Intrusion Truth - Five Years of Naming and Shaming China’s Spies

zetter.substack.com/p/interview-with-intrusion-truth

Kim Zetter

Share this post

Intrusion Truth - Five Years of Naming and Shaming China’s Spies

zetter.substack.com

In 2017, a mysterious group called Intrusion Truth began exposing the real identities of hackers behind Chinese spy operations. In an interview, the group discusses their controversial work.

Kim Zetter
Mar 29

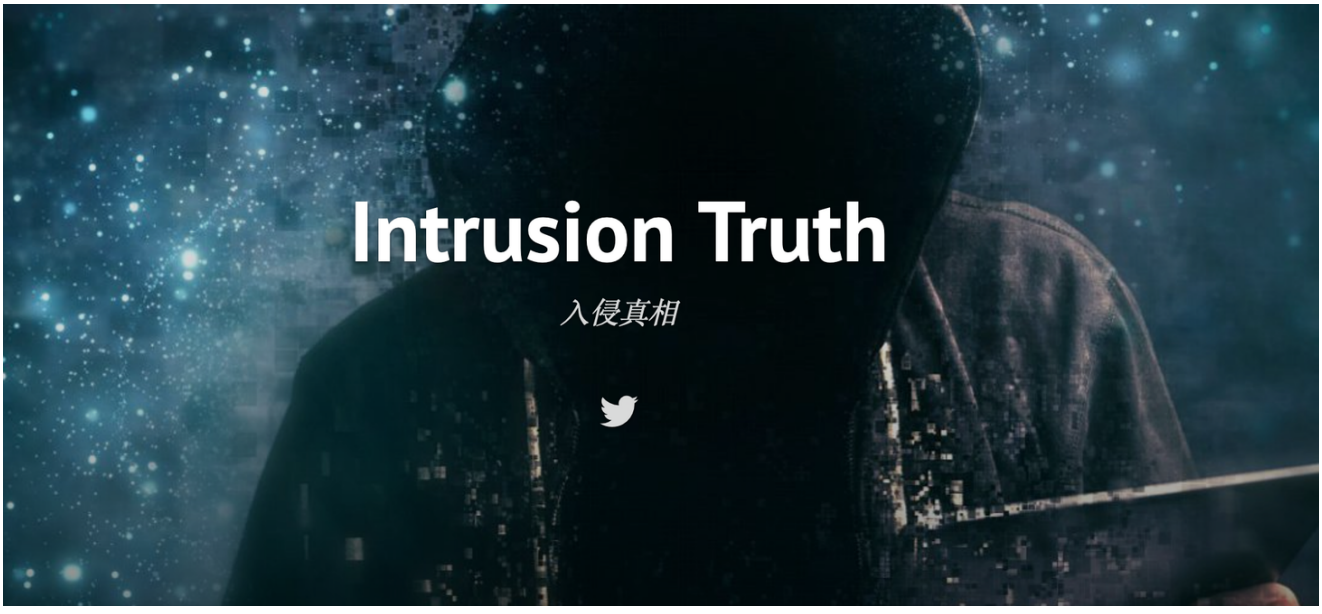
13

4

Share this post

Intrusion Truth - Five Years of Naming and Shaming China’s Spies

zetter.substack.com



In 2017, a mysterious person or group going by the name Intrusion Truth began to systematically expose the real identities of hackers behind some of China's most egregious spying operations.

They don't expose just any hackers on their anonymous blog, but focus on teams that pilfer intellectual property from western companies and scientific institutions for the purpose of enriching China's industries — a violation of what the U.S. deems acceptable espionage practices.

Intrusion Truth has outed low-level hackers as well as the intelligence officers allegedly directing the spy campaigns, documenting the steps they took in each case to uncover the names.

Although Intrusion Truth publishes only once or twice a year, it has garnered respect and interest in the security community both for the depth of its investigations and the accuracy of its findings. And twice after Intrusion Truth publicly exposed individuals allegedly behind China's theft operations, the U.S. Justice Department indicted the hackers Intrusion Truth exposed. This, of course, has raised questions about whether the group's research is directed by the government or done in coordination with it.

The group has managed to keep its identity secret for five years, though there is a lot of speculation about who is behind it. There are also questions about some of the group's methods. Most of the investigations are done using publicly available information. But the group has, on occasion, relied on information that wasn't public — for example, credit card statements they obtained through an unnamed Bank of China source, which helped them identify a Chinese intelligence officer.

Zero Day spoke with Intrusion Truth via email about their motivations for exposing Chinese hackers, their limits for what they will not publish, and whether they work with any governments to out Chinese hackers. The interview has been lightly edited.

For more on Intrusion Truth, I've also published a separate story that takes a deeper look at what Intrusion Truth has uncovered over the last five years, examines their sometimes unorthodox methods for gathering information, and looks at some of the concerns around the group's work.

You refer to yourself in the plural. Is Intrusion Truth an actual group or is it one person operating a public front for information amassed by a lot of different threat intelligence groups?

Intrusion Truth is a global network of anonymous contributors united by a common goal to expose Chinese APTs. We come from a variety of backgrounds and all bring something unique to the table. We never reveal who we are or who we work with. That is central to our identity and is so we can protect our contributors and partners.

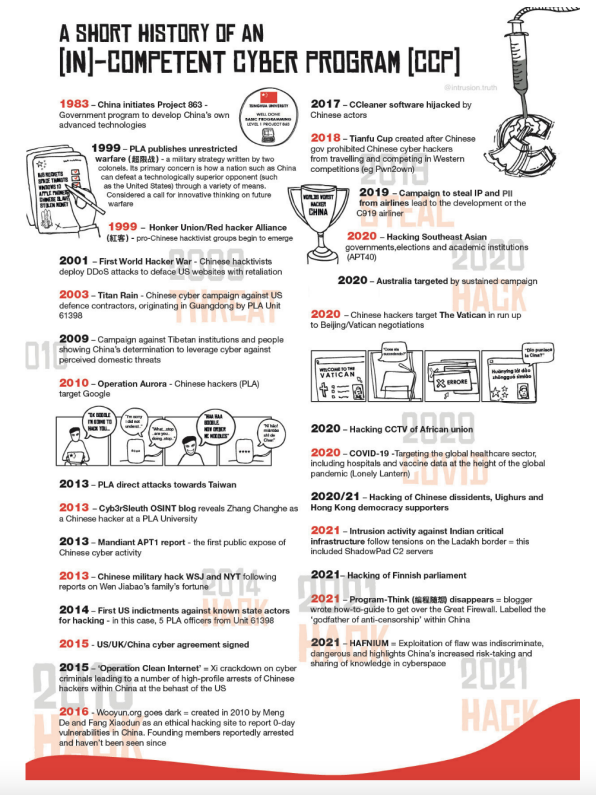
[Readers who write-in with tips and information] are a key part of our Intrusion Truth network. We have had some crucial contributions from write-ins which have proven to be a real game-changer. On top of that, the Chinese internet is huge and awash with lots of information which can help our investigations. Accessing it is easier than most people think. The more you dig behind the Chinese firewall, the more you find.

You've indicated that Cyb3rsleuth was an inspiration for launching the Intrusion Truth identity and blog. Can you talk more about the impetus for doing this?

The OSINT [open-source intelligence] community, including Cyb3rsleuth, has done some incredible work to expose Chinese hacking, but we wanted to go where not all threat hunters are comfortable going. We wanted to actually unmask the hackers. We created Intrusion Truth to demonstrate time and time again the MSS' [China's Ministry of State Security] key failing: it cannot (and often makes little effort to) protect the identities of the hackers it employs. We want Chinese hackers to open their eyes and realize how little their government cares about them. At any given moment, their MSS handlers could scapegoat them as criminals in order to do what China tries so hard to achieve: protect the state.

Why focus only on threat actors and groups in China? Has there been talk about doing this for Russian actors as well, or Iran?

There is a battle going on. It's not China vs. the West as the [Chinese Communist Party] would portray it. It is China vs. the World. We see their activity everywhere — from Africa to South East Asia to Europe and the US. Chinese cyber hackers are operating on an unprecedented scale, and that's why they are our focus. What these hackers do affects us all; it is our personal data that is hacked and our intellectual property which is stolen.



Intrusion Truth timeline tracking pivotal points in the history of China's government-led hacking groups.

There are a lot of APT groups working out of China. How do you decide which one to focus on for your research and to publicly expose? [APT stands for Advanced Persistent Threat and refers to hacking groups, generally state-sponsored, with advanced skills.]

Given the amount of hacking coming from China, the surface area is large. Intrusion Truth follows leads from a number of sources, including write-ins [from readers], industry reporting, blogs and indicators of compromise. We listen to what our readers want to see.

Have you received any criticism for doxxing individuals who haven't been charged or convicted of a crime, or for accusing companies of being front operations for Chinese-government hacking when the owners haven't been indicted?

We are rigorous in our verification of information, and this can take time. We always publish in good conscience, knowing that we have tried our best to make sure we are revealing "the whole truth." Our work is often independently corroborated by other threat hunters. We have received a lot of support, and it is rewarding to see the threat hunter community going from strength to strength in pinning these attacks on the Chinese state.

Are you concerned that China might turn the tables and start doxxing government hackers working for the U.S. or other western countries?

Intrusion Truth's primary goal is to expose the whole truth of Chinese state-sponsored hacking. It has been our goal from day one. We understand people might have a number of different concerns about what we do and how far we go. But it is important for us and our

community that we stick to that primary objective. We can't let state-sponsored Chinese hackers act with impunity.

Years ago the threat intelligence company Threat Connect published a report about Chinese hackers that included a photo of an infant — with its face obscured — taken from the birth announcement of a Chinese hacker's social media account. It prompted some criticism in the community. Are there boundaries you won't cross? Are there actions you won't take or information you won't publish?

Interesting question. It's something that we keep in mind, yes. We don't have a drawn-up list of "red lines". But we do think about it.

Credit card statement from the Bank of China that Intrusion Truth says it used to confirm that a Chinese national named Zhao Jianfei is an intelligence officer working with state-sponsored hackers.

Most of your information comes from open-source research, but I counted four cases where you obtained information that wasn't publicly available: credit card statements from the Bank of China, Uber receipts, the identity of a Chinese hacker obtained from his frequent flyer account, and information you received about plane trips that two Chinese nationals took. How often do you use non-public information in your investigations?

The information we find comes in different ways, making no two investigations the same. So it's hard to put a figure on how often we rely on the information provided by the Intrusion Truth community vs information found from open-source searching.

We receive tips on a weekly basis from around the world on Chinese cyber activity and the actors suspected of being behind it. We always try to corroborate what is sent to us. When we're focusing on a particular investigation, we also reach out to see what the community can help us discover. Sometimes, they're able to provide us with information which helps us tell the story. But we have to stress here too, the Chinese internet is huge and there's so much out there to be found. It is also, contrary to popular belief, very much accessible. There are some good online guides now too on how to navigate it, even if you don't speak Mandarin.

The U.S. government has indicted several Chinese nationals after you publicly exposed them. Do you coordinate with the Justice Department or any other U.S. or non-U.S. government agency before you publish?

We know the impact of Intrusion Truth is real. It is not surprising to us that governments are interested in our work and read what we have to say. We at Intrusion Truth want to initiate a change, but we can only do this by making governments and the private sector wake up to the threat that the Chinese state poses.

When we publish our work, our main objective is always to expose the truth. The topics we cover are guided by what we know our readers are interested in. Our readers come to us with ideas for a variety of their own reasons: for some its enthusiasm for OSINT work and for others, it is about a particular interest in an APT group. Intrusion Truth follows leads where we find them. Our readers want to use the information we publish for a number of their own reasons. So long as we know we have an Intrusion Truth community interested in our work, we will continue to expose the Chinese APTs that pose a threat to us all.

There has been a suggestion that some of the investigations you conducted might have involved parallel construction — that is, a government agency that already identified the Chinese hackers using classified intelligence methods and sources has tasked you with creating a trail of public evidence to these individuals so the government could indict them without exposing the classified intelligence methods used to originally identify them. Are you working or cooperating with any government to publicly expose Chinese hackers?

The Intrusion Truth community guides and informs all the work we do, including what Chinese hackers we go after. We mentioned write-ins before — we're currently working collaboratively with a couple of members of our community on an investigation to try and identify a long-standing Chinese hacker after they fancied a challenge. We will see how successful we are in doing so (watch this space).

We keep the identities of the Intrusion Truth community hidden. Honestly, we don't always know their real-life identity, sometimes just their online persona. That's fine with us as long as they can help us tell the whole truth. We always try to corroborate tips that come in. Related

to that, if anyone reading this does have information that can help us, please reach out and share it. We're always on the look out for new opportunities.

Do you feel any sympathy for government hackers who live in oppressive regimes and might not have a choice in their occupation?

We feel for the COVID-19 vaccine developers working around the clock who had to endure Chinese hacking attempts to steal their IP. We feel for universities around the globe plagued by Chinese state-backed intrusions while they try to provide an education for our families and friends. We feel for people all around the world that fear their personal data may have been stolen and sold… by Chinese state-backed hackers for personal profit.

Chinese hackers do have a choice about their occupation. There is a booming tech industry in China — and around the world — where these hackers could really put their skills to better use. Just look at the way India-born tech entrepreneurs now lead some of the biggest companies in Silicon Valley. And India has as a result maintained a much better global image when it comes to trust and confidence.

After Intrusion Truth wrote that it planned to expose the identity of someone known only as "MSS Officer 1" in a Justice Department indictment, someone created a Twitter account under the name Ren Yuntao and sent a tweet to Intrusion Truth with an image of American singer Lionel Richie asking "Hello, Is it me you're looking for?"

What is the most interesting person or entity you and your team exposed?

Our article linking Ren Yuntao to an unnamed APT from Chengdu (now named Lonely Lantern by our readers) was a real highlight.

After you wrote that you planned to expose the identity of "MSS Officer 1" mentioned in a DoJ indictment, someone created a Twitter account under the name ren_yuntao and posted a photo of American singer Lionel Richie with the words: "Hello, Is it me you're looking for?" Have you had any reactions or communication from other people you discussed on the blog?

It's fair to say we were thrilled — and surprised — when [Ren Yuntao] set up a Twitter account in his own name and tweeted a Lionel Richie gif at us. You can really get a sense of Ren Yuntao's arrogance. You can't help but wonder how the MSS reacted to him baiting us. If anything, it has made us even more determined to look into him and all the other hackers and MSS officers he will lead us to.

Every time we see the reaction from our readers, we are reminded just why we set up Intrusion Truth. We have so much more in the pipeline for 2022, including a couple of our big, traditional APT investigations. Intrusion Truth will not give up until China stops its large-scale and reckless cyber hacking.


Intrusion Truth @intrusion_truth

Intrusion Truth now knows that Chinese hackers are conducting cyber attacks against Ukraine. We can only assume these have been ordered, or are at least condoned, by the Chinese state. If they haven't, the CCP has a big problem: hackers getting ahead of CCP foreign policy.
March 15th 2022

215 Retweets471 Likes

You recently published a tweet indicating that some of China's APT actors have begun to direct their operations against targets in Ukraine, following the Russian invasion there. Can you elaborate?

On Ukraine, we're only at the beginning of uncovering what's going on. But it looks as though there is a decent amount of Chinese activity getting off the ground, which is a clear change of tactics since the invasion began. We're seeing some Chinese actors pivoting onto Ukraine even though they normally cover other areas, so they are obviously taking advantage of a desperate situation. Given what we know about Chinese APTs, these orders are likely coming from the top.

A separate deep-dive story about Intrusion Truth is currently only available to paid subscribers. This piece takes a more in-depth look at what the group has uncovered over the last five years, examines their sometimes unorthodox methods for gathering information, and looks at some of the concerns around the group's work. If you wish to become a paid subscriber, click here:

Other Stories of Interest:

When Russia Helped the U.S. Nab Cybercriminals

Former NSA Hacker Describes Being Recruited for UAE Spy Program

The Spy Story that Spun a Tangled Web

If you like this story, feel free to share with others.

Share

If you'd like to receive future articles directly to your email in-box, you can also subscribe: