The Toyota subsidiary lost $ 37 million just after an online fraud campaign

Toyota Boshoku has confirmed the loss of more than 37 million dollars after becoming the victim of an online email fraud attack campaign.

Toyota Boshoku, a member company specializing in the production of car components of Toyota Motor Corporation of Japan, recently confirmed the loss of more than 37 million dollars after the company became victim of an online email fraud (BEC scam) campaign.

The parent company Toyota also mentioned in a previously published press release about "a case of fraud involving fraudulent payment activities from a malicious third party, resulting in financial losses. serious for our European-based subsidiary ".

Toyota Boshoku is a subsidiary of Japan Toyota Motor Corporation

This cyber security incident occurred on August 14, and the initial anticipated financial loss was a maximum of about 4 billion yen (as of September 5), equivalent to $ 37,472,000. (approximately 33,904,000 euros).

1. French police successfully cracked down on a botnet that exploits 850,000 computers from more than 100 countries.

Detailed information about security incidents has been recorded by the authorities

After discovering this dangerous fraud incident, Toyota Boshoku almost immediately started an investigation with the assistance of a number of legal experts, then reported the entire situation to the authorities. local as well as relevant authorities.

'We are committed to cooperating fully in all aspects of the investigation, and at the same time implementing the necessary measures to implement the procedures for securing / recovering leaked funds, minimizing Most of the negative effects on production activities as well as not causing any inconvenience to partners, and especially customers, " Toyota Boshoku representative said in a press release today. 8.9 past.

1. Overview of building an enterprise security detection and feedback system

Production activities of Toyota Boshoku were not affected by the new scam attack

Further details of the ongoing investigation remain unpublished, along with Toyota Boshoku's plans to "disclose any amendments to the earnings forecast published in March 2020 if the incident occurs." this makes that modification necessary. "

This serious incident occurred less than 6 months after another security breach occurred in March that also affected about 3.1 million Toyota customers worldwide. The breach occurred in the Japanese automaker's database, causing customers' personal information to leak, causing privacy and personal privacy concerns.

In February of this year, Toyota Vietnam also had to issue an urgent message confirming that the company's computer system was hacked and could have unauthorized access to some customer data. in Viet Nam. The leaked data warehouse included information about individuals, partners and customers of Toyota with hundreds of thousands of records.

1. Honda database leaked, revealed many "fatal" weaknesses in the intranet system

Toyota Vietnam was attacked by hackers, illegally accessing the internal database

Earlier, the network of Toyota dealers in Australia also became the victim of a localized cyber attack, resulting in the company's IT system completely numb on February 19.

BEC scam - a new but effective method of fraud

Business Email Compromise (BEC), sometimes known as Email Account Compromise (EAC), is a scam cybercriminals, those who try to deceive one or more employees of an organization, with the ultimate goal of making these employees transfer the money of the business to the bank account in their name.

This type of attack has been around for a long time, almost paralleling the development and popularity of email. However, it has never been 'hot' because the success rate is always high. This stems from the fact that crooks always know how to set a problem and target key locations of the business. The most common scenario is to pretend to be a trusted business partner or even the CEO of a company to gain the victim's trust.

1. Alarming statistics on the situation of cyber security in our country in the first half of 2019

BEC scam is an online scam through email and targeting businesses

BEC is one of the most common frauds in the internet world, with reports almost being recorded day by day, hour by hour. Fortunately, there have been many victims of this fraud method have regained part or even all of the money lost by quickly freezing accounts before the fraudsters promptly transferred money. out of that account. Such as the case of Portland Public Schools, Oregon, USA. The school has recovered almost all of the $ 2.9 million after falling victim to a BEC attack in August.

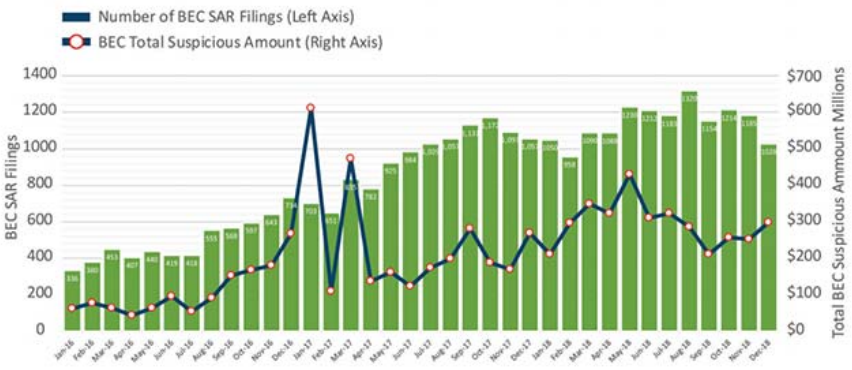
However, most other victims are not so lucky. Often, only a small part of the lost money can be recovered with great success, while many cases of losing acceptance because the necessary measures were not taken immediately after the "disaster" happened.

1. Crypto theft and fraud in 2019 could hit a record of $ 4.3 billion

According to the annual Internet Crime report released by the FBI's Internet Crime Complaint Center (IC3) in April 2019, in the US alone in 2018, the BEC scam caused more than $ 1.2 billion in damages.

Another statistic conducted by the Financial Crimes Enforcement Network (FinCEN) shows that the damage caused by BEC scam has increased from an average of $ 110 million a month in 2016 to over $ 301 million. every month in 2018. Thus, despite the fact that advanced security measures are being launched every hour, every minute, BEC fraud is still one of the top concerns for every business today.

1. Awareness and experience - the most important factor in all network security processes



The amount of damage caused by BEC scam monthly has almost doubled from 2016 to 2018

In order to minimize the risk of their employees becoming victims of BEC attacks, organizations and businesses are required to adhere to the strict security procedures of network security service providers and tighten them. checking and verifying all changes to payment information through a variety of verification processes, including but not limited to meetings or direct phone calls to authenticate when there is any behavior. Modify which payment information is detected on the system.

The fight against online frauds is still very demanding and does not promise an end.