The need for OT security revealed **after the cyber-attack to the pipeline**

Colonial Pipeline became the victim of a ransomware on May 8th, and as a result, all operations had to be stopped. Eray Atlas from OTD Bilisim said that: "The attack against Colonial Pipeline points out to the closure of fuel pipeline and need for increased OT security."

One of the biggest fuel pipelines in USA, Colonial Pipeline was exposed to a ransomware attack on May 8, and had to stop all operations. The attack committed against Colonial Pipeline where nearly the half of the petrol and gas in East Coast is obtained is the latest example showing why cyber attackers target petrol and gas industries.

COLONIAL PIPELINE, SUBJECT OF RANSOMWARE

According to the report of The Wall Street Journal, Colonial Pipeline, the biggest gas pipeline operator of USA had to sop its operations on May 7 because of a ransomware attack. Cyber criminals are not only threatening to wreak havoc on energy markets but also disrupting gas and diesel supplies on the East Coast. Colonial Pipeline serves as an important gateway for the east half of the USA The pipeline is one of the main sources of gasoline, diesel and jet fuel for the East Coast with its capacity nearly 4 million barrels per day. They published a statement stating that they were the victims of a ransomware attack which affected corporate IT networks as well, on Saturday. The attack was not carried out on operational networks controlling the pipelines and distributing fuel, separate from the corporate network. Colonial Pipeline announced to have closed the pipelines as a precaution to prevent the spread of the attack. The first opinion of many people in the security industry was that the attack was carried out by a foreign government. However, Bloomberg presented a report stating that the attack was led by a ransomware group named DarkSide on May 8. Known for its "double extortion" plans, DarkSide obtained almost 100 gigabytes of data from the Colonial network on Thursday in two hours. The attackers threatened the Colonial Pipeline data they had stolen to Internet and to lock the network of Colonial by encrypting them to the attackers' computers unless the demanded ransom is paid. It is not known how much money the cyber criminals demand or how they use the networks. But what is pretty obvious that this attack is the tangible indicator that cyber criminals are focused on industrial organizations regardless of the scale or sector of the attack.

ATTRACTING TARGET: PETROL AND GAS INDUSTRY

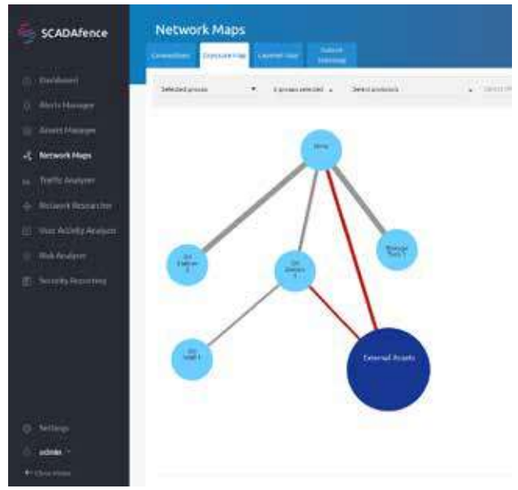
Petrol and gas industry has become a critical importance for global and national economies over years, and therefore, it has become one of the strongest and economically-global industries. Since the competitors deem such industries as valuable targets to exploit Industrial Control Systems (ICS) vulnerabilities, it has been seen as a bit target.

The operational technology (OT) in petrol and gas operations was isolated and air gapped; however, in today's world, operational technology networks provide more frequent connections to different IT structures, Internet that pave the way for new attacks. The convergence of OT and IT environments in oil petrol and gas operations has caused the emergence of endless number of vulnerabilities in both IT and OT environments. Besides, there are some ongoing and growing priorities focused on compliance and risks arising from Internet of Things (IoT) devices. As seen in the recent attacks committed against gas and petrol organizations such as Pemex and Colonial Pipeline, attackers have many advantages varying from understanding different behaviors to how to use organizations. Therefore, it is a necessity for petrol and gas organizations to be protected against any cyber-attacks in order to prevent the global economy and civil security from being affected by any attack.

PROTECTION OF PETROL AND GAS OPERATIONS

Even though the details regarding how competitors successfully exploited corporate networks in the Colonial Pipeline attack have not been made public, it pointed out that it is high time for gas and petrol organizations to implement a strong OT security strategy. The NSA published a report the last month to underline the importance of protecting industrial control systems (ICS) and operational technology (OT) against cyberattacks. In the report, NSA stated that: "Unless a direct action is taken to make OT networks and control systems resilient to vulnerabilities through IT and business network intrusions, OT system owners and operators will remain at untenable risk levels." Additionally, the NSA report expressed that the organizations and operators must protect the critical operations. "OT systems rarely require external connectivity to function properly. However, they frequently provide connection for convenience without considering the actual risk and potential adverse job and task outcomes. To take action without losing time might help to develop cyber security and become ready for the task." Before publishing this report covering its suggestions as well, NSA In the last seven years, SCADAfence has been cooperating with many critical infrastructure organizations including the petrol and gas operators in order to ensure the security of OT networks and implementation of appropriate cyber security infrastructure. To do so, it provides full network visibility and directly detects any abnormal activity and malicious behavior including the abnormalities arising from ransomware attacks.

SCADAfence works in cooperation with many critical infrastructure organizations including petrol and gas operators in order to ensure the safety and security of OT networks and implementation of appropriate cyber security infrastructure.



OIL SAMPLE CHART IN APPLICATION

The chart above shows how SCADAfence helps organizations in the Petrol & Gas and pipeline industries have full visibility across their IT and OT networks. In this way, the location of attack vectors can be detected and all connections among the networks can be defined with full accuracy. This approach has ensured for hundreds of organizations to reduce the abnormal activities which might turn into a cyber-attack later in their operational networks.

FAILED TO PLAN = PLAN TO FAIL IN THE OPERATIONAL TECHNOLOGY WORLD

Basic cyber security application might help to prevent the development of these attacks, which includes making the whole network visible since it is difficult to protect what we cannot see. Furthermore, it covers the micro segmentation process, and constant network monitoring activity is of great importance to prevent the emergence of similar attacks. Numerous petrol and gas operators use continuous network monitoring and threat detection technologies to provide visibility for their OT networks and keep critical infrastructure networks secure. Through this holistic approach for network monitoring, anomaly detection, remote access visibility and compliance, many oil and gas companies have reduced the risk level against future attacks by 95%. The best aspect of this is that such solutions are tool-free, non-intrusive, and capable of performing the tasks at a fraction of the cost of personnel. If you need to secure the industrial networks of our organizations, the only thing you need is to download our case study conducted with 100 Petrol and Gas Industry Leaders to find out how SCADAfence provides full visibility into OT networks and performs real-time threat detection of malicious activity. We would be very happy to help you if you want to try SCADAfence platform and reveal all vulnerabilities in your OT network. If you want to try SCADAfence Platform and find out all vulnerabilities in your OT network, we'd be very pleased to help you. For detailed information about the products and PoC Request, please visit "https://onlineteknikdestek.-com/Pocrequest?culture=tr" For detailed information about the event and product, you can get into contact with OTD BILISIM sales team.