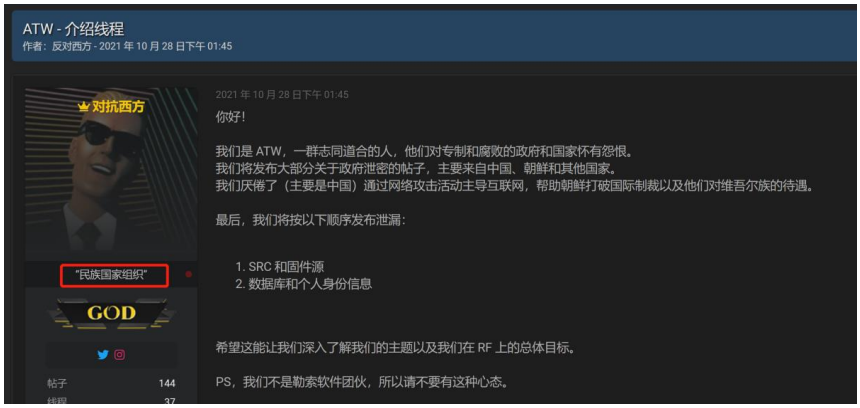
斩断危害中国数据安全的魔手
——揭秘疯狂对华实施数据窃取的 ATW 组织

2021 年 10 月以来，一自称 AgainstTheWest（下称“ATW”）的黑客组织，将中国作为主要攻击目标，疯狂实施网络攻击、数据窃取和披露炒作活动，对我国的网络安全、数据安全构成严重危害。ATW 组织究竟什么来头？我们该如何应对？让我们来庖丁解牛，见招拆招。

ATW 组织及其主要攻击活动

ATW 组织成立于 2021 年 6 月，10 月开始在“阵列论坛”（RaidForums）上大肆活动。虽然将帐号个性签名设置为“民族国家组织”，但实际上，这是一个以欧洲、北美地区从事程序员、网络工程师等职业的人员自发组织成立的松散网络组织。



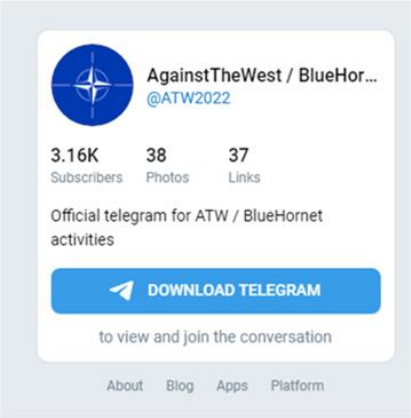
ATW 组织自我介绍

ATW 组织自成立伊始，便表达了鲜明的反华立场，公开称“将主要针对中国、朝鲜和其他国家发布政府数据泄密帖子”，还专门发布过一篇题为“ATW-对华战争”的帖子，赤裸裸地支持

“台独”、鼓噪“港独”、炒作新疆“人权问题”。

ATW 组织发布的“ATW-对华战争”帖

2021 年 10 月，ATW 组织开始频繁活动，不断在电报群组（https://t.me/s/ATW2022，Email:AgainstTheWest@riseup.net，备份 Email:apt49@riseup.net）、推特（@_AgainstTheWest，https://mobile.twitter.com/_AgainstTheWest）、Breadched（账号：AgainstTheWest）等境外社交平台开设新账号，扩大宣传途径，并表现出较明显的亲美西方政治倾向，多次声明“攻击目标是俄罗斯、白俄罗斯和中国、伊朗、朝鲜”、“愿意与美国、欧盟政府共享所有文件”、“愿受雇于相关机构”。

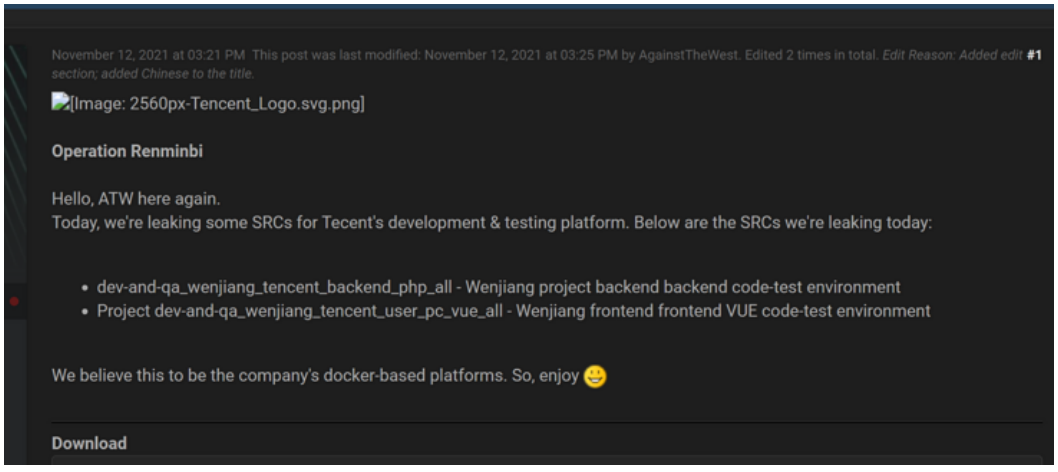


ATW 组织群组账号

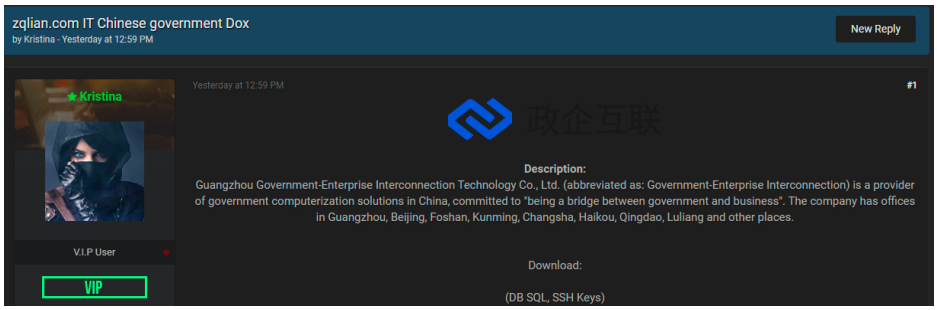
ATW 组织推特账号

据不完全统计，自 2021 年以来，ATW 组织披露涉我重要信息系统源代码、数据库等敏感信息 70 余次，宣称涉及文化和旅游部、海南省政府、山西省司法厅、南方航空公司、广州地铁等 100 余家单位的 300 余个信息系统。实际上，所谓泄露的源代码主要是中小型软件开发企业所研发的测试项目代码文件，不包含数据信息。但 ATW 组织为了博取关注，极尽歪曲解读、夸大其词之能事，动辄使用“大规模监控”、“侵犯人权”、“侵犯隐私”等美西方惯用的“标签”，意图凸显攻击目标和所窃数据重要性，以至于看起来，一个比一个吓人。

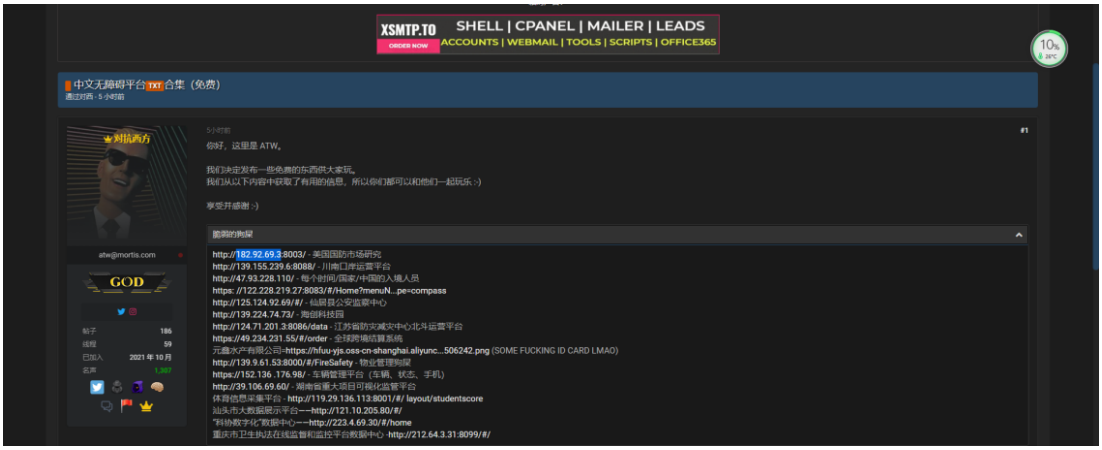
- 2021 年 10 月 14 日，ATW 在“阵列论坛”（RaidForums）发布题为“人民币行动（Operation Renminbi）”的帖子，称“出售中国人民银行相关软件项目源代码”。



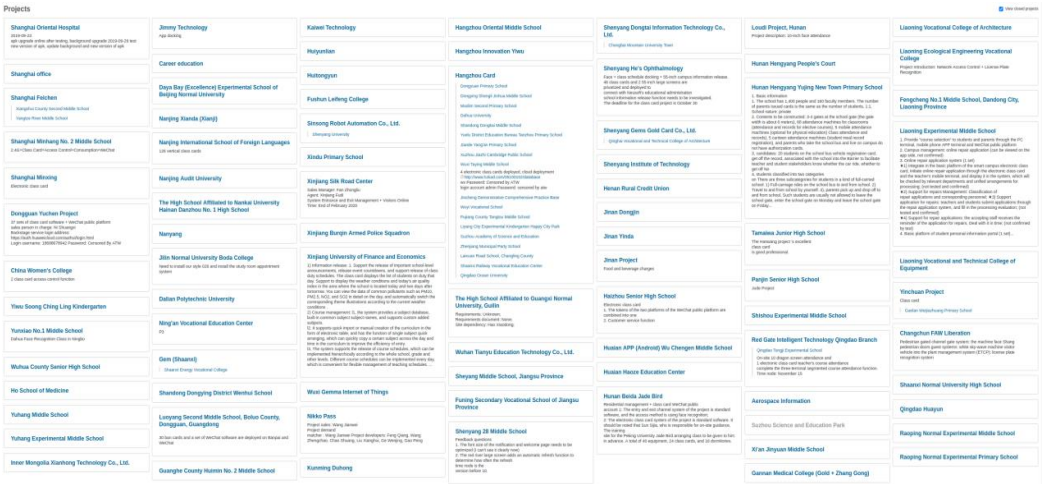
- 2021 年 11 月 2 日，ATW 组织在“阵列论坛”发布信息，称“广州政企互联科技有限公司已被其攻破”，并提供了数据库和 SSH 密钥的下载方式。



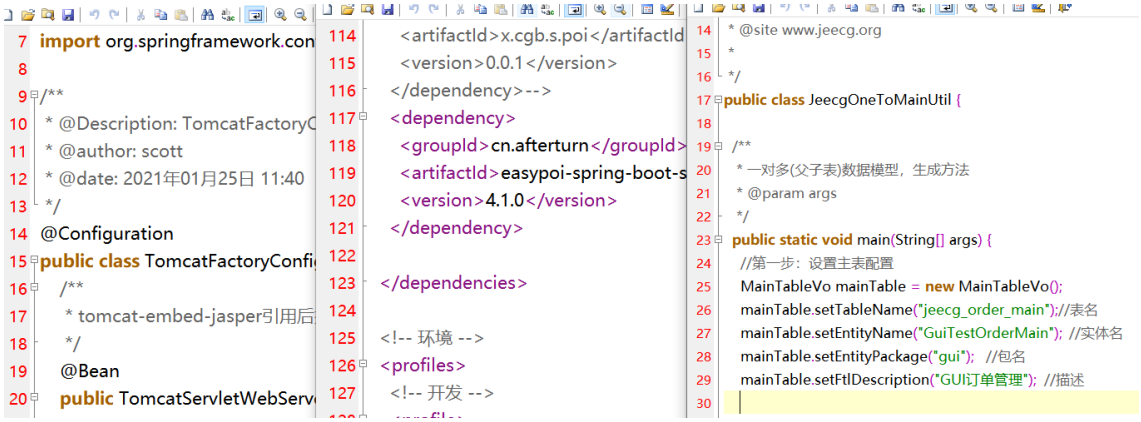
- 2021 年 11 月 24 日，ATW 组织发布了 16 个政府网站大数据系统存在漏洞情况，涉及北京、浙江、四川、重庆、广东、江苏、湖北、湖南等地。



- 2022 年 1 月 7 日，ATW 组织声称出售“中国大量政府、非政府组织、机构和公司数据，待售数据涉及 102 家中国实体单位”。

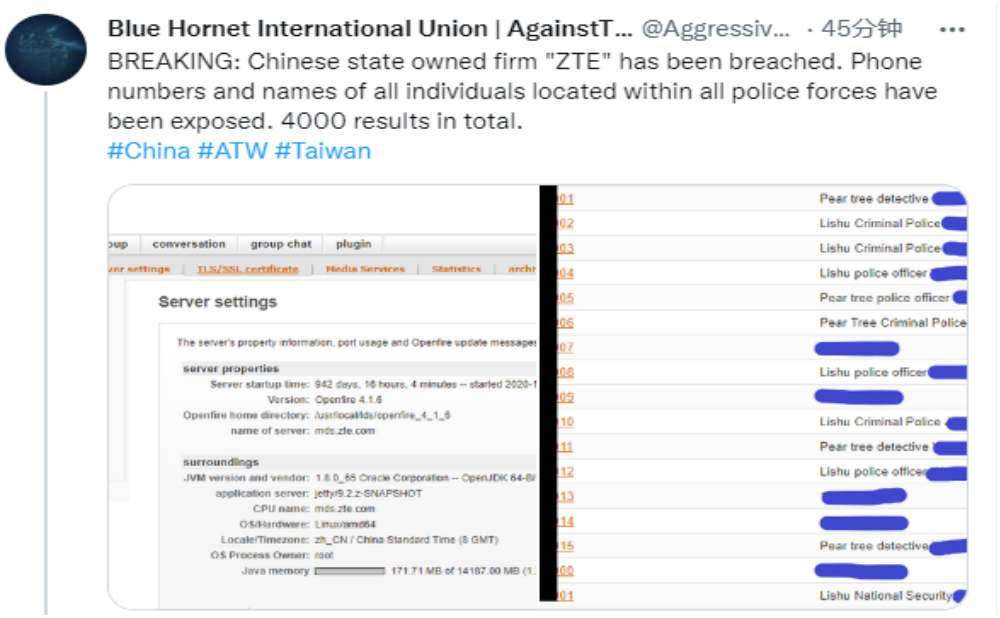


- 2022 年 3 月 4 日，ATW 组织宣布解散，但 3 月 5 日又宣布经费充足再次上线。
- 2022 年 3 月 6 日，ATW 在电报群组中发布消息称“攻破了中央汇金投资公司，窃取了大量数据”，并提供了数据的下载链接。
- 2022 年 3 月 28 日，宣称“广发银行已被攻破”，发布“整个后端源代码、maven 版本”等数据。

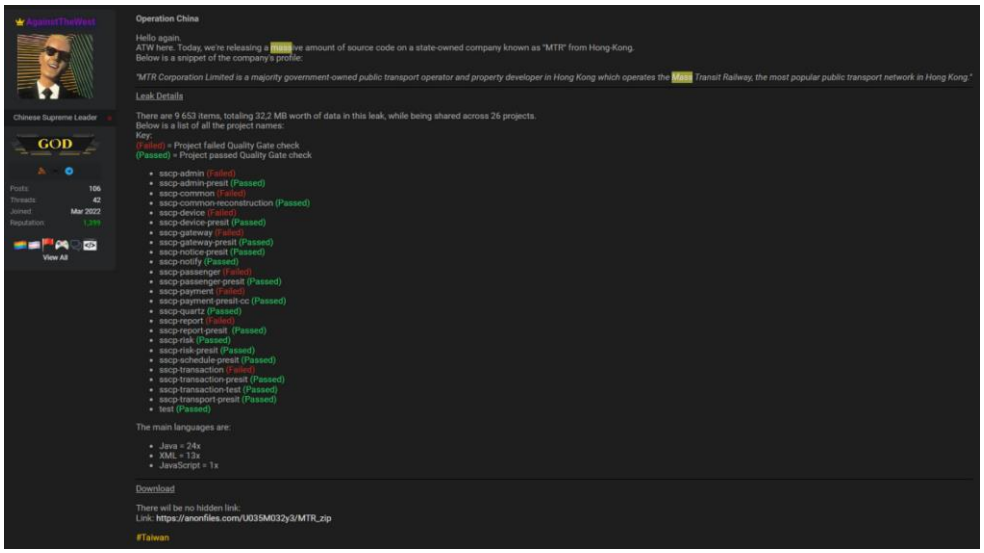


- 2022 年 4 月 5 日，ATW 组织发布“中国各省市共计 48 家医院信息系统源代码”。

- 2022 年 8 月 12 日，ATW 组织在推特发布数据售卖帖，称其从中兴通讯公司服务器获取了 4000 条警察人员的电话号码和姓名数据。



- 2022 年 8 月 16 日，ATW 组织通过 Breached 黑客论坛公布港铁系统源码文件，内容涉及香港铁路公司的交易、排程等 26 个系统项目代码。

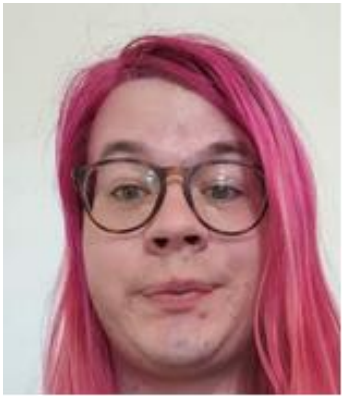


ATW 组织主要成员

技术团队长期跟踪发现，ATW 组织平日活跃成员 6 名，多从事程序员、网络工程师相关职业，主要位于瑞士、法国、波兰、加拿大等国。

梳理该组织成员活动时段发现，其休息时间为北京时间 15 时至 19 时，工作时间集中在北京时间凌晨 3 时至 13 时，对应零时区和东 1 时区的西欧国家。其中，2 名骨干成员身份信息如下：

◆蒂莉·考特曼（Tillie Kottmann）



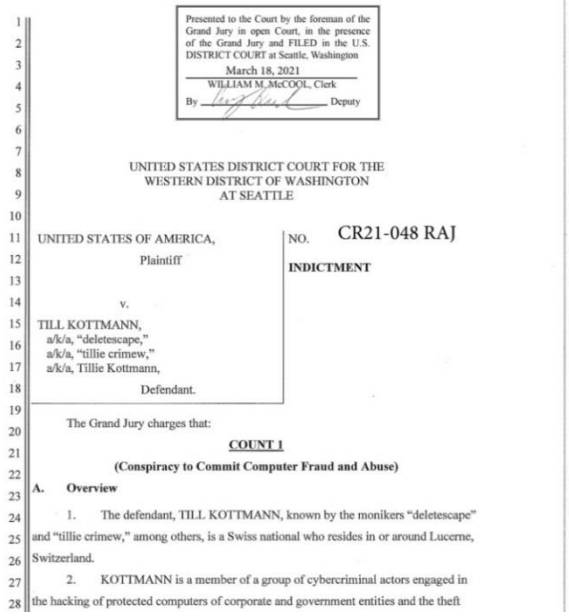
1999 年 8 月 7 日生于瑞士卢塞恩，自称是黑客、无政府主义者、同性恋，以女性自居。主要学习、工作经历如下：

- 2012—2015 年，瑞士 Kantonsschule Alpenquai 州立中学学习；
- 2015 年 8 月—2019 年，瑞士 BBZW Sursee 思科学院；
- 2017 年 3 月—2020 年 1 月，Lawnchair Launcher 公司担任项目负责人兼首席开发人员；
- 2020 年 2 月—8 月，德国 auticon GmbH 公司担任 IT 顾问；

- 2020 年 11 月至今，瑞士 Egon AG 公司程序员。

蒂莉·考特曼还是 Dogbin 网站（短链接转换网站）的创始人和首席开发人员。本来专心做技术，这份履历是很漂亮的。只可惜：

- 2020 年 4 月以来，蒂莉·考特曼通过“声呐方块”平台漏洞获取企业信息系统源代码数据；
- 2020 年 7 月，蒂莉·考特曼在互联网上曝光了微软、高通、通用电气、摩托罗拉、任天堂、迪士尼 50 余家知名企业信息系统源代码；
- 2021 年 3 月 12 日，瑞士警方搜查蒂莉·考特曼住所并扣押大量网络设备；
- 2021 年 3 月 18 日，美国司法部发布对蒂莉·考特曼的起诉书，但 3 月底突然中止该案审理。此后，中国成了蒂莉·考特曼的主要目标之一。



Presented to the Court by the foreman of the Grand Jury in open Court, in the presence of the Grand Jury and FILED in the U.S. DISTRICT COURT at Seattle, Washington
March 18, 2021
WILLIAM M. McCOOL, Clerk
By _____ Deputy

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff
v.
TILL KOTTMANN, a/k/a, “deletescape,” a/k/a, “tillie crimew,” a/k/a, Tillie Kottmann, Defendant.

NO. CR21-048 RAJ
INDICTMENT

The Grand Jury charges that:

COUNT 1
(Conspiracy to Commit Computer Fraud and Abuse)

A. Overview

1. The defendant, TILL KOTTMANN, known by the monikers “deletescape” and “tillie crimew,” among others, is a Swiss national who resides in or around Lucerne, Switzerland.

2. KOTTMANN is a member of a group of cybercriminal actors engaged in the hacking of protected computers of corporate and government entities and the theft

美国司法部对蒂莉·考特曼的起诉书及公布照片

蒂莉·考特曼 (Tillie Kottmann) 的 Twitter 账号@nyancrimew 被推特公司停用后，于 2022 年 2 月重新注册使用。个人简介中自称为“被起诉的黑客/安全研究员、艺术家、精神病患者以及同性恋”。2023 年 1 月至今，发布及转推 78 次。

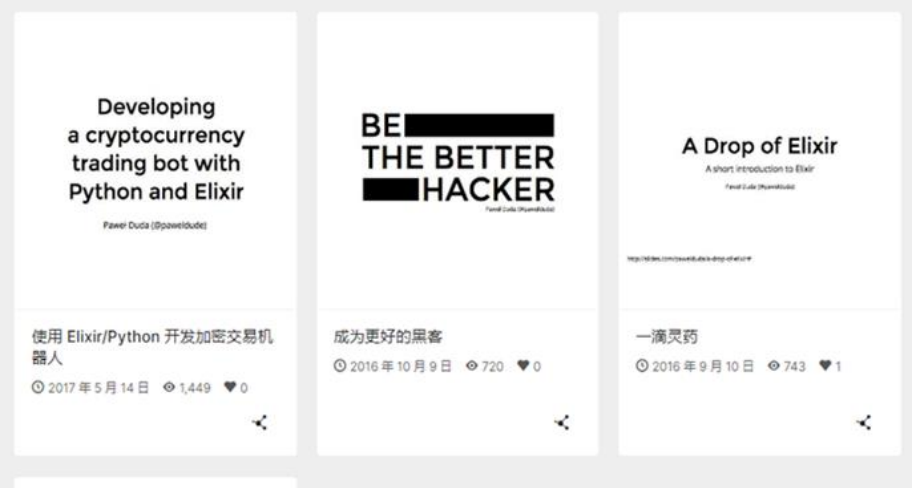
◆帕韦尔·杜达（Pawel Duda）

男，波兰人，软件工程师。

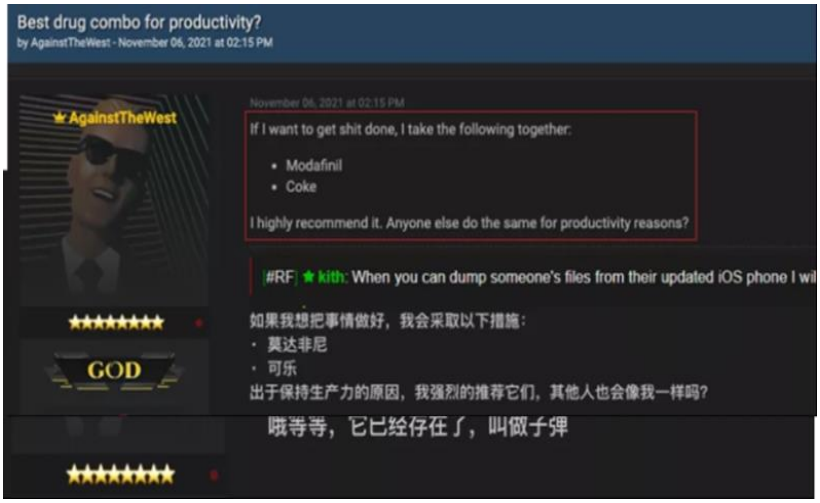
- 2012 年 11 月—2013 年 5 月，Ageno 公司 web 前端开发工程师。
- 2013 年 6 月—2013 年 12 月，自称从事某保密项目开发，任 web 前端开发工程师。
- 2014 年 1 月至 2015 年 1 月，OX media 公司 web 前端开发工程师；
- 2014 年 4 月至 2019 年 8 月，Selleo 公司软件工程师，负责开发捐款管理系统、物流服务系统、跨平台办公系统、定制化电子商务平台、酒店管理系统等项目；

- 2016年9月—2017年4月，voicefox公司软件工程师(兼职)，负责开发基于 Zoom 等视频会议解决方案；
- 2019 年 11 月至 2020 年 6 月，versum 公司软件工程师，负责开发沙龙管理系统；
- 2020 年 6 月至 2021 年 10 月，TjeKvik 公司软件工程师，负责开发汽车服务管理系统；
- 2021 年 10 月至今，自称参与了某非公开项目。

该人日常会进行黑客技术研究，并在 Slides.com 网站共享文件中设置了“成为更好的黑客”的座右铭。



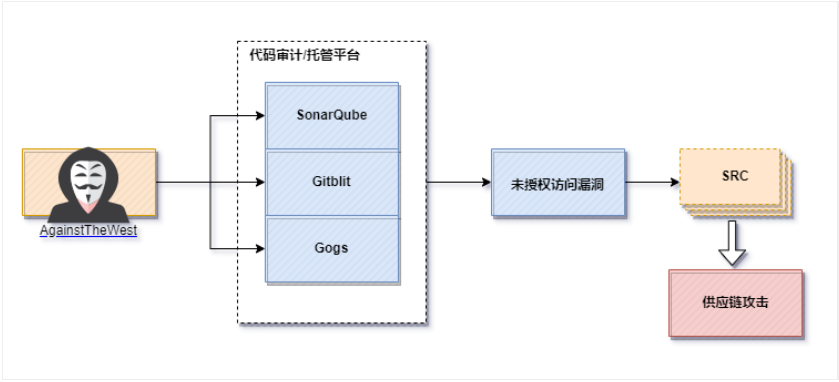
此外，该组织成员长期服用精神类药物、吸食毒品等行为，包括吸食氯胺酮（K粉），还会将莫达非尼(治疗嗜睡的药物，具有成瘾性）和可乐



一起服用。

ATW 组织主要攻击手法

- 攻击部位：调查发现，ATW 组织宣称攻击窃取涉我党政机关、科研机构等部位的数据，实则均来源于为我重要单位提供软件开发的中小型信息技术和软件开发企业，窃取数据也多为开发过程中的测试数据。
- 攻击手法：主要针对 SonarQube、Gogs、Gitblit 等开源网络系统存在的技术漏洞实施大规模扫描和攻击，进而通过“拖库”，窃取相关源代码、数据等。相关信息可用于对涉及的网络信息系统实施进一步漏洞挖掘和渗透攻击，属于典型的“供应链”攻击。



- 攻击目的：与自我标榜的“道德黑客”着实相去甚远，并非向存在漏洞的企业发布预警提示信息，以提高这些企业的安全防范能力。相反，更多的是利用这些漏洞实施攻击渗透、窃取数据，并在黑客论坛恣意曝光，炫耀“战果”。2022 年以来，ATW 组织滋扰势头加剧，持续对中国的网络目标实施大规

模网络扫描探测和“供应链”攻击。为凸显攻击目标和所窃数据重要性，多次对所窃数据进行歪曲解读、夸大其词，竭力配合美西方政府为我扣上“网络威权主义”帽子，并大力煽宣、诋毁中国的数据安全治理能力，行径恶劣，气焰嚣张，自我炒作、借机攻击中国的意图十分明显。

ATW 组织漏洞攻击利用情况

ATW 对中国企业单位开展网络攻击过程中，大量使用了源代码管理平台、开源框架等存在的技术漏洞。主要包括：

- SonarQube 漏洞。漏洞编号为 CVE-2020-27986，该漏洞描述为 SonarQube 系统存在未授权访问漏洞。涉及版本：SnoarQube 开源版<=9.1.0.47736；SonarQube 稳定版<=8.9.3。

Technical Details

Beginning in April 2020, the FBI observed source code leaks associated with insecure SonarQube instances from US government agencies and private US companies in the technology, finance, retail, food, eCommerce, and manufacturing sectors. SonarQube is an open-source automatic code review tool that detects bugs and security vulnerabilities in source code.

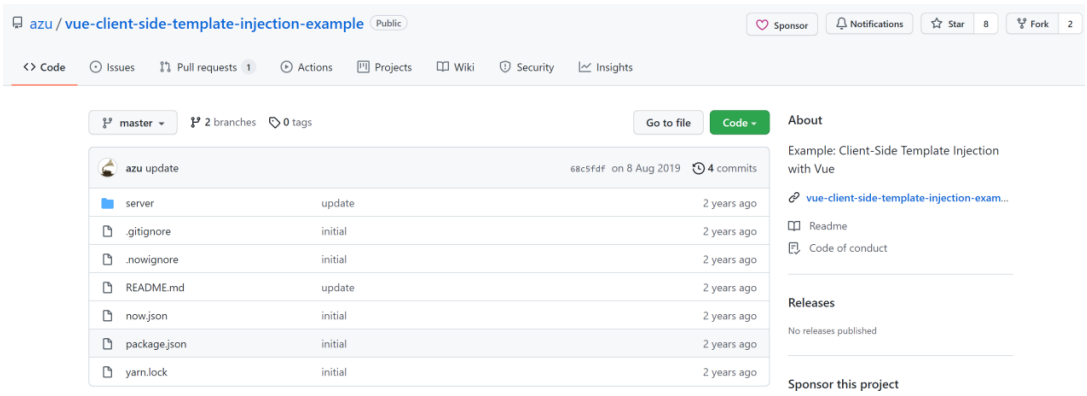
In August 2020, unknown threat actors leaked internal data from two organizations through a public lifecycle repository tool. The stolen data was sourced from SonarQube instances that used default port settings and admin credentials running on the affected organizations' networks. This activity is similar to a previous data leak in July 2020, in which an identified cyber actor exfiltrated proprietary source code from enterprises through poorly secured SonarQube instances and published the exfiltrated source code on a self-hosted public repository.

During the initial attack phase, cyber actors scan the internet for SonarQube instances exposed to the open Internet using the default port (9000) and a publicly accessible IP address. Cyber actors then use default administrator credentials (username: admin, password: admin) to attempt to access SonarQube instances.

Recommended Mitigations

- Change the SonarQube default settings, including changing default administrator username, password, and port (9000).
- Place SonarQube instances behind a login screen, and check if unauthorized users have accessed the instance.
- Revoke access to any application programming interface keys or other credentials that were exposed in a SonarQube instance, if feasible.
- Configure SonarQube instances to sit behind your organization's firewall and other perimeter defenses to prevent unauthenticated access.

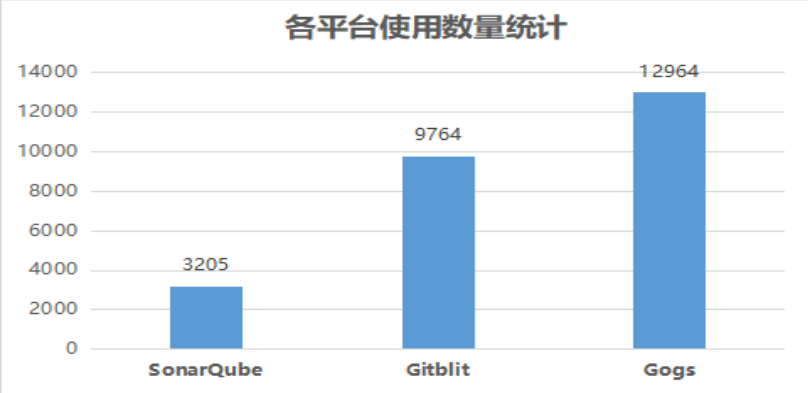
- VueJs 框架漏洞。VueJs 框架为 JavaScript 前端开发框架，VueJS 源代码在 GitHub 发布，同时本身具备较多漏洞，使用网络指纹嗅探系统可直接扫描探测，GitHub 上同样存在专门针对 VueJS 的漏洞利用工具。



- Gogs、GitLab、Gitblit 等其他源代码管理平台漏洞。上述

平台存在的未授权访问漏洞，无需特殊权限即可访问和下载存储在管理平台上的系统源代码数据。

通过对全网设备进行空间测绘，发现上述开源平台在国内使用广泛。对存在风险的资产项目进行进一步分析发现，其中包含涉及我国多家重要单位的系统源代码。SonarQube、Gitblit、Gogs 的各平台使用情况如下：



ATW 组织攻击使用码址资源

为掩护其攻击行为，ATW 组织使用了一批“跳板”和代理服务器，主要分布在英国、北马其顿、瑞典、罗马尼亚等国家。相关 IOC 指标信息如下：

序号	IOC 指标	序号	IOC 指标
1	178.175.142.195	9	194.66.201.2
2	185.65.135.169	10	194.66.201.17
3	185.65.135.177	11	141.98.255.145
4	185.65.135.178	12	141.98.255.149
5	185.65.134.181	13	91.193.4.59

6	185.225.28.158	14	51.222.253.2
7	220.143.129.216	15	51.222.253.3
8	193.138.218.162	16	51.222.253.12

在 RaidForums 论坛上发现的 ATW 黑客组织关联账号：

- “AgainstTheWest”注册于 2021 年 10 月 12 日，是发布泄露涉中国数据的主要账号。
- “AgainstTheYankees”为该组织 11 月 16 日最新注册帐号，地理位置标注在台湾花莲，职业为情报经销商，由“AgainstTheWest”推荐加入论坛。
- “Majestic-12”疑为匿名者黑客组织与 ATW 反华黑客组织的中间联络人，曾回复“ATW-对华战争”网帖，号召更多黑客、程序员加入，共同对抗中国。
- “NtRaiseHardError”在论坛多次售卖涉我数据，表示只攻击和收购中国政府数据，不会攻击美国、加拿大、英国、俄罗斯政府。该黑客与“AgainstTheWest”有数据交易，互动频繁，关系密切。
- “Kristina”在论坛发帖称广州政企互联科技有限公司已被其攻破，并提供数据库和 SSH 密钥下载，涉及“国家政务服务平台”、“内蒙古自治区政府门户网站”。
- “Ytwang”曾发帖表示要购买新疆营地、警察系统等数据库信息，以及留言表示对滴普科技相关信息很感兴趣。
- 其余账号信息如下：

注册昵称	注册时间

0x7cO0	2021/10/23 06:39
colebrain	2021/11/1 15:26
Ansimear	2021/11/2 06:47
yalishandazhongma	2021/11/15 02:07
countertek	2021/11/15 06:25
AteerCfcrCiRce	2021/11/16 16:19
IndiaTop10Worrior	2021/11/22 08:32
findA8988	2021/11/23 02:07
SHAUN2022	2021/11/23 18:34
jojo1215	2021/11/29 02:20

防范对策建议

- 建议软件开发企业立即修复 SonarQube、VueJs、Gogs、GitLab、Gitblit 等软件漏洞，严格控制公网访问权限，及时修改默认访问密码，进一步提高对源代码的安全管理能力。
- 针对已在用户单位部署的系统源代码外泄情况，软件开发企业应加强系统源代码安全审计，及时发现并修复软件安全漏洞，防止黑客利用系统漏洞进行攻击，并对重要信息系统源码及数据进行加密存储，落实网络安全防护措施。
- 建议国家有关职能部门、技术安全团队加强对 ATW 组织非法网络攻击活动的监测，及时预警攻击动向，开展背景溯源和反制打击。

小 结

本报告公布 ATW 黑客组织的攻击手法及使用的漏洞、网络码址，目的是使大家看清 ATW 组织长期以来针对中国实施网络攻击、数据窃取活动的本质，针对性修补漏洞，做好安全加固，不断提升网络安全、数据安全防护能力水平。

后续，我们的技术团队还将陆续公布对相关事件调查的更多技术细节。