ENGLISH TRANSCRIPT OF VOICE OF AMERICA VIDEO

8b0466f5-9483-4516-9649-6f5b798e819b.mp4

https://www.golosameriki.com/a/cyber-security-colonial-pipeline/5890953.html

Атака на Colonial Pipeline

Как вирус-вымогатель остановил ключевой трубопровод?

How did the ransomware virus stop a key pipeline?

Speaker1 (Daria Dieguts): [00:00:00] Not the norm, but far from being news, strategic infrastructure facilities in the U.S. regularly suffer from colony-wide hacking attacks. the largest supplier of petroleum products in the u.s. accounting for %80 of fuel consumption on the east coast has been hit by the so-called ransomware virus. cybercriminals cyber group Darkside allegedly from eastern europe gained control of the company's system demanded a ransom for resuming operations. is one of the easiest cybercriminal schemes out there. but the energy giant's falling into a primitive trap didn't surprise experts.

Speaker2: [00:00:37] The surprise was that it didn't happen sooner. The U.S. energy system is in many ways unique in that it is virtually all privately owned. Not only does the state not control it, but it doesn't regulate it very much either. there are 385 facilities in the U.S. energy sector and about 385 private companies that manage them. they all have different levels of security. the colony turned out to be one of the companies that couldn't defend itself.

Speaker1: [00:01:07] Such a structure creates additional opportunities for cyber criminals to improve their techniques day by day. energy infrastructure is under attack

around the world, from a pipeline bombing in turkey in 2008 to an attack on energy companies in ukraine in 2015. At the same time, experts note that not only the approach but also the goals are changing. and the line between foreign intelligence agencies and groups pursuing purely financial gain is blurring.

Speaker3 (Madnick): [00:01:35] We're talking about a system perhaps even more diverse than the arms trade. there are two main categories: First, people who create cyber weapons. it's happening all over the world. but most of it is in eastern Europe. The second category is the so-called businessmen. they buy the weapons they need for the planned attack. in other words, you don't have to be an advanced programmer at all to carry out a ransomware attack only costs about $1,400.

Speaker1: [00:02:03] According to Stuart, however, energy infrastructure facilities are particularly vulnerable because of the relative newness of the attacks, coupled with the obsolescence and technology at the facilities. Under such conditions it is impossible to develop a perfect security system, however, the usual carelessness of employees is often the cause of attacks, ranging from bringing personal computers to work to insecure passwords.

Speaker3 (Madnick): [00:02:26] You may live in a bad neighborhood, so it is not wise to leave the door wide open. there are many basic cyber hygiene rules that many companies do not adhere to. Also a ransomware attack usually does not come instantly. There is a series of steps to get into the system and infect it. One of our studies showed that on average a cyber attack lasts for two hundred days before it is detected.

Speaker1: [00:02:51] Strengthening cooperation between the private and public sector is another important aspect of preventing such attacks. The day before, President Joe Biden signed an executive order aimed at enhancing cybersecurity of strategic assets through a partnership between private companies and the federal government.
Daria is currently in America. Washington.