Recommendations Following the Colonial Pipeline Cyber Attack

By Mike Hoffman

Published: 2021-05-12 · Archived: 2026-04-10 02:19:11 UTC

On May 7th, public reporting emerged about Colonial Pipeline operations being impacted by a ransomware incident in their IT environment, and then operators temporarily halted OT operations as a precaution. Like any pipeline, Dragos would expect Colonial Pipeline to have so many dependencies between their control and SCADA systems into their business systems that it becomes hard to reasonably delineate and separate. With this in mind, out of an abundance of caution, halting operations becomes the safest choice.

Colonial Pipeline is a midstream Oil and Natural Gas (ONG) pipeline and storage company based in Alpharetta, Georgia, USA that transfers refined petroleum products between downstream refining facilities to storage sites and handling transfer from upstream production sites to downstream refining facilities for a large majority of the United States.

This blog is intended to share what is known about the Colonial Pipeline cyber attack, offer a perspective of what subsystems can be found and what operations occur within pipelines to those unfamiliar, and offer recommendations to asset owners based on similar ransomware cases Dragos has worked in OT networks, including from the same group, DarkSide.

DarkSide and Ransomware Outlook

On Sunday, May 9th Dragos released an intel report to our customers that assessed with high confidence that the DarkSide ransomware group was responsible for the IT compromise. During the past year, various manufacturing industries have reported similar incidents and have attributed them to other ransomware groups such as REvil, and CL0P. The recent pattern of ransomware incidents encrypts filesystems and steals either confidential information or Personally Identifiable Information (PII) from the organizations and threatens to post the information on dedicated leak sites (DLS) unless the ransom is paid in a timely manner. During the past year, Dragos has observed several instances of this happening in multiple industrial sectors, including against the major vendor and asset operator, Honeywell. No industry has been immune to this with numerous cases taking place in manufacturing as well as electric power sectors. However, the Colonial Pipeline cyber attack is the most disruptive incident Dragos has witnessed on US energy infrastructure from cyber intrusions.

DarkSide, and many other ransomware groups, are opportunistic. They find soft targets, evaluate if they are a strong candidate to ransom, and then they attack.

Unfortunately, this applies to many industrial companies. These groups rely on weak passwords via unsecured internet exposed services such as Remote Desktop Protocol or exploits against a vulnerable version of common internet-facing devices. Numerous vulnerabilities have been released over the past year for these types of devices to include **Pulse Connect Secure**, **Fortinet FortiOS**, and **Accellion FTA** devices. Once initial access is achieved, they quickly bring in tools focused on gaining Domain Administrator access to enable them to then deliver their

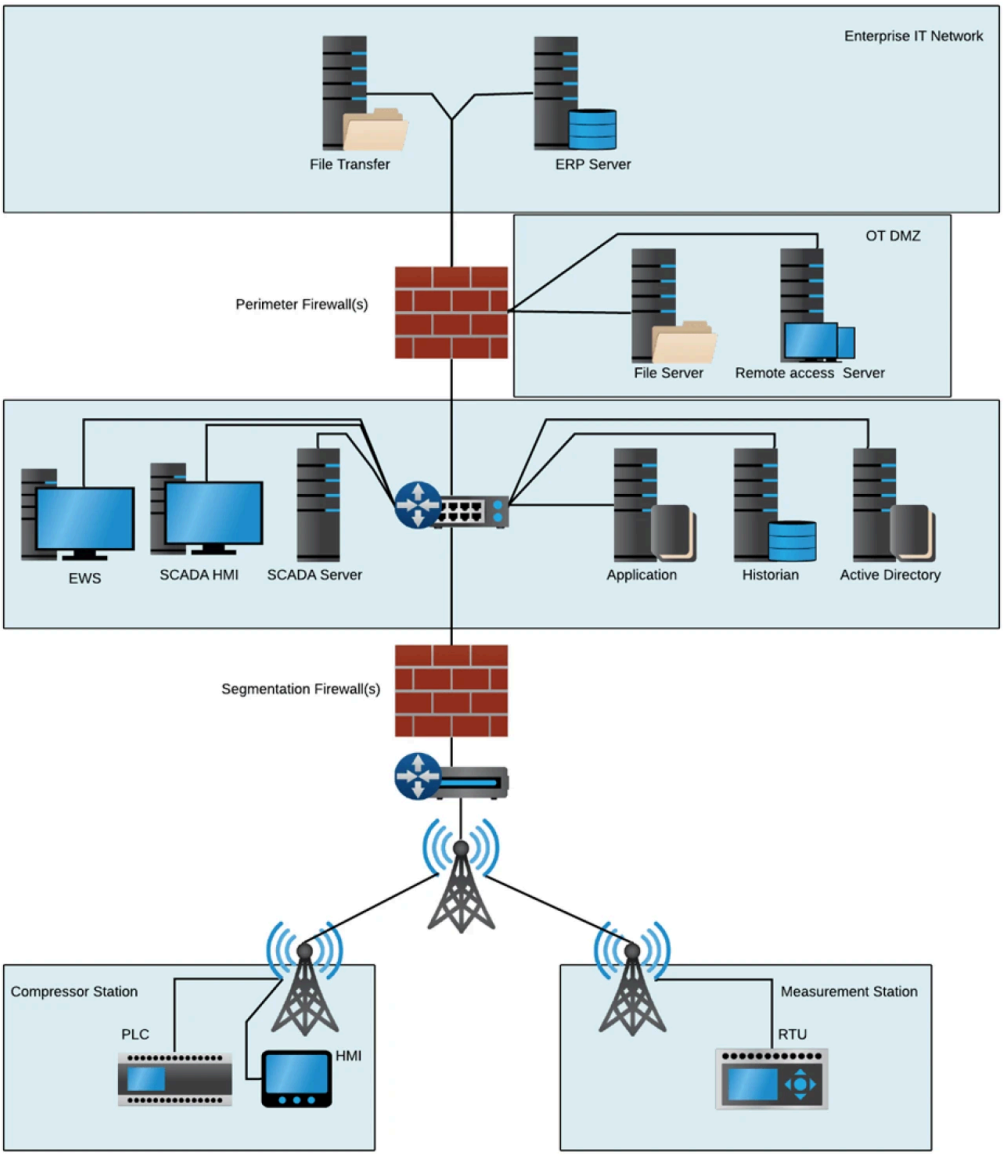
ransomware. Dragos response teams have observed this initial access to the deployment of ransomware ranging widely with ransomware delivered as quickly as 24 hours from initial access while in other cases several months before the group deploys their ransomware payload. In our incident response cases and assessments, Dragos often finds shared credential management between IT and OT networks such as connected Domain Controllers as a mechanism to impact OT.

How a Strong Architecture Can Support Response Efforts

Although this attack was carried out on the Enterprise network, it brings to light the highly interconnected nature of OT operations that businesses must consider. Many organizations feel they have highly segmented OT networks to include their industrial control systems (ICS). However, in Dragos's assessments and cases, we find this to not be the case. It is common to hear about pending IT-OT convergence, but in reality, much of that convergence took place a decade ago, and the preventative controls, such as segmentation, that the organizations had in place have atrophied over time through misconfigurations, additional devices, or just the nature of needing increased connectivity for the business. What the industry is experiencing now is the digital transformation of our infrastructure, which is resulting in hyper-connectivity not only to the corporate IT networks but also personnel, vendors, integrators, original equipment manufacturers, and cloud resources.

Responding to ransomware attacks in the OT environment is even more challenging due to the overall lack of network monitoring and host-and-network based logging. At a minimum, crown jewels, which are the most critical assets in operational systems, should be actively monitored. When preventative measures fail or atrophy over time, asset owners and operators are often at the mercy of discovering the incident only after the malware has executed and run its course, encrypting systems and taking them offline. Unfortunately, during incident response engagements, Dragos has found that many companies have little visibility into the operations and production networks. This slows down incident response and removes options from the company on what they can do to blunt the incident. Those organizations that are proactive and develop consistent insights using frameworks such as the collection management framework are able to know what the most relevant logs are, where they are stored, and how long they are available. These simple types of actions rapidly increase the ability to respond to incidents. Often in incident response cases, almost nothing is available.

Complete segmentation is often impractical, but a defensible architecture can still be maintained that significantly reduces risk and makes the response more effective. As shown in **Figure 1** below, SCADA systems should be architected in such a way as to provide communications segmentation and disconnection points in case of an attack. Limit what protocols communicate through this segmentation, as ransomware groups will use protocols such as remote desktop (RDP), windows file sharing (SMB), and Active Directory authentication (NTLM) to move from one zone into another.



With network monitoring and visibility in place, a defender could view malicious traffic coming into the DMZ and begin changing the environment or disconnecting the systems from the outside world. Next, defenders will want to ensure monitoring is taking place down in the SCADA server to identify changes to outstation communications or at the application server to identify if configurations or modifications are occurring. Project files at the Engineering Workstation (EWS) are also a valued target that needs monitoring, protection, and offline backups as they often contain programs and configurations of the SCADA itself or those of remote PLC and RTU devices.

Continuing this example, if remote polling and operational visualizations systems are compromised, the next isolation point is around the communications out to remote pipeline pump and metering stations. Isolating here ensures local systems are kept operational, and control is still possible. If we made it to this point, remote teams would be activated and sent to the remote locations. This is difficult to achieve in a reduced workforce setting

common among highly automated environments. Each of these scenarios needs to be discussed and documented in OT incident response plans and regularly exercised.

Again, this is a best-case response scenario with many fallback options. Many of our responses are instead based on loosely segmented networks or networks with no segmentation at all.

Mike Hoffman is a Principal Industrial Consultant at the industrial cybersecurity company Dragos, Inc., where he serves as the primary subject matter expert with customers to perform architecture assessments, network vulnerability assessments, consequence driven modeling, etc. of their industrial environment. Before joining Dragos, Mike was a global Principal ICS Security Engineer at Shell and held the role of ICS Security SME across the Americas region. Among his 20 years working at Shell, he also held the positions of ICS Security Specialist, Controls & Automation Specialist, Process & Environmental Analyzer Specialist, and Instrumentation & Electrical Technician.
