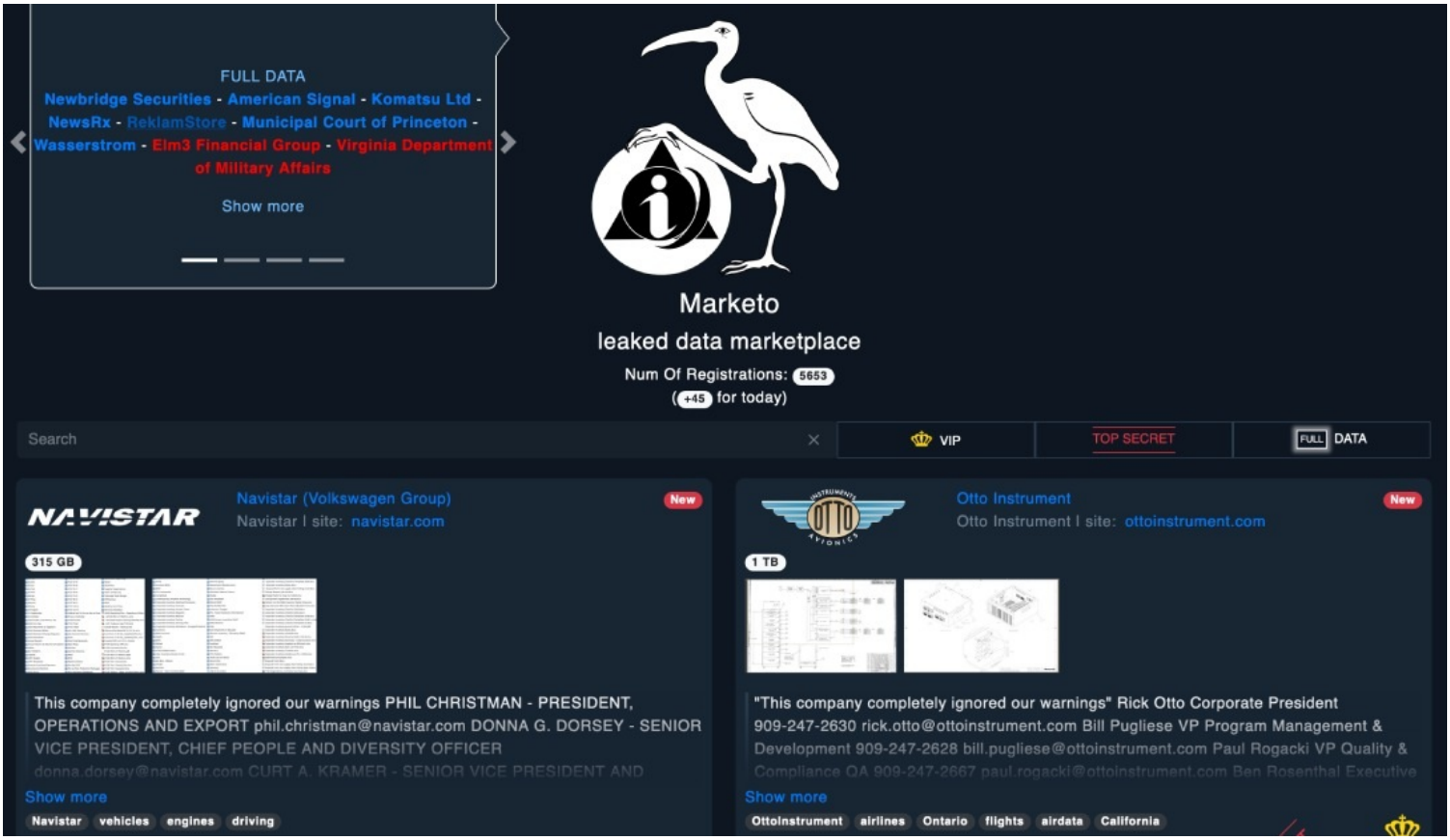


Dmitry Smilyanets | September 17, 2021

# 'Yes, we are breaking the law:' An interview with the operator of a marketplace for stolen data

Cybercrime News

**Editor's Note:** A website called Marketo emerged earlier this year, billing itself as a marketplace where people can buy leaked data. Although Marketo isn't a ransomware group, it appears to borrow key strategies from those types of threat actors.

In late August, the group wrote that it was selling confidential data from Japanese tech firm Fujitsu. Earlier this month, reports emerged that data stolen from the Virginia Department of Military Affairs was available for purchase on the site. But the group's extortion efforts have gone further than many ransomware operators—they reportedly reach out to their victim's competitors and law enforcement to pressure organizations into paying for the data.

Although it's unclear how Marketo fits into the broader cybercrime ecosystem, Recorded Future's Insikt Group recently identified that the same victim was announced on both the Conti ransomware extortion blog and Marketo—the Conti ransomware gang threatens their victims with "other ways" to monetize stolen data, which may include selling it to the highest bidder.

Recorded Future expert threat intelligence analyst Dmitry Smilyanets spoke to a Marketo representative this month about the group's tactics and approach to breaking the law. The interview was conducted in English and has been lightly edited for clarity.

**Dmitry Smilyanets: You call Marketo a leaked data marketplace—what makes you different from multiple ransomware families who operate extortion blogs?**

**Mannus Gott (Marketo):** Our radical difference is that we are not a ransomware group. Besides, we are the first in this industry who started working by the "no to ransomware, yes to audit" scheme. Apart from profit, we are driven by what is called "true hacking"—the search for knowledge, unusual moves and decisions, a search for elegant solutions, advancing technical progress, and developing the information security sphere. In our activity, there is, apart from the profit, human thought, and morale—the seeking of knowledge and securing data of people, who trust it to the megacorps and companies, the only target of which is profit at all cost. We are for the safety of the data and we draw attention to that matter, even though it's radical. We are passionate and spend all our time on that, that's why the cost is corresponding. You can see it is all in our manifest, in our rules and actions, we are actually first in that too. Same as the media—we are the first ones to create official representatives. By the way, there soon will be official representatives in other protected networks, like ZeroNet, FreeNet, Mastodon and etc.

**DS: Researchers have compared you to the pioneers of ransomware extortion. The Dark Overlord. Are you affiliated with that threat actor in any way?**

**DS: Researchers have compared you to the pioneer of cyber extortion, TheDarkOverlord. Are you affiliated with that threat actor in any way?**

**Marketo:** We are aware of the actions of that group and we are flattered by the comparison. However, we have nothing in common with them and we do not know each other. Actually, perhaps, someday we'll meet. You never can tell.

**DS: How old were you when you got involved in cybercrime? Are you a hacker yourself?**

**Marketo:** Now that's an interesting question. I can't tell you my age, nor can I tell you the date when I joined the market. This will lead to my deanonymization. It is much more interesting to talk with a person without a face—a person in a mask. And, how do you define "hacker?" The etymology of this word means a search for an optimal, unusual solution, which means technical creativity. Hacker is not necessarily a criminal, but a criminal can be a hacker. Such a criminal should be called a "cracker." Hacker is the one who has the spirit of hacking, the spirit of learning, and the elegance of the IT industry. At some point, journalists didn't want to use the unconventional word "cracker." Then yes, I am a hacker, but that doesn't mean that I'm personally participating in an attack or something else. I can be the face for the media, I can participate in attacks, or I can do nothing at all—but I will remain a hacker. So let's use the right nomenclature, would you agree?

**DS: Is Marketo a group of people, or is it operated by you alone? Do you operate the blog and sell the data stolen by third-party hackers?**

**Marketo:** Back to the anonymity questions, I can confirm that I can't disclose the structure of our organization and Marketo as a project. As you've stated, we are pioneers in our field. And as I've said before, we—meaning that we are a group of people. We are the force, advancing the progress. My name is Legion, for we are many. Marketo is not the blog, it's a marketplace. The buyer of data could be absolutely anyone. However, our priority is always the victim.

**DS: You mention several federal agencies as your "partners." What does this partnership look like? Why don't you mention the FBI?**

**Marketo:** We mark as partners those who we provide with weekly reports about [hacked] companies with proof. In these reports, there is everyone who decides not to work with us. That's how we make sure that they are punished for not having the initiative and for not bothering about the security of the data of their employees and clients, partners, and suppliers. Despite the fact that we are advancing the progress, at the end of the day we must pay our bills. That's why the company either becomes our advertisement, cooperates, and pays up, or their data is sold. We wrote about it in our manifest, by the way.

IMAGE: MARKETO

**DS: In your code of conduct, you stated that some parts of "critical data" will not be published or sold. What will happen to that data? Why did you create that code in the first place?**

**Marketo:** Perhaps you misunderstood what we meant. We sell the data, as we said in the manifest, first to the company itself. If the company does not buy back the data, it is sold to those who are willing to pay. The data is sent only to the buyer and we do not publish it. The rest of the critical data, that is stated as unsold, will be released in 100% of cases when organizations don't pay for our work. That is actually an information security audit. And part of the data is published right away as proof. That's how we work.

The manifest itself was created to answer frequently asked questions and to show that we have principles and we will follow them in any situation. Our manifest covers almost all scenarios and demonstrates our actions. Later we will add the proofs and results of each scenario, something like a business offer, so everyone will see how we work. If, of course, the team will decide to do so. We are for transparency, we are providing services, although by force. That's our position.

> "In the US, people like to insure but not to defend."
>
> **— Mannus Gott (Marketo)**

**DS: You labeled some leaks as "Top Secret." How do you make those calls? Does any of the stolen data carry the classified status?**

**Marketo:** Here we can have discourse. Imagine, in the data, there are blueprints that have a mark—it is secret, it is a property of some company and cannot be disclosed to the third parties, it is a trade secret. In those cases, the data will be marked as top-secret.

On the other hand, even if the blueprint doesn't have the classified status, we analyze data and make conclusions. For example, a company managed to lose data of onboard electronics for the F-16 Fighting Falcon and a blueprint of the hard wing of the B-2 Spirit bomber. Of course, this is secret data. Such blueprints we have from many other companies [redacted] who also have secret data.

Despite that, companies are managing to ignore us for 1-2 months and some even said "fuck you" without even thinking about the safety of the citizens and their countries.

**DS: How much money have you made since you started in April? What is the most expensive data you sold?**

**Marketo:** Unfortunately, this is far beyond my authority and against our confidentiality policies. We are not an IT company and we are not publishing financial reports. Besides, we guarantee to all companies the privacy of negotiations and destruction of data upon agreement.

**DS: You called DarkSide and their statements "disgusting" because "they should know what they are doing." Do you? How do you classify your own standings with the law?**

**Marketo:** You've misunderstood me. We didn't call them disgusting, but their actions are. And there is one simple reason: they attack critical infrastructure, which can lead to hunger, riots, and even civil war. We do not support such actions. We aim to develop the economies of the countries, to force them to invest in information security, to advance it to the next level. The same goes for companies. We are not interested in the destruction of the

economies of any county, we do not pursue any political cause. We are enthusiasts. Yes, we are breaking the law. But we never trade human life.

**DS: Are you financially motivated only or is there a political/hacktivist side to this operation?**

**Marketo:** I think I've made it clear that we have principles and we support hacking in its primal meaning, but we do not pursue any political cause.

**DS: How do you choose targets?**

**Marketo:** Consider it a trade secret—I can't disclose this.

**DS: What are the most interesting leaks that you've seen elsewhere? What is your inspiration?**

**Marketo:** Hard to pick the most interesting. The most astounding cases I've pretty much covered in the previous answer. They would probably be the most interesting. My inspiration—learn something new. Search of knowledge, elegant and simple solutions.

**DS: Why are most of your victims based in the US? Why is Asia, South America, etc virtually not present at all?**

**Marketo:** The US seems like a promising country for developing information security. The agile legal system, fast decisions, worldwide known technology development centers. Remember the history—the internet was born by the US Department of Defense and its ARPANET project. But that does not mean that there wouldn't be targets from all around the globe. This is nothing but a coincidence. In the US, people like to insure but not to defend, that's it.

**DS: Tell me a secret, who is your next target?**

**Marketo:** You can look at the banner on our site. Everything else is a surprise, otherwise, it wouldn't be that interesting, would it?

Tags data breach Marketo

Mission-driven and Russian-speaking intelligence analyst with type A personality. Dmitry has twenty years of experience and expertise in cybercrime activity that includes being a former member of an elite Russian-based hacking organization.

Previous article Next article

## BRIEFS