An Interview with AgainstTheWest

Dissent Doe -- April 3, 2022

They are anonymous, but they are not Anonymous. Meet the individuals who are using their skills to take on the West's enemies.

Names can be misleading. When I first read about a group called "AgainstTheWest," I assumed they were working against the west. But while threat actors from Russia, China, Belarus, and North Korea attack the west, "AgainstTheWest" (ATW) has their heads down collecting intel to provide to NATO and the U.S. As they described themselves to me, they are western-friendly threat actors who go after those who are working against the west.

For the past week, DataBreaches.net has had the opportunity to chat with them as they pursued some of their activities. The following interview was conducted by chat and email over a period of days. Some answers to the interview questions represent the collective answers of group members, while other answers reflect the views of the group's public spokesperson (called "Sand" in this article).

NOTE: Because ATW functions anonymously, DataBreaches.net is unable to verify their claims about their credentials and history. Nor is DataBreaches.net qualified to assess the accuracy or the quality of the intel they provide. Those assessments and determinations will be made by others. Some typographical errors have been corrected in the transcript below and there has been light editing for clarity.

Getting Started

DataBreaches.net (DBN): When did your group first become AgainstTheWest?

> *ATW: In September of 2021, AgainstTheWest was created. We first came out with data breaches and leaks in October of 2021, releasing the Bank of China and Ministry of Public Security of China during the same month.*

DBN: As Cyberknow reported in their interview with you, you listed the data for sale on RaidForums initially. Why didn't you just leak it?

> *ATW: No one is going to listen to an account that is posting free stuff. It was our first post and we wanted attention. The same can be said for the previous other leaks.*
>
> *We got a lot of attention from it (albeit unwanted)*

So we then released a horde of data under the same names

DBN: Did you all know each other before you began working together on ATW or did some of you just meet for the first time?

ATW: We had previously worked together on different jobs around the world. We're all ex-intelligence and we lived close to each other already, so it would only make sense to form a group and be together, IRL. This also defeats the chances of insiding or secrets spilling, as we're all together, no need for dependence for online connectivity.

DBN: What was your original shared goal for ATW?

ATW: Our goal has always been the same. At the beginning, it was to steal state-secrets, government software (in the form of source codes), private documents and such. However, we also had the idea that we should act on China for attacking the west in cyber espionage campaigns over the years. Another note worthy mention would be the invasions of Hong Kong, Tibet and soon-to-be Taiwan. The last point would be the "Re-Education" camps that the Chinese government are doing on Uighurs in China.

DBN: Has your goal for ATW changed at all?

ATW: The main goal has not changed. It has been improved, as we've begun going after countries such as Iran (for attacking the west with state-sponsored APT groups), North Korea (Human rights violations, ignoring sanctions & attacking the west with APT groups), Russia (Massively impacting the west with its use of cyber espionage) & Belarus (For being closely connected to Russia).

DBN: How many people were in ATW at the start and how many are there now?

ATW: Originally, there were 6 members. However, something has happened to our main member, Pascal, who passed away in March from cancer. However, we're unsure on this being the truth, as we were only told by his parents that he passed. We have not seen him at his home, nor have we heard from him since. So there are currently 5 members from the original 6. The potential for more could be changed.

ATW declined to answer questions about what countries their members were from and their age range. And while they stated that they had all worked for intelligence agencies, they would not indicate which agencies. They tell DBN that ATW is not state-sponsored but declined to answer a question as to whether they currently get any support or help – directly or indirectly – from either the U.S. government, NATO, or any other government or NGO. DataBreaches.net turned to their backgrounds and credentials:

DBN: Infosec professionals often lament that there is too much focus on degrees and certs to get jobs. Can you say something about ATW members' formal training or certs? Are you self-taught? And do you view yourselves as elite hackers?

> *ATW: All our members have multiple certifications in their own fields. Regarding cyber certifications, we all share a Communications Information Exploitation certification, which is from the armed forces in our respective countries. Personally, I (Sand) have the CEH V10 and CISSP. Not sure about the other members exactly. In terms of actual degrees, I have a Masters in Cyber Security and Computer Science.*
>
> *We are all self-taught with some added training from work experiences.*
>
> *We do not view ourselves as elite hackers at all. We're not heroes, we're not scary hackers. We are just people. Anyone can train themselves and do this stuff.*

DBN: How many languages do ATW members speak or read?

> *ATW: We all speak English, however, secondary languages, such as French, Russian, Chinese, German and Dutch are among our members.*

How It's Going

DBN: So how does ATW pick its targets or prioritize targets? Do all team members discuss and agree, or does just one person decide whom or what to target? Or does everyone just go after targets they select for themselves?

> *ATW: Everyone votes and agrees in the team on who to target next. If the larger online community has voted for something to happen, we'll try to put that at the top of the TODO list. However, with the APT documents, we're only doing them because no other group (except KelvinSecurityTeam) has decided to go after them and expose them further than the FBI / NSA.*

DBN: Related to the above: does ATW have one leader? If not, how is the team organized?

> *ATW: Back when it was 6 members, Pascal was the main leader. He spoke to the community and found information out and would relay it to the whole team in group meetings IRL. However, as there are now 5 members, we don't have that position, so someone had to take it up.*

DBN: So who took it up?

> *ATW: I did (called "Sand" for purposes of this interview).*

DBN: Is everyone in the group a hacker or do some have other roles?

ATW: Everyone has their own designated roles. We have a translator, financer, hacker / exploiter, programmer & graphics artist.

ATW declined to answer questions about their methods and tools, but they did address questions about how quickly they seemed to be able to uncover intel that others had not produced

DBN: One of the things that struck me was how quickly you claimed to find new material on your targets. As one example, while we were chatting, you told me that you were about to start researching a particular APT group. That message of yours was timestamped 8:53 pm (my time). At 9:30, you messaged: "Just letting you know, that this APT34 info will be massive." And at 9:52, you wrote, "Already got a lot of info" which you told me was "Completely new" information on the group.

ATW: When we all work together, the flow of work is a lot quicker than most groups, which tend to be disorganized. We know what we're doing and we're experienced. We know what to look out for and we use that to our advantage. The information we try to find (if any) will be new, and we try our hardest, with all our resources, funding, experience, and skills.

A lot of people suggested that our previous attacks were automated. This isn't true. It's all manual.

Unofficial US Intelligence Community feedback about ATW's work products has been positive. “Keep anything/everything coming [from ATW],” one source asked DBN after reviewing material this site sent them for comment. They were also reportedly excited to receive ATW's latest document on APT28. That document contains additional information that ATW has not made publicly available.

DBN: Do the groups you target just have poor security or are you all just phenomenal at OSINT?

ATW: It's a mix. We'd like to think we're good at what we do. Our OSINT skills are pretty good. Not anything crazy, however, these APT groups are the top tier of hackers. They are very skilled. Looks like they just left a trail of what they've left behind from their campaigns, which we've found and exposed.

While ATW generally works as their own team, they have occasionally collaborated with others, telling DataBreaches.net that they have collaborated with Intrusion Truth, Anonymous, Belarusian Cyber Partisans, GhostSec, Anonymous Taiwan, BrazenEagle, and PucksReturn.

Successes and Frustrations

So what has been the group's biggest success and its biggest frustration?

ATW: The most satisfaction? Out of everything, it would be the APT documents we've produced. They are by far, the most interesting leaks we've produced. The data on them, the classification of the info on them, the notable groups it's involved with, it's crazy.

The most frustrating would be the Main Directorate of the General Staff of the Armed Forces of the Russian Federation. They have been so hard to crack. We've employed every ace up our sleeves, yet we're unable to breach them. We've given this info to BrazenEagle.

Ethical Concerns

DBN: Are there any targets that ATW definitely wouldn't hit or leak?

ATW: We will never, ever hit any western country, government, persons, company at all. Hospitals and schools are also off-limits. Full stop.

DBN: ATW has publicly stated its support for Ukraine. Given that Russia threatens retaliation for any assistance to Ukraine or attacks on Russia, do you think there's a risk that you might make things worse instead of better by attacking Russian targets and leaking the data?

ATW: They could retaliate for our actions, but after looking at their joke of a military and their pathetic security, along with their allies, APTs and security, I don't think they have a chance against NATO and the west.

DBN: When some of us have interviewed ransomware operators, we ask them to tell us something about themselves that our readers might be surprised by. You are not ransomware operators but are probably perceived as threat actors by those you target, so.... tell me something about yourselves that might surprise my readers.

ATW: We all have separate jobs in the ethical hacking sector. We all work for contracted ethical hacking companies, yet these companies don't know about ATW or our work. We've been working on tightening security on companies and government agencies since the Ukraine invasion. Mostly on German and US systems.

DBN: Speaking of "threat actors," do you even view yourselves as criminals or threat actors? Do you think you will ever be caught and prosecuted?

ATW: We don't see ourselves as anything. Hackers. That's all. We're doing our job in the hopes that it benefits western intelligence. We share all private documents with anyone from the government in the US / EU.

Countries in the east, such as China & Russia may see us as an APT group, or a threat actor group, but we don't see ourselves as such. Hopefully, we can actually finish ATW

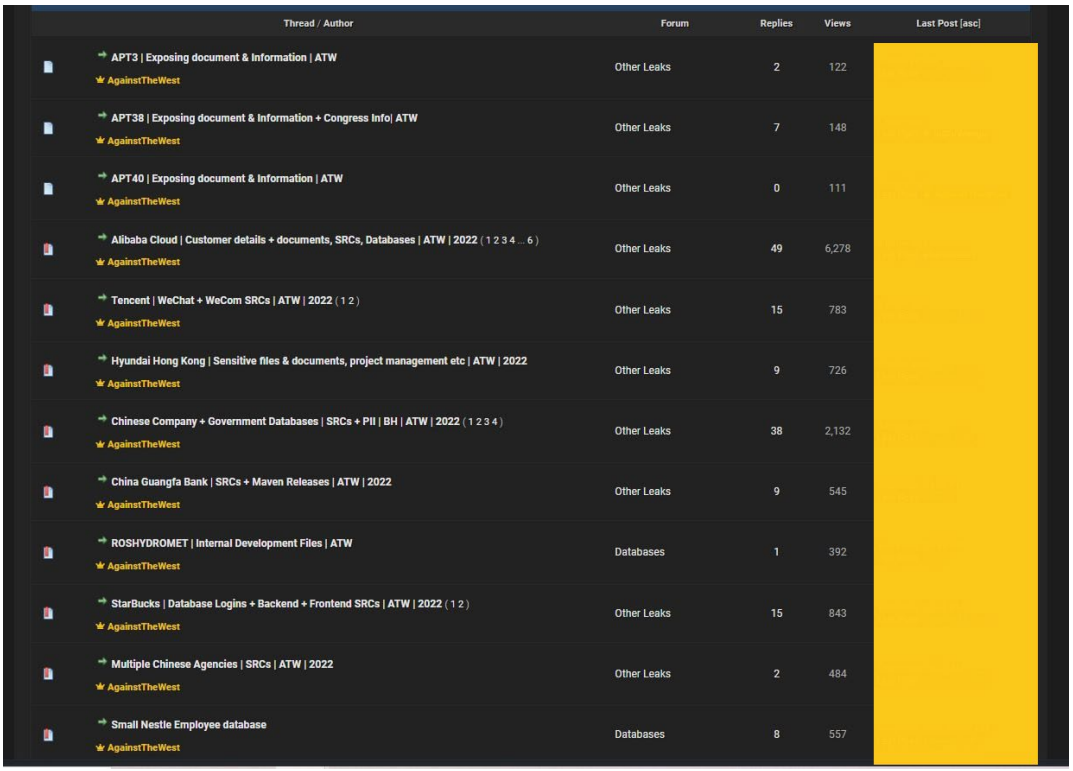
after the APT groups have been exposed and get employed by these countries we're trying to help.

DBN: In one of our chats, you indicated that a lot of agencies have reached out to contact your group. Are you available to be hired if any of these agencies want to contract with you?

ATW: Yes, we're available to be hired. If a legitimate agency feels that they want our skills, then they can find us IRL and ask us in person.

Some of ATW's Activities

ATW has engaged in a number of attacks on entities in Russia and China, as well as attacks on entities in North Korea and Iran. The following is just a partial sample.



Thread / Author	Forum	Replies	Views	Last Post [asc]
APT3 | Exposing document & Information | ATW AgainstTheWest	Other Leaks	2	122	
APT38 | Exposing document & Information + Congress Info| ATW AgainstTheWest	Other Leaks	7	148	
APT40 | Exposing document & Information | ATW AgainstTheWest	Other Leaks	0	111	
Alibaba Cloud | Customer details + documents, SRCs, Databases | ATW | 2022 (1 2 3 4 ... 6) AgainstTheWest	Other Leaks	49	6,278	
Tencent | WeChat + WeCom SRCs | ATW | 2022 (1 2) AgainstTheWest	Other Leaks	15	783	
Hyundai Hong Kong | Sensitive files & documents, project management etc | ATW | 2022 AgainstTheWest	Other Leaks	9	726	
Chinese Company + Government Databases | SRCs + PII | BH | ATW | 2022 (1 2 3 4) AgainstTheWest	Other Leaks	38	2,132	
China Guangfa Bank | SRCs + Maven Releases | ATW | 2022 AgainstTheWest	Other Leaks	9	545	
ROSHYDROMET | Internal Development Files | ATW AgainstTheWest	Databases	1	392	
StarBucks | Database Logins + Backend + Frontend SRCs | ATW | 2022 (1 2) AgainstTheWest	Other Leaks	15	843	
Multiple Chinese Agencies | SRCs | ATW | 2022 AgainstTheWest	Other Leaks	2	484	
Small Nestle Employee database AgainstTheWest	Databases	8	557	

Some recent listings of leaks by ATW on a hacking forum. Earlier listings on RaidForum are no longer accessible from that site but screenshots showing the former listings can be found online.

Partial List of Notable Chinese Data Breaches (there have been more than 200):	**Some Notable Russian Government Data Breaches**:
Alibaba Cloud (3 times) Bank Of China Huawei China Petroleum Technology & Development Corporation Chinese Prisons China Oil Ministry Of Justice China WeChat Tencent Starbucks China Xiaomi Cloud Ministry Of Public Security Lenovo China China's Hunan Government JD.com Amazon China (Privated) Center for Disease Control and Prevention Ministry of Public Security Ministry of Science and Technology State Market Regulatory Administration cable maker Zhongtian Technology Submarine Cable Co	Russian Space Forces AIP of the Russian Federation PJSC Aeroflot (Russia Airlines) Ministry of Digital Development, Communications and Mass Media of the Russian Federation, Pskov Region Ministry of Emergency Situations of the Russian Federation Federal State Statistics Service Federal Service for Labour and Employment (Ministry of Labor and Social Protection of the Russian Federation) Novolipetsk Steel Sberbank DNPP ROSHYDROMET Belarusian Media CTV AMD Russia BrandSquad Russia Delans Russian Postal Development of Territories of the Russian Academy of Sciences Federal State Budgetary Educational Institution of Higher Education Altai State Pedagogical University of the Russian Federation Gazprom Nauchnyy Tsentr Prikladnoy Elektrodinamiki OJSC Ak Bars Holding PromEngineering Russia Air Russian Rail ScanexRU X5 Russia Bee Russia xTrack Almaz-Antey Joint Institute for Nuclear Research

A timeline of ATW's activities from mid-October 2021 through the end of November 2021 can be found at Observable.

In addition to the attacks on specific sites or organizations, ATW has also acquired and compiled what they say is new intel on known APT groups including:

- APT38 / Lazarus Group
- APT3 / Boyusec
- APT40 / Periscope Group; and
- APT28 / Fancy Bear

DBN: Given how you have targeted China and Russia, does ATW have any concerns for your safety?

> *ATW: We do. We've expected to be drone striked & poisoned. However, where we're placed, it doesn't look like that'll work. We ensure that we are safe at all times, acting covertly. Given our prior roles in the world, we have some political protection in place.*

For their sake, DataBreaches.net hopes these masked crusaders for the West do stay safe.

