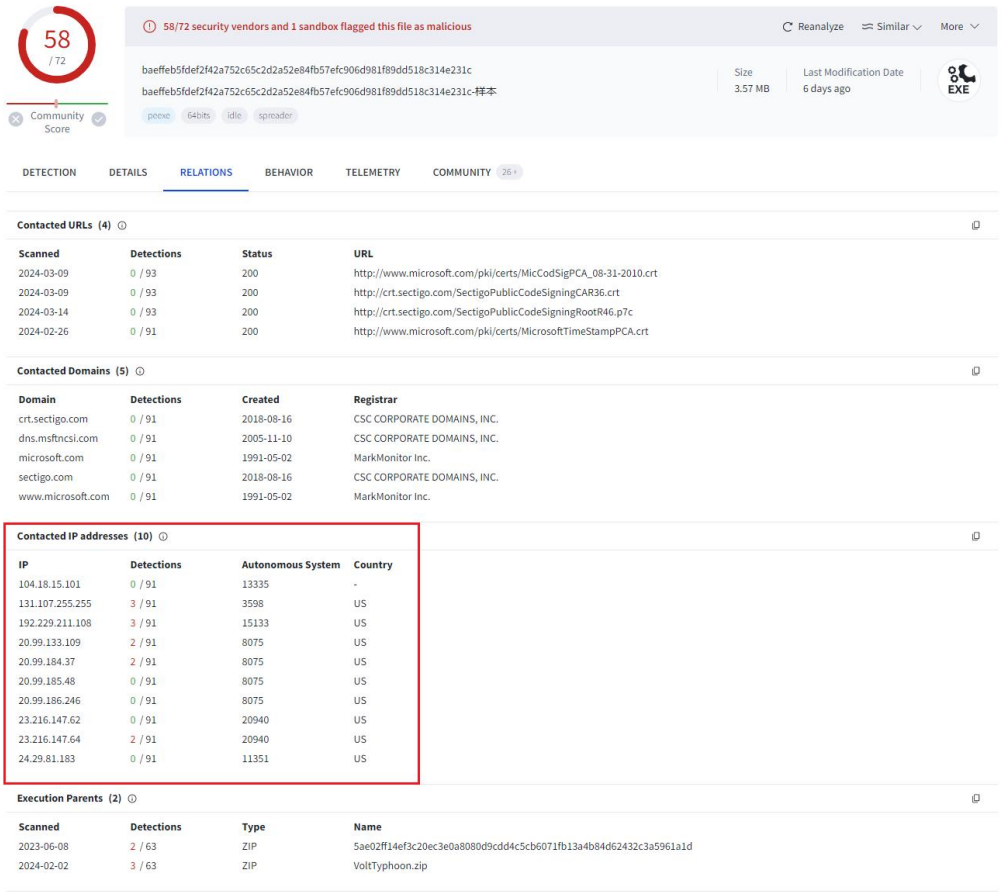


图 2 相关样本 VT 平台检索结果

重复上述过程，我们发现 13 个样本分别与多个 IP 地址存在关联，而且每个 IP 地址都关联多个样本，统计结果如表 2 所示。

表 2 样本关联 IP 地址

序号	关联 IP	SHA-256	来源
1	192.229.211[.]108	baeffeb5fdef2f42a752c65c2d2a52e84fb57efc906d981f89dd518c314e231c	微软公司报告
2		c0fc29a52ec3202f71f6378d9f7f9a8a3a10eb19acb8765152d758aded98c76d	微软公司报告
3		389a497f27e1dd7484325e8e02bbdf656d53d5cf2601514e9b8d8974befddf61	微软公司报告
4		c4b185dbca490a7f93bc96eefb9a597684fdf532d5a04aa4d9b4d4b1552c283b	微软公司报告
5		e453e6efc5a002709057d8648dbe9998a49b9a12291dee390bb61c98a58b6e95	微软公司报告
6		6036390a2c81301a23c9452288e39cb34e577483d121711b6ba6230b29a3c9ff	微软公司报告

序号	关联 IP	SHA-256	来源
7		cd69e8a25a07318b153e01bba74a1ae60f8fc28eb3d56078f448461400baa984	微软公司报告
8		8fa3e8fdbaa6ab5a9c44720de4514f19182adc0c9c6001c19cf159b79c0ae9c2	微软公司报告
9		472ccfb865c81704562ea95870f60c08ef00bcd2ca1d7f09352398c05be5d05d	微软公司报告、五眼联盟报告
10		3e9fc13fab3f8d8120bd01604ee50ff65a40121955a4150a6d2c007d34807642	微软公司报告
11		f4dd44bc19c19056794d29151a5b1bb76afd502388622e24c863a8494af147dd	五眼联盟报告
12		3c2fe308c0a563e06263bbacf793bbe9b2259d795fcc36b953793a7e499e7f71	五眼联盟报告
13		41e5181b9553bbe33d91ee204fe1d2ca321ac123f9147bb475c0ed32f9488597	五眼联盟报告
14	20.99.133[.]109	baeffeb5fdef2f42a752c65c2d2a52e84fb57efc906d981f89dd518c314e231c	微软公司报告
15		c0fc29a52ec3202f71f6378d9f7f9a8a3a10eb19acb8765152d758aded98c76d	微软公司报告
16		389a497f27e1dd7484325e8e02bbdf656d53d5cf2601514e9b8d8974befddf61	微软公司报告
17		c4b185dbca490a7f93bc96eefb9a597684fdf532d5a04aa4d9b4d4b1552c283b	微软公司报告
18		6036390a2c81301a23c9452288e39cb34e577483d121711b6ba6230b29a3c9ff	微软公司报告
19		cd69e8a25a07318b153e01bba74a1ae60f8fc28eb3d56078f448461400baa984	微软公司报告
20		8fa3e8fdbaa6ab5a9c44720de4514f19182adc0c9c6001c19cf159b79c0ae9c2	微软公司报告
21		472ccfb865c81704562ea95870f60c08ef00bcd2ca1d7f09352398c05be5d05d	微软公司报告、五眼联盟报告
22		3e9fc13fab3f8d8120bd01604ee50ff65a40121955a4150a6d2c007d34807642	微软公司报告
23		f4dd44bc19c19056794d29151a5b1bb76afd502388622e24c863a8494af147dd	五眼联盟报告
24		3c2fe308c0a563e06263bbacf793bbe9b2259d795fcc36b953793a7e499e7f71	五眼联盟报告
25		41e5181b9553bbe33d91ee204fe1d2ca321ac123f9147bb475c0ed32f9488597	五眼联盟报告
26	20.99.184[.]37	baeffeb5fdef2f42a752c65c2d2a52e84fb57efc906d981f89dd518c314e231c	微软公司报告

序号	关联 IP	SHA-256	来源
27		c0fc29a52ec3202f71f6378d9f7f9a8a3a10eb19acb8765152d758aded98c76d	微软公司报告
28		389a497f27e1dd7484325e8e02bbdf656d53d5cf2601514e9b8d8974befddf61	微软公司报告
29		c4b185dbca490a7f93bc96eefb9a597684fdf532d5a04aa4d9b4d4b1552c283b	微软公司报告
30		e453e6efc5a002709057d8648dbe9998a49b9a12291dee390bb61c98a58b6e95	微软公司报告
31		6036390a2c81301a23c9452288e39cb34e577483d121711b6ba6230b29a3c9ff	微软公司报告
32		cd69e8a25a07318b153e01bba74a1ae60f8fc28eb3d56078f448461400baa984	微软公司报告
33		8fa3e8fdbaa6ab5a9c44720de4514f19182adc0c9c6001c19cf159b79c0ae9c2	微软公司报告
34		472ccfb865c81704562ea95870f60c08ef00bcd2ca1d7f09352398c05be5d05d	微软公司报告、五眼联盟报告
35		3e9fc13fab3f8d8120bd01604ee50ff65a40121955a4150a6d2c007d34807642	微软公司报告
36		f4dd44bc19c19056794d29151a5b1bb76afd502388622e24c863a8494af147dd	五眼联盟报告
37		3c2fe308c0a563e06263bbacf793bbe9b2259d795fcc36b953793a7e499e7f71	五眼联盟报告
38		41e5181b9553bbe33d91ee204fe1d2ca321ac123f9147bb475c0ed32f9488597	五眼联盟报告
39	23.216.147[.]64	baeffeb5fdef2f42a752c65c2d2a52e84fb57efc906d981f89dd518c314e231c	微软公司报告
40		c4b185dbca490a7f93bc96eefb9a597684fdf532d5a04aa4d9b4d4b1552c283b	微软公司报告
41		e453e6efc5a002709057d8648dbe9998a49b9a12291dee390bb61c98a58b6e95	微软公司报告
42		cd69e8a25a07318b153e01bba74a1ae60f8fc28eb3d56078f448461400baa984	微软公司报告
43		8fa3e8fdbaa6ab5a9c44720de4514f19182adc0c9c6001c19cf159b79c0ae9c2	微软公司报告
44		472ccfb865c81704562ea95870f60c08ef00bcd2ca1d7f09352398c05be5d05d	微软公司报告、五眼联盟报告
45		3e9fc13fab3f8d8120bd01604ee50ff65a40121955a4150a6d2c007d34807642	微软公司报告
46		f4dd44bc19c19056794d29151a5b1bb76afd502388622e24c863a8494af147dd	五眼联盟报告

序号	关联 IP	SHA-256	来源
47		3c2fe308c0a563e06263bbacf793bbe9b2259d795fcc36b953793a7e499e7f71	五眼联盟报告
48		41e5181b9553bbe33d91ee204fe1d2ca321ac123f9147bb475c0ed32f9488597	五眼联盟报告
49	23.216.147[.]76	6036390a2c81301a23c9452288e39cb34e577483d121711b6ba6230b29a3c9ff	微软公司报告
50		cd69e8a25a07318b153e01bba74a1ae60f8fc28eb3d56078f448461400baa984	微软公司报告
51		472ccfb865c81704562ea95870f60c08ef00bcd2ca1d7f09352398c05be5d05d	微软公司报告、五眼联盟报告
52		3e9fc13fab3f8d8120bd01604ee50ff65a40121955a4150a6d2c007d34807642	微软公司报告
53		f4dd44bc19c19056794d29151a5b1bb76afd502388622e24c863a8494af147dd	五眼联盟报告
54		3c2fe308c0a563e06263bbacf793bbe9b2259d795fcc36b953793a7e499e7f71	五眼联盟报告
55		41e5181b9553bbe33d91ee204fe1d2ca321ac123f9147bb475c0ed32f9488597	五眼联盟报告

随后，我们再次利用 VT 平台的威胁情报关联分析工具对上述 5 个较为集中的 IP 地址进行了分析，发现这些 IP 地址与很多的网络攻击事件相关，并且也存在多个 IP 地址与同一攻击事件或网络安全风险存在关联的现象，而其中与上述 5 个 IP 地址都有关联的一个网络攻击事件报告是美国威胁盟（ThreatMon）公司在 2023 年 4 月 11 日发布的《关于“暗黑力量”（Dark Power）勒索病毒团伙研究报告》[11]，如图 3、图 4 所示。

[11] https://threatmon.io/the-rise-of-dark-power-a-close-look-at-the-group-and-their-ransomware/ https://threatmon.io/storage/the-rise-of-dark-power-a-close-look-at-the-group-and-their-ransomware.pdf

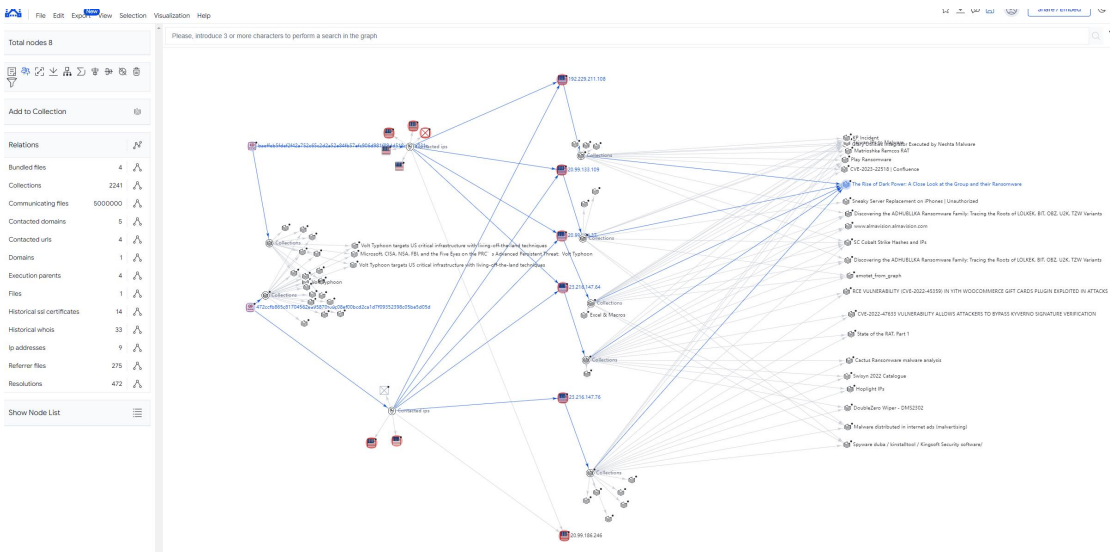


图 3 IP 地址关联关系

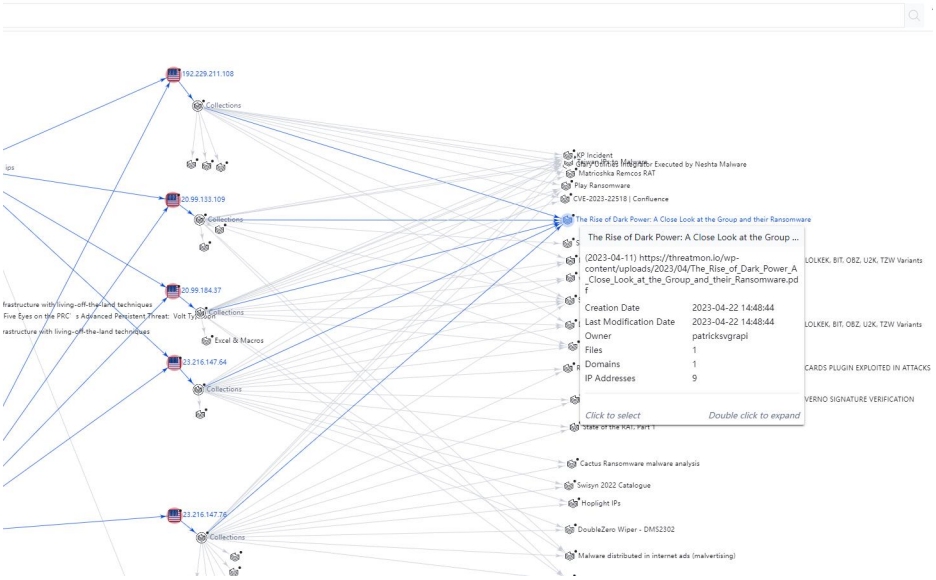
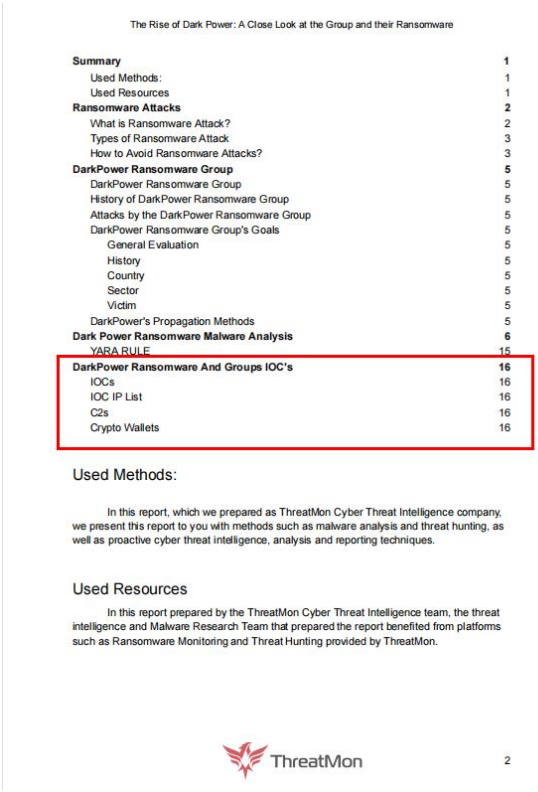


图 4 关联的网络安全事件信息

根据下载链接，我们下载了报告的 PDF 版本，并期望在报告中找到这些 IP 地址。但奇怪的是，虽然在报告的目录部分，我们看到了该报告包含 IoC 的 IP 地址列表在报告第 16 页，然而，16 页作为报告正文的最后一页，并没有这个 IP 地址列表，如图 5 和图 6 所示。



The Rise of Dark Power: A Close Look at the Group and their Ransomware

Summary 1
Used Methods: 1
Used Resources 1
Ransomware Attacks 2
What is Ransomware Attack? 2
Types of Ransomware Attack 3
How to Avoid Ransomware Attacks? 3
DarkPower Ransomware Group 5
DarkPower Ransomware Group 5
History of DarkPower Ransomware Group 5
Attacks by the DarkPower Ransomware Group 5
DarkPower Ransomware Group's Goals 5
General Evaluation 5
History 5
Country 5
Sector 5
Victim 5
DarkPower's Propagation Methods 5
Dark Power Ransomware Malware Analysis 6
YARA RULE 15
DarkPower Ransomware And Groups IOC's 16
IOCs 16
IOC IP List 16
C2s 16
Crypto Wallets 16

Used Methods:

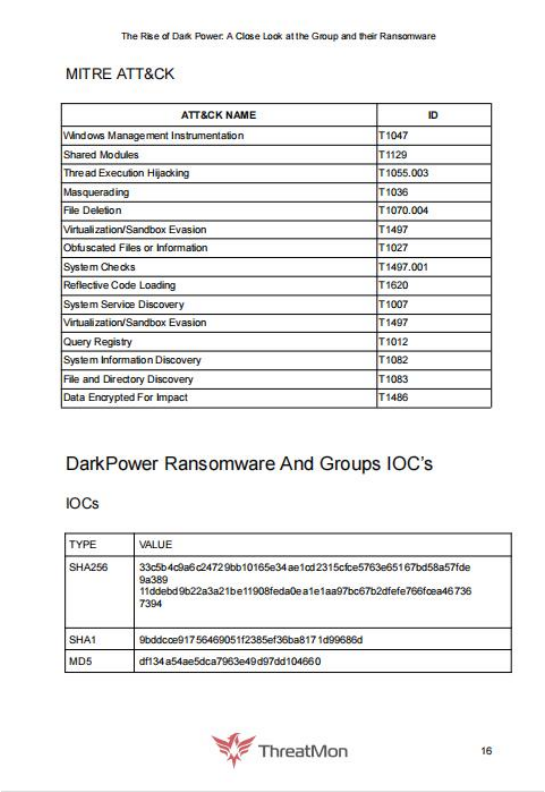
In this report, which we prepared as ThreatMon Cyber Threat Intelligence company, we present this report to you with methods such as malware analysis and threat hunting, as well as proactive cyber threat intelligence, analysis and reporting techniques.

Used Resources

In this report prepared by the ThreatMon Cyber Threat Intelligence team, the threat intelligence and Malware Research Team that prepared the report benefited from platforms such as Ransomware Monitoring and Threat Hunting provided by ThreatMon.

ThreatMon 2

图 5 威胁盟报告的 IoC



The Rise of Dark Power: A Close Look at the Group and their Ransomware

MITRE ATT&CK

ATT&CK NAME	ID
Windows Management Instrumentation	T1047
Shared Modules	T1129
Thread Execution Hijacking	T1055.003
Masquerading	T1036
File Deletion	T1070.004
Virtualization/Sandbox Evasion	T1497
Obfuscated Files or Information	T1027
System Checks	T1497.001
Reflective Code Loading	T1620
System Service Discovery	T1007
Virtualization/Sandbox Evasion	T1497
Query Registry	T1012
System Information Discovery	T1082
File and Directory Discovery	T1083
Data Encrypted For Impact	T1486

DarkPower Ransomware And Groups IOC's

IOCs

TYPE	VALUE
SHA256	33c5b4c9a6c24729bb10165e34ae1cd2315cfce5763e65167bd58a57fde9a389 11ddebd9b22a3a21be11908feda0ea1e1aa97bc67b2dfefe766fcea467367394
SHA1	9bddcce9175646905 1f2385ef36ba8171d99686d
MD5	df134a54ae5dca7963e49d97dd104660

ThreatMon 16

图 6 未找到 IoC 中的 IP 列表

我们起初认为，报告可能存在文核错误，并试图从威胁盟公司的 GitHub 仓库中找到报告中的 IoC 文件，然而，我们虽然在 GitHub 上找到了威胁盟公司的仓库和对应报告的文件夹[12]，但仍然没有找到 IP 地址信息，如图 7 所示。而且上传日期是 2023 年 5 月 8 日，而不是该报告发布的 4 月 11 日或临近的日期。

[12] https://github.com/ThreatMon/ThreatMon-Reports-IOC/commits/main/The-Rise-of-Dark-Power-A-Close-Look-at-the-Group-and-their-Ransomware/IOC.txt

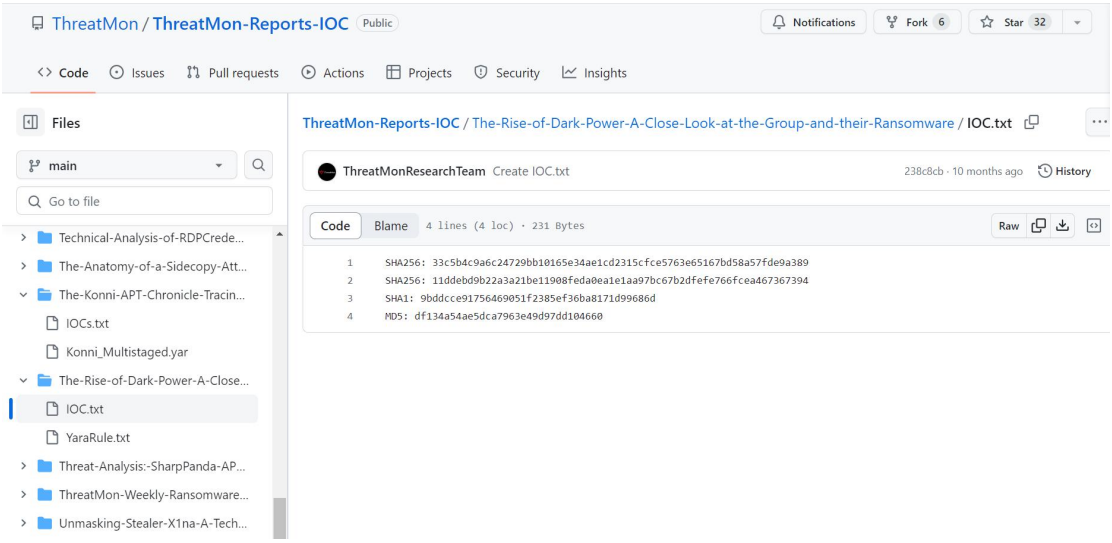


图 7 威胁盟公司 Github 仓库

然而，坚持带来了好运，我们发现，在威胁盟公司 PDF 版本报告的封底其实并非只是一幅图片，移动封底图片后，我们找到了我们想要的 IP 地址列表，而且前文提到的 5 个 IP 地址都在这个列表中。如图 8、图 9 所示。

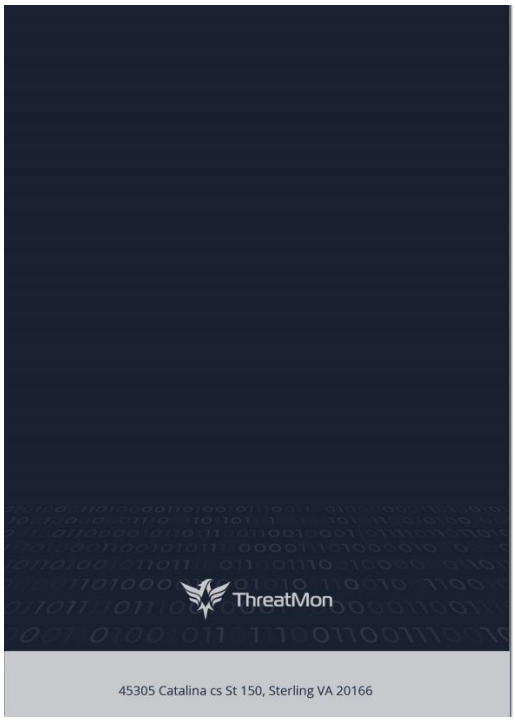


图 8 原威胁盟报告封底

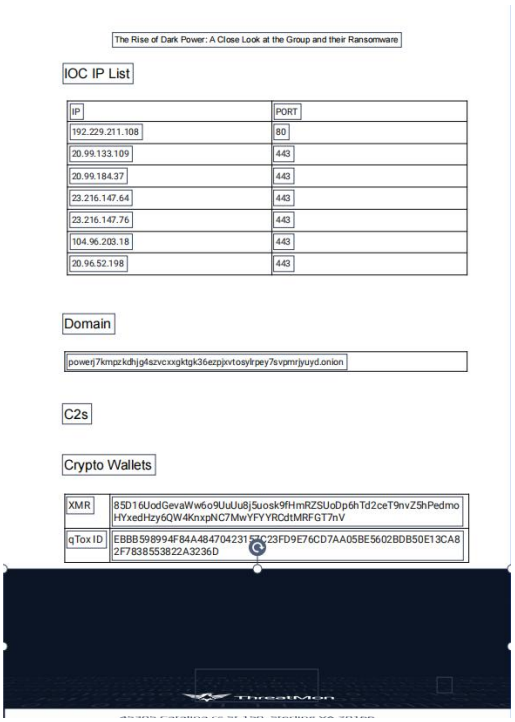


图 9 移动封底图片后威胁盟报告

尽管我们对威胁盟公司的做法感到很疑惑，但还是仔细

研读了这份报告。在报告中，威胁盟公司介绍了一个自称“暗黑力量”的勒索病毒组织，并且据该公司监测，第一次发现该组织攻击活动是在 2023 年 1 月，也就是说该组织很可能在 2023 年以前就已经开始进行攻击活动，而且仅 2023 年 3 月就至少有 10 个以上的全球范围内机构遭到该组织攻击并被勒索。受害机构所在国家包括阿尔及利亚、埃及、捷克、土耳其、以色列、秘鲁、法国、美国等。该组织使用典型的“双重勒索”方式，即：先入侵受害单位的内网，进行数据窃取，窃取到重要数据后，再最后进行加密勒索，同时威胁用户如果不按时缴纳赎金，将在网络上公开泄露受害单位的敏感内部数据。报告中也详细介绍了该组织的攻击技战术，该组织同样也在攻击中部分使用了“离地生活”技术，即使用 Windows 操作系统自带的管理工具（WMI）关闭系统进程，并在攻击结束前对攻击过程中产生的相关系统日志信息进行清理，最后留下一个勒索信告知受害单位，如图 10 所示。

图 10 暗黑力量组织的勒索信

值得注意的是，2023 年 3 月 21 日，据美国记录未来（Recorded Future）公司旗下网络安全媒体“TheRecord.media”报道[13]，关岛最大的电信公司 DOCOMO PACIFIC（日本 NTT DOCOMO 的全资子公司）于 2023 年 3 月 16 日遭到网络攻击并导致服务中断，并指出包括汤加、瓦努阿图等多个太平洋岛国都遭到过勒索病毒组织攻击。DOCOMO PACIFIC 公司也承认了这一事件[14]。

另外，我们还对美国流明科技公司发布的关于 KV 僵尸网络的报告中包含的恶意程序样本和 IP 地址等技术特征进行了检索（使用 VT 平台），但并未找到其与微软公司和“五眼联盟”预警通报中所述技术特征之间的关联关系。

至此，我们对相关报告的恶意程序样本技术特征进行分析后，发现这些样本并没有表现出明确的国家背景黑客组织行为特征，反而与勒索病毒等网络犯罪团伙的关联程度更为明显。在这种情况下，微软公司和“五眼联盟”国家仅凭受害单位和攻击者的攻击技战术这些模糊的归因因素就把“伏特台风”扣上所谓“中国政府黑客”的帽子未免过于牵强，但是我们相信，他们这么做一定有着深层次的原因，接下来就让我们一窥端倪。

四、金钱的味道

回顾以上内容，我们不难发现，2024 年 1 月 31 日对于

[13] https://therecord.media/guam-telecom-cyberattack-restore
[14] https://bettertogether.pr.co/224192-docomo-pacific-responds-to-multiple-service-outage

美国国会、美国政府网络安全主管部门和美国网络安全企业来说是一个重要的时间节点。在同一天，美国国会、美国司法部、美国国土安全部共同针对“伏特台风”打出了一套“组合拳”。为什么选在1月31日这个时间？根据1921年颁布的美国《预算与会计法案》[15]，美国总统必须在每年2月的第一个星期一，也就是今年2月5日前，向国会提交包括联邦政府下一财年预算申请在内的预算报告。这就解释了为什么美国国会众议院中国问题特别委员会在当天举办的听证会演变成了“哭穷大会”。首先，参加听证会的美国国会议员以及美国国家安全局、美国网络安全与基础设施安全局、美国联邦调查局和美国国家网络总监办公室的一把手们大肆鼓吹“中国威胁论”，要求国会在网络安全方面进一步加大人、财、物投入。其次，2024年美国总统大选举世瞩目，共和、民主两党自然都不想在中国问题上“丢选票”，通过公开“讨伐”中国，国会议员们还可以提高自身曝光率，收获不错的政治资本，部分议员甚至叫嚣对中国进行反击，并封禁TikTok。最后，美国网络安全企业当然希望美国联邦政府这个最阔气的“甲方爸爸”的钱包越鼓越好，而且“中国威胁论”也成为这些企业开拓欧美市场最好的营销广告。

最终，在2024年3月11日拜登政府公布的2025财年预算申请文件中[16]，美国联邦政府在民事行政部门和机构的

[15] https://www.govinfo.gov/help/budget#about
[16] https://www.whitehouse.gov/wp-content/uploads/2024/03/budget_fy2025.pdf

网络安全预算达到了创纪录的 130 亿美元，较 2024 财年又提高了 10%。其中，美国网络安全与基础设施安全局预算达到 30 亿美元，较上一年度增加 1.03 亿美元。美国司法部和联邦调查局预算增加了 2500 万美元专门用于“网络和反间谍调查能力”建设。当然，作为坐拥 8500 亿美元总预算的美国国防部的下属单位，美国国家安全局从来不担心预算问题。

另外，我们还观察到一些细节，就在微软公司发布报告的前两个月，也就是 2023 年 3 月 24 日，微软公司获得了美国国防部总额 90 亿美元的联合作战云（JWCC）项目的第一批任务订单[17]，价值约 380 万美元。在美国流明科技公司发布有关 KV 僵尸网络与“伏特台风”存在关联的分析报告的前一个月，2023 年 11 月 7 日，美国流明科技公司刚刚赢得了美国国防信息系统局（DISA）价值 1.1 亿美元的五年期合同订单[18]。

总之，美国政客、高官和企业家因“伏特台风”虚假叙事赚得盆满钵满，而且也达到在国际社会抹黑中国形象、离间中国与盟友关系，遏制中国经济发展的目的，这种卑劣的做法一但被拆穿，将被民众所唾弃！

---

[17] https://defensescoop.com/2023/03/29/defense-department-has-awarded-first-jwcc-cloud-task-order/

[18] https://ir.lumen.com/news/news-details/2023/Lumen-wins-110-million-contract-from-Defense-Information-Systems-Agency/default.aspx

五、结语

我们不得不承认，网络攻击活动的归因分析是国际性难题。网络武器泄露和攻防技术快速扩散导致网络犯罪分子的技术水平显著提高。早在 2016 年，初代物联网僵尸网络 Mirai 就造成美国国内大范围断网，而美国关键基础设施运营单位科洛尼尔管道公司被勒索病毒组织攻击导致美国部分地区进入紧急状态和黑客组织之间的大混战都充分表明了，一些勒索病毒组织和僵尸网络运营者拥有的资源和技术能力已经超过一般国家，甚至已经能够达到网络战水平。同时，勒索病毒组织与僵尸网络运营者早已建立了成熟的地下黑色产业合作模式，在利益的驱使下，这些网络犯罪团伙活动日益猖獗。这些互联网公害是包括中美两国在内的全球各国面临的共同威胁，然而美国政府却搞小圈子、小院高墙，甚至操弄微软等公司开展虚假叙事，把网络攻击溯源当成政治游戏、当成打压中国的工具、当成攫取资本为自身谋利的抓手，也彻底暴露了美“歇斯底里”和“无底线”的对华政策，以及美国政客、高官和企业家勾连腐败的真相，这样只会破坏国际公共网络空间的正常秩序，破坏中美关系，影响美国政府在全球的声誉。引用中国一句谚语：多行不义必自毙！

最后，感谢 360 公司在溯源分析过程中提供的支持与协助！

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