THE MOST RESOURSEFUL HACKERS' ATTACK IN THE USA

Kupratsevich A. I.

Belarusian State University of Informatics and Radioelectronics Minsk, Republic of Belarus

Karpik L. S. – Lecturer

Annotation. A short survey about the largest hackers' attack in the history of the United States: it took place due to the rapid development of information technology and the imperfection in the system.

Keywords. Black hat, hacker, carder, rogue, accomplice, programming, FBI, resale.

Each business organization tries to increase its profit in every possible way, to achieve this goal the latest achievements of science and technology are used. Information technologies are highly employed in commerce, banking industry, internet stores, etc. Due to such innovations, such things as online money transfers and making online purchases have become real.

Unfortunately, in the pursuit of adding new user features and improving the already available features, many organizations do not bother about such things as protecting their customers' data. Russian hackers Dmitry Smilyanets and Vladimir Drinkman seized such an opportunity of making a fortune stealing credit card data and reselling them.

The future accomplices met in 2003 in a computer game; even then Smilyanets liked to cheat, using programs that gave him advantages over other players.

Drinkman spent his childhood in Syktyvkar, was interested in computers science since his studying at school, learned the C++ programming language without anyone's help and got a job as a system administrator at the university. Smilyanets grew up in Moscow, where he studied at the Faculty of Information Security at Bauman University.

The criminal case says that since 2005, the friends began to break into the computer networks of financial companies, payment systems and stores, gaining access to bank card data. Dmitry Smilyanets was also engaged in their sale: the cost of cards was from 10 to 50 dollars per unit. It depended on the country where the credit card was issued. The accomplices infiltrated the NASDAQ stock exchange, 7-Eleven supermarkets, the French Carrefour chain and other large companies. A team of hackers from Russia infected computers with a specially created virus "GOZI". Over the next ten years, they allegedly

stole about 160 million credit cards and caused $ 300 million damage. Another well-known hacker, Alberto Gonzalez, pointed out Drinkman's trail to the US intelligent services, and due to Vladimir, they learned about Smilyanets [1].

The arrest of the cybercriminals duo was quite unusual: the FBI was preparing an operation to capture the largest gang of carders in history for two years. To do this, the special services created a website for scammers in the Darknet, where users from all over the world could anonymously share tips on credit card fraud. This platform recorded all the information that entered by visitors, and after collecting enough evidence, on June 26, 2012, the FBI conducted a large-scale operation to detain carders around the world.

Despite the detentions, on June 27, Dmitry Smilyanets published his photo with the inscription "I Amsterdam" (located on the territory of the airport of the capital of the Netherlands) in social networks. American intelligence agencies immediately contacted the Dutch, and Smilyanets was detained. A few hours later, the police found Vladimir Drinkman in one of the rooms of a nearby hotel.

But how were the responsibilities distributed in a group organized by rogue friends? Drinkman and several other Russian hackers were known to have stolen bank card information by hacking online stores, and Smilyanets profited from this information by selling it to smaller organizations, which, in turn, continued the chain by collaborating with individual carders. The system was so fine-tuned that Dmitry's regular customers even had discounts, and, as the secret service investigator D. Repper says, Dmitry Smilyanets at some point accounted for more than 50% of the turnover of stolen payment card details on our entire planet [2].

Initially, Smilyanets and Drinkman faced 25 and 35 years in prison respectively, but in 2015, both pleaded guilty, and Dmitry even went to cooperate with the FBI. The sentencing was constantly postponed, and only in 2018, everything became known: Smilyanets was sentenced to 4.5 years, and Drinkman – to 12 years. By that time the accomplices had already spent almost 6 years in prison, Dmitry Smilyanets was released in the courtroom [1].

Now Smilyanets is officially listed as an information security expert in the United States and intensively pays off a debt of $ 300 million. Vladimir Drinkman continues to serve his sentence.

Unfortunately, there is quite a number of cases of Internet fraud, and in order not to become a victim of such an incident, let us specify a few security rules one should follow while working on the network:

1. Organizations that have access to your data must be reliable. Therefore, choose only those companies that have an excellent reputation and are constantly developing in this area.

2. Enter your data only on official secure sites. Often scammers counterfeit them, so you need to carefully monitor the sites addresses, in particular, the domain.

3. If you receive a call from a person who introduces himself as a bank employee and asks you to perform some actions -- end the call and make a call back to the number that you will find on the official website of your bank.

References:

1. Смелый и другие главные киберпреступники планеты Даниил Туровский рассказывает, как спецслужбы США охотятся за российскими хакерами — Meduza [Electronic resource] – Access mode: https://meduza.io/feature/2017/09/15/psih-smelyy-i-drugie-glavnye-kiberprestupniki-planety – Date of access: 19.04.2021.

2. ХАКЕР который НЕ СМОГ / Тёмная история Димы Смелого и Moscow Five – [Electronic resource] – Access mode: https://www.youtube.com/watch?v=z85fT79bQ10 – Date of access: 19.04.2021.