"I'm Not Pro-Russia and I'm Not a Terrorist!" —- InfraGard and Airbus Hacker “USDoD” Unveils His New Campaigns - DataBreaches.Net

Published: 2023-09-17 · Archived: 2026-04-09 02:14:14 UTC

The first time DataBreaches remembers hearing about the man who calls himself “USDoD” was when he posted a sales listing for member data from InfraGard. He had not only managed to acquire data on 80,000 members of an organization dedicated to protecting critical infrastructure, but his revelation of his method exposed some embarrassingly inept security on InfraGard’s part. But that incident and his newest leak involving 3,200 vendors of Airbus aren’t the only reasons to pay attention to him. In a somewhat rambling interview with DataBreaches, conducted over several days online, USDoD reveals some of his current operations and future plans with respect to US defense agencies and firms.

This post is divided into two major sections. The first provides some background on USDoD as he describes himself. The second part reveals some of his current operations and developing projects. Because USDoD is not a native English speaker and requested that typos and errors be corrected, there are numerous instances where typos or confusing phrasing have been edited for clarity. At other points, his writing has been left as in the original. Those parts reflect his usual writing style.

Part 1. Background

Who is USDoD?

USDoD is a man in his mid-30’s. He describes himself as single but as being in a serious relationship with his girlfriend, who is a doctor. When asked if she knows what he does, he said that she does know. USDoD tells DataBreaches that he was born in South America but moved to Portugal. He holds dual citizenship in Brazil and Portugal, but currently lives in Spain. USDoD speaks three languages: Portuguese, English, and German. “English is not my main one,” he told DataBreaches, who had pretty much already figured that out quickly. When asked whether he speaks Russian, he responded that he is first starting to learn it this year.

When Did He Start Hacking?

USDoD states that he first got started in 1999 after joining a Brazilian gaming community. He was 11 at the time, and says he was able to use social skills to help take down a pedophile. He also states that a moderator of that community, who was also a developer for r3x software, took him under his wing and encouraged him and helped him develop skills. He says he was also greatly impressed by Kevin Mitnick. “Sadly, I never met him, but damn, this guy is a legend in my generation. His social engineering skills inspired me a lot to become what I am now.”

USDoD’s preferred learning style is to attack real, but small and unknown, companies. “I learn in real scenarios. Got my hands really dirty to get experience. I wasn’t learning in local labs and stuff like that. I don’t like that,” he

told DataBreaches.

Early Campaigns Against the Military and Defense Contractors: 2021-2022

USDoD was known as "NetSec" on RaidForums. "As 'NetSec', I breached a number of entities, but my most notorious one was my own operations against the U.S. Army and defense contractors in my #RaidAgainstTheUS campaign," he told DataBreaches.

In February 2022, Cyble Research Lab wrote a report on NetSec, describing him as a pro-Russian threat actor. The report provided a timeline of his activities:

Source: Cyble

The incidents included a US Defense Technical Information Center database, a US Army Special Operations Center of Excellence database, a US Strategic Command database, a US Central Command database, a U.S. Special Operations Command database, and a Lockheed Maring database. All of those releases were within a two-day period in February 2022. The report also included screenshots of how USDoD listed and explained the attacks.

"I'm Not Pro-Russia"

Because a number of NetSec's posts referred to Russians or collaborating with a Russian or Russians, it was understandable that Cyble and others might view him as pro-Russia, but USDoD takes strong exception to that. He tells DataBreaches that what others seem to assume was a political alliance of some kind was not political at all. He got involved because of a private request from a friend to whom he felt indebted.

In other cases, he may have collaborated with Russian individuals or sold data to Russian individuals, but not due to any political views on his part.

Perhaps it was partly an English problem, but USDoD really didn't seem to have insight into how his words were creating an impression that he was pro-Russia. And to show me that such claims were not true, he started telling DataBreaches about U.S. clients and what some of the February 2022 posts were really about.

As a specific case in point, the "Russian" referred to in February 2022 posts that Cyble reported was an independent security researcher he is close to. The researcher had showed him an AI platform he was developing called "Tulip" and asked him to collect any military data that may or may not help him in that project. Believing that there was no intention to harm U.S. critical infrastructure, USDoD agreed to help. He still believes the project was and is an innocent one.

"Since that time and my work on it, there has never been any evidence publicly or in private that there was any harm done by what I did or any leak of intel. This was never political," he said. "Maybe I messed up my writing when I wrote I was selling to "the Russians" as if there was something political about it. No. I just got info for them for what an AI project that is not targeting the U.S."

In addition to telling DataBreaches that he also has U.S. clients, USDoD noted that shortly after the Cyble report appeared in 2022, he was contacted by someone very close to the Iranian government who tried to buy the intel he had described in his posts, "but I declined to sell it to him. I won't attack certain countries but I also won't do business with their governments or political people or military. I don't do political business with anyone at all. Same rules apply to all," he told DataBreaches.

More on Standards and Ethics

Some hackers avoid hacking entities in specific countries, like CIS. When DataBreaches asked USDoD if he excluded any countries or sectors, he answered that, for ethical reasons and standards he created for himself, "I won't attack Russia, China, South and North Korea, Israel, and Iran. The rest I don't care," he said.

When asked why he thought it would be unethical to hit those countries, he replied, "Because I got people that I truly know and I truly respect there. People that I care enough to not pissing any gov or corp off. My beef with USA is not personal. I don't hate the USA culture. I like what they do. I just have zero respect for any govs."

Somewhat baffled by his response, DataBreaches asked, "But you will hit U.S. gov even though you have people in this country you like and respect?" "Good question," he responded, and then told me about a personal incident in his life that was significant. He spoke of being in New York in 2012 for cancer treatment and how he got deeply involved with an employee at the hospital where he was a patient. But being a hacker and suspecting corruption in the hospital, he hacked the hospital. He says the employee knew what he was doing and helped him, but the day before he was scheduled to meet with the media and expose the hospital's corruption, she disappeared. He says he was never able to find her again, despite searching and hiring a private investigator. Because she disappeared suddenly that way, he never went public that day with what he had found, and without any support in New York, he finished his treatment and left, taking with him a personal grudge against the U.S. and great sadness and grief about her leaving him that way. Although he is clear that he will never attack U.S. hospitals or childcare facilities, he harbors some resentment against the U.S. and says he still gets very emotional about her disappearing that way.

It was difficult to understand how that one experience of personal betrayal could translate into a lasting grudge against our government. So till trying make sense of it all, and feeling something like the ghost of Senator McCarthy, DataBreaches asked him directly: "Are you now, or have you ever been, paid by or financially supported by any government for your hacking activities?"

"No. I don't like politics," he answered. "The world should live free of politics. I won't take any money from governments, no matter how much they might offer." He also denied any religious, racial, or ethnic biases in his decisions and operations.

"My reasons are purely personal vendetta. I don't take sides. I play both sides of the war and no politics."

It's Not Political, But It's Not Just Vendetta or Business, Either

"A lot of hackers tell me that 'It's just business' and their motivation is financial. You have said it's not political and it's personal vendetta. Do you have any other motivation?" DataBreaches asked him.

"It is not only business. It is about challenge. I like a real challenge." USDoD would later illustrate just how much he likes a challenge when he gave DataBreaches a glimpse into his current and future activities. Those are described in Part 2 of this article.

USDoD on Breached.vc and the InfraGard Incident

Like many other RaidForum members, USDoD made his way to Breached.vc when it was opened by "Pompompurin" after the seizure of RaidForums. On Breached, he used "NetSec." USDoD first used the moniker "USDoD" in December 2022 when he posted data from InfraGard. "I picked USDoD as a joke for people to think that DoD breached InfraGard. I also used their seal as my avatar. It was literally just a joke to make the FBI feel even worse after seeing it in the news. I don't use their seal anymore as my avatar, though," he told DataBreaches. These days, his avatar is a cute kitten.

The InfraGard incident captured media attention because InfraGard is a public and private partnership between the FBI and private sector firms that work together to protect critical infrastructure. USDoD managed to get access to their membership data by simply applying to become a member and getting accepted. He didn't apply under his own name. He used the name of a CEO of a financial firm who was not a member but whose application would likely be accepted. The application was submitted with an email address that he controlled. To his surprise, his application was accepted without any further vetting. But there's more to the story than was revealed last year. USDoD told DataBreaches that his method involved a prior test run application.

"First I created a sketchy application with some false information and submitted it to see how InfraGard would respond. Once I saw what they said was wrong with my application, then I knew what I had to be accurate about. I was very surprised, though, that they accepted the final application because I did not use the professional email for the CEO I was impersonating. I had created a fake Tutanota email address and impersonated a staff member." According to USDoD, the email address he used for the application with the CEO's application was staff@tuta.io.

"I really don't understand why InfraGard approved the application at all," he said. Neither do we, but we note that InfraGard was compromised by someone impersonating someone who wasn't an employee or member and had an anonymous mail service. When DataBreaches asked USDoD how much he relies on social engineering to gain access, he replied, "100%, but I'm not perfect. I have failed sometimes. It is normal."

When asked about his preferred social engineering technique, he replied that it was impersonation. "My technique is to become someone else. I love impersonating and becoming someone else. This is how I got access to

InfraGard, NATO Cyber Center Defense, and CEPOL." [Note: the NATO and CEPOL attacks are discussed in Part 2]. USDoD says that he also researches his targets using ZoomInfo to see how big the potential target is in the military and defense sector.

USDoD says that he felt somewhat badly after the InfraGard incident when some people suggested it might be the reason Pompompurin was arrested and the forum subsequently seized. DataBreaches does not know who suggested that, but it's extremely unlikely that InfraGard was the proximal cause of the arrest and seizure. Those occurred quickly after the D.C. Health Links incident involving the personal and health insurance-related data of members of U.S. Congress, their families, and employees in the D.C. region. Supporting that hypothesis is the fact that the Office of the Inspector General of the U.S. Department of Health and Human Services was involved in both disrupting the forum and getting it seized. They would likely not have been involved if the concern was Infragard, which was three months earlier.

Is He Ever Scared?

Because he has often picked high-value targets in the defense sector, DataBreaches asked USDoD if he worried a lot about getting caught.

"Well it depends on my mood and what is going on, but due to the nature of my work, I always stand in high alert and monitor some platforms to keep an eye on what researchers are doing or what some key figures are saying," he responded.

But at other times during this interview, USDoD would say that he was not worried and that he "had that part covered." When asked to explain what that meant by that, he replied that he "got a green card or free pass to operate in Spain or do whatever I want in Spain. It's from some key people in Spain. Sadly, I can't share any more intel as it could compromise the situation."

In response to that somewhat surprising claim, and having been told by him that he worked in the field of cybersecurity and occasionally came to the U.S., DataBreaches asked if he had any coverage outside of Spain or if he would be at risk if he came to the U.S. "You are right, but I would still risk everything going there if something is worth it. It depends on the situation, and you are one of these that I am willing to risk," he replied. Not sure that I understood him correctly, and because he had mentioned several times that he would like to meet in person for coffee in New York, DataBreaches followed up, "You are willing to risk getting caught for this interview, or to come to NY to meet me???" "Not only an interview," he answered. "To come to you, meet you, drink a cup of coffee," he answered. That could be a really costly cup of coffee for him, and it flies in the face of OpSec that most hackers would employ.

Part 2. Current Activities and Future Plans

RIP Breached.vc, Hello BreachForums!

On September 12, USDoD announced on BreachForums.is (BreachForums) that he was back, and he indicated he would be working on some solo projects. He quickly made headlines again with a post announcing that he was leaking data from 3,200 vendors for aeronautics giant Airbus:

"This month I got access to airbus site using a emploey acces from some turkish airline and this got me inside of alot of stuff plus their vendors data. (sic)

3200 records. It is their entire vendors data," he wrote in a thread on BreachForums.

After providing some sample data and a link, he included this line:

"Lockheed martin, Raytheon and the entire defense contractos I'm coming for you bitchs" (sic)

Neither his post nor that last line went unnoticed. Hudson Rock reported on the breach and leak, claiming they had identified the Turkish airline employee whose credentials had been compromised by an infostealer. Airbus subsequently confirmed their analysis. NOTE: some news outlets seem to have misunderstood USDoD's post and Hudson Rock's reporting. DataBreaches has seen some sites claiming that USDoD infected the employee's computer. He didn't. He simply found the login credentials in infostealer logs and used them. Using infostealer logs is a fast and easy way to find credentials for a target and saves the time of trying to figure out how to gain access. Many forums have sections where such infostealer logs are posted freely for anyone to download and misuse.

"I Am Not Pro-Russia, and I Am NOT a Terrorist, Either!"

Brian Krebs, who had reported on the InfraGard story in 2022, also picked up the Airbus story. In a post headlined, "FBI Hacker Dropped Stolen Airbus Data on 9/11," Krebs wrote, in part:

"USDoD didn't say why they decided to leak the data on the 22nd anniversary of the 9/11 attacks, but there was definitely an aircraft theme to the message that accompanied the leak, which concluded with the words, "Lockheed martin, Raytheon and the entire defense contractos [sic], I'm coming for you [expletive]."

To say that USDoD was upset by Krebs' reporting would be an understatement and he told DataBreaches that he felt like Krebs was calling him a terrorist. USDoD submitted the following statement to DataBreaches and asked that it be included in this article. With only one small typo correction, this is his full response to Krebs' reporting:

Statement About Krebs' Report

First off i would like to apology to every single USA Citzen.

Airbus breaching shouldn't come in 911 but for more than one month I'm out of my usual routine so

Im working more than 20h a day without proper sleep time and this is fucking me off so much that when I breached airbus and leaked i didn't noticed that as 911.

I will never trying get attention or fuck a corp or person in people pain.

It is not who am I. i wasn't raised like that so my truly and honest apology to every single USA Citizen.

It was the first and last time.

Now lets put something right because this shit is not right.

Mr krebs know that almost 1 year ago he approach me to interview about the infragard situation and it is not the first one who asked.

and i told personally to him that I will only speak to him because I have seen his work how very detailed it is his report and I always liked of his work and I even admire him and that is why I talked with him but this guy after the Airbus situation have zero respect for his career or his collogues who work in same sector.

i feel stabbed in the back with that statement from him.

He should contact me. not publishing a lie to get more views.

He as so disrespectful that no one on the media sector fall for his non sense. Dirty move from a dirty fucker and that is why I keep doing my business, for people like this kind of guy.

He will fall from his own acts.

This was a personal attack.

Maybe because he is mad of his friend who work in Alaska not able to catch me.

Both are useless asset from FBI time to put jersey off folks and retire this is not a playground it is real business.

DataBreaches reached out to Krebs with a copy of USDoD's statement to give him an opportunity to provide a response or comment. He did not offer one.

But What Was That Raytheon and Lockheed Warning About?

"Lockheed martin, Raytheon and the entire defense contractos I'm coming for you bitchs (sic)," USDoD had written in his post leaking the Airbus data. Was he serious?

No, he wasn't. USDoD informed DataBreaches that he has no interest in Raytheon and Lockheed and he named them simply to misdirect people while he was pursuing other targets. Those other targets, he says, were Deloitte, NATO, CEPOL, Europol, and Interpol.

"I was happy to have Raytheon and Lockheed spending most of their time and efforts in fixing their issues while I got access to Deloitte, NATO, and CEPOL all in the same day," he told DataBreaches.

NATO? CEPOL? What Was He Doing??

USDoD claims he has targeted a number of entities, including Deloitte, Interpol, Europol, NATO, and CEPOL. He also claims that he has already gained access to some of them and provided DataBreaches with some screenshots as proof.

"I have already accomplished access to NATO and CEPOL, so Phase 1 of operations is finished and now I will pivot to Phase 2. In Phase 2, I will be exploiting that, but I need to study and exploit their weak spots," he says.

USDoD gained access to CEPOL by registering for an account as Greek police officer, "Gran Kolettis" <g.kolettis[at] police[.]gr>. USDoD also sent DataBreaches an email from that email address, showing that he still

had access to that police officer's email account.

Image provided by "USDoD." In the upper right corner, it shows that the user logged in is "GK."

USDoD also provided DataBreaches with screenshots from the NATO Cyber Security Defense Center showing he had successfully registered and had access to them, too. Only someone who has registered and logged in would see the menus displayed in the second screenshot below.

"USDoD's" attempt to register for the NATO portal was successful. Image provided by "USDoD."

Image taken from with portal provided by "USDoD" and redacted by DataBreaches.net.

USDoD gained access by registering as "Karlaina Ustinov" <t.g.papakarmezis[at]army[.]gr>. He also sent DataBreaches an email from that Greek army email account showing he still had access.

But USDoD's plans failed, in part. After accessing the center, he requested access to community services. When he didn't get a reply and tried to login, he found an "under maintenance" notice.

Image provided by "USDoD."

There has now been a maintenance note for the last four days. NATO has not responded to two email inquiries sent to it asking whether the maintenance notice was an unplanned response to some possible cybersecurity incident. Did they detect something and are hardening security? He does not know, but it seems reasonable to think that they may have detected something wrong.

But why was USDoD even publicly revealing his targets if his operations are not really completed?

"This will capture their attention," he told DataBreaches, "and tbh, I want this. I want to beat them while they are watching."

"Why?" DataBreaches asked.
"For the lols. fun. challenge," he answered.

And why these targets? Were there any U.S. defense targets?

What's the Endgame?

After acknowledging that he had failed with Deloitte and needed to find other methods to access them, and after having been unable to access community services in NATO's portal, he started to explain why these targets:

"CEPOL is an Elearning platform for law enforcement from Europe and it is directly associated with Europol. They have plenty of programs together. I got entire access to how CEPOL teaches their agents, so I will find their weak spots for my end game. NATO uses custom and modifed versions of endpoint security and AV. Plus they have their own version of policy, browser, etc. So put both together and I can take them down because I know their methods and I know how they protect themselves. This is enough for me to get more access."

DataBreaches pressed for a more complete roadmap or explanation: "I don't understand when these ops will end or how they will end. Can you explain?"

"Alright," he said, "the end game is an ongoing situation. This is not a country-scaled attack. it is an entire continent attack. Something that I have considered at this point.
I will use their entire resource to increase the size of my operational."

"You know? The door is already opening. It is a golden opportunity. The challenge comes along.
This is the endgame: grow up my influence.
There is no comeback.
I will keep moving forward.
I guess this will clear our confusion:
I crossed the line of point of no return and you asked my end game.

I can't lie to you.
This is the endgame: full control."

"So you have no plans to leak or sell any of the data from CEPOL, NATO, or other agencies?" DataBreaches asked.

"Yes that is right. I will not leak that," he replied. "My intention in getting full control of some system is to get access to even more private data. I want to find more data points and expand my operational and take part of some European critical infra. It is a crucial part of my endgame."

"Let's be clear here," he continued (while DataBreaches prayed for even a little clarity by now): Besides the countries that I will never atttack that I already told you, the rest of around the globe should stay alert."

"Stay alert because you might attack them?" DataBreaches asked.

"That's right. And I'm telling you this because I want to beat them in their max capabilities."

"But what about U.S. defense? You mentioned CEPOL, NATO, EUROPOL, and INTERPOL as targets. Do you have any current operations against any U.S. defense firms or agencies now?"

"Yes I do have some operations going on behind the scene right now," he answered. "But this will never go public or leak anywhere. It is a private request for a private user case. After my contracts end, I will tell you my targets."

When asked if he could say a bit more, he responded:

“I will explain. I entered a new level of data acquisition. My main focus on USA will be military intelligence – every single military intelligence info from classified to private ones.”

“This is for a private user contract or just for your own interest/challenge?” DataBreaches asked.

“My own use case,” he answered. I’m building a new private company solely run by myself. I will be selling military intelligence on the dark web. After Breached was seized, I always thought to run my own business.”

“So you will sell intel?” DataBreaches asked.

“Yes, from classified to private intel. This is related to European endpoint. I need European endpoints for this. This will not run only on USA. I can even give you a name. My first target will be Constellis.”

Once again, it seems, USDoD is throwing down a gauntlet – announcing his target and plans. DataBreaches had never heard of Constellis, but hopes they have good defenses against his social engineering tactics and use of infostealer logs or their information may become his first offering on his new business when it opens.

And Then There’s BreachForums

USDoD announced his return on BreachForums and it seems that in addition to having a business plan involving the acquisition and sale of intel, he also wants to help BreachForums grow.

“I want to see the community get more engaged like it used to be. Having someone who’s active and engaged can bring more people. ShinyHunters used to do that for RaidForums. He was and still is a beast and a legend, but he is not really involved in the forum he now owns. Everyone keeps waiting for him and he doesn’t seem really interested in the forum.”

USDoD had a very high positive reputation on Breached.vc, and almost certainly will have one again on Breach Forums. And he engages in activities that will likely bring media attention and interest to the forum. He tells DataBreaches that he was disappointed when he reached out to ShinyHunters this week to offer his help and Shiny said “no” without any explanation and without saying that Shiny would do anything himself.

What Next?

It was difficult to get a clear understanding of what USDoD is doing and what he plans to do, but it seems clearer now that he has a business model involving U.S. military intel. Should defense contractors and agencies remain vigilant about him? Given how skilled he is at social engineering and how he loves a challenge, it would seem wise to keep an eye out for him.
