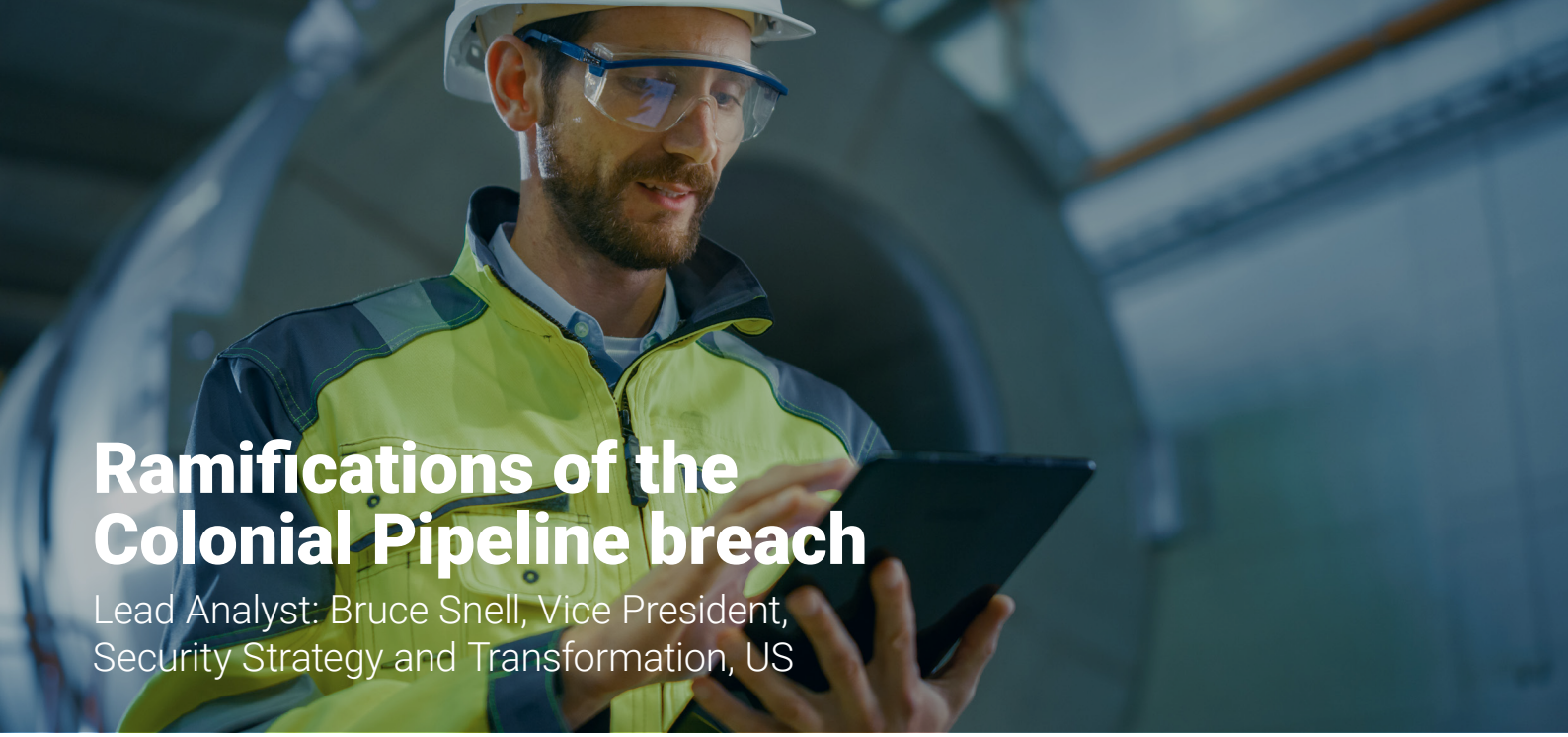
Global Threat Intelligence Center

Monthly Threat Report

June 2021

Contents



Ramifications of the Colonial Pipeline breach

Lead Analyst: Bruce Snell, Vice President, Security Strategy and Transformation, US

On Friday, 7 May, Colonial Pipeline suspended operations due to a ransomware outbreak, attributed to the DarkSide ransomware group, in their network. With Colonial supplying around 45% of the East Coast's fuel, this led to panicked runs on gas stations as consumers rushed to fuel their vehicles – and in some cases, stockpiling fuel in whatever containers they had on hand.

In the past, when a large breach takes place, the people affected receive a notice that they need to change their passwords and monitor their credit report for the next 12–18 months. However, the fallout of the Colonial breach resulted in literal fistfights at gas pumps.

So why was the pipeline shut down in the first place? When the news first broke, people made a lot of assumptions that the ransomware had infected the physical pipeline systems – commonly referred to as operational technology, or OT – themselves. The reality was that Colonial proactively shut down their OT systems to protect them from the internal systems which actually had been compromised. For Colonial, this was probably their best option, as an infection throughout their OT network could have led to greatly extended downtimes for the pipeline and created massive fuel shortages that could have taken weeks if not months to recover from. Given that Memorial Day, after a year or more of quarantine, was right around the corner, we could have seen a massive strain on the Eastern United States.

OT infrastructure is dramatically different from a traditional IT network. While there has been a huge push towards modernization, it's not uncommon to see control systems running outdated operating systems. Windows NT and XP still exist in large numbers in OT networks. This is partly due to systems that may have been in place for 20 years and cannot be readily upgraded due to 24/7 demand or replacement being cost-prohibitive. The problem ends up being control systems that can no longer be patched for vulnerabilities and often cannot run modern security tools already in use on the IT side of the organization. So, in Colonial's case, had their pipeline systems been impacted, a massive restart and restore operation would have been required. When you have a pipeline that stretches from Texas to New Jersey, a manual restart would require a herculean effort.

For Colonial, shutting down the pipeline was probably their best option, as an infection throughout their OT network could have led to greatly extended downtimes for the pipeline and created massive fuel shortages.

The pipeline shutdown was the tip of the iceberg

People seemed to focus a lot of attention on the actual shutdown and the ransomware payout. However, many things had to go wrong before Colonial even got to that point. To date, details around the Colonial breach have not been released, but if we look at how DarkSide has operated in the past, there were most likely multiple breaches that led to the ransomware being installed:

1. **Infiltration:** First, the attackers had to gain access to Colonial's network. In previous DarkSide incidents we have seen entry via a vulnerable VPN concentrator, however the breach could have happened via an easily guessed password or someone clicking a malicious link on their company laptop.
2. **Persistence:** Once in, an attacker will set up multiple beachheads in the network in case the initial entry point is discovered and fixed. Previously DarkSide threat actors have simply downloaded legitimate tools like TeamViewer to allow easy remote access to internal systems.
    a. **Bonus step:** It's not uncommon for the threat actors to take this opportunity to disable backup software or potentially delete any backups they can find.
3. **Exfiltration:** A tactic that's becoming more and more popular is 'double extortion,' where the threat actor first copies data (customer data, financial information, intellectual property, etc.) to a remote location operated by the attacker before encrypting the files. Then they charge a ransom to delete the stolen data and a ransom to unlock encrypted systems. One previous forensic investigation showed the threat actors downloading the open-source tool 'rclone' to move (and encrypt) the data to a cloud storage service.
4. **Encryption and ransom demand:** Once the organization has completed all these steps, the threat actor deploys a tool to encrypt the file system and places ransom notes with instructions on how to pay the ransom and recover the data from the infected systems.

> Everyone from the board to the front desk should have **regular security awareness training to help prevent common issues.**

Recommendations

There are steps an organization can take to help defend against attacks by threat actors like DarkSide:

1. **Take a holistic approach to security:** IT and OT security are very different animals, but organizations cannot afford to look at them as separate entities. IT and OT teams must work together to form an overarching security approach that utilizes the right tools for each environment and rolls security information up into a single pane of glass. It's not uncommon for the IT and OT teams to have 'frosty' relationships, so bringing in an unbiased third party can help break through roadblocks that prevent cooperation.
2. **Security training for everyone:** Security must be part of your organization's culture. Everyone from the board to the front desk should have regular security awareness training to help prevent common issues like easily guessed passwords or clicking on malicious links in phishing emails.
3. **Proactive security:** Colonial appears to have made the right choice to shut down operations to prevent ransomware spread from IT to OT. The situation could have played out much differently with a tool like Palo Alto's Extended Detection and Response (XDR) to step in and isolate the infected systems before they spread any further in the IT network. If the organization had been able to enforce isolation, there may have been no need to shut down the OT side of the operation.

Attacks against critical infrastructure and OT assets have been steadily increasing in recent years. The modernization of OT allows for dramatic improvement in productivity and cost savings, however, added connectivity also potentially increases exposure. Through proper planning and the judicious application of modern security tools, organizations can manage OT implementations in ways that help ensure uptime, safety and reliability.

#Spotlight 1

Securing education for the next generation

Lead Analyst: Mihoko Matsubara, CISSP,
Chief Cybersecurity Strategist, NTT Ltd., Japan

Education is one of the industries most impacted by the COVID-19 pandemic. Changes forced colleges, schools and universities to switch their education to remote learning and have their staff work remotely. This sudden shift has left the education industry even more vulnerable to cyberattacks. According to our 2021 Global Threat Intelligence Report (GTIR), education was the fifth most targeted industry in 2020, garnering 6% of all attacks, including ransomware attacks and cryptocurrency mining.

Some researchers report ransomware attacks on education grew by as much as 388% between the third and fourth quarters in 2020. Some attacks specifically targeted schools returning online after their summer break to generate extra pressure to pay ransoms. For example, after a ransomware attack disrupted a California school district in September 2020, it had to cancel five days of remote learning for 6,000 elementary school students. The University of California, San Francisco made a 'difficult decision' to pay a ransom of USD 1.14 million in June 2020 because 'The data that was encrypted is important to some of the academic work we pursue as a university serving the public good.'

About 72% of all malware activity in education was some form of coin miners or cryptocurrency miners. Miners are popular among students who likely seek to exploit unprotected IT infrastructure to generate passive income. Their presence can strain system resources, potentially leading to machines overheating or performing poorly. The presence of coin miners can also prove to threat actors there are vulnerabilities in systems, leading to further, more malicious exploitation.

Alarmingly, the cybersecurity maturity level of education is lower than other critical infrastructure industries. According to Cybersecurity Advisory assessments analysed for our 2021 GTIR, education's measured maturity level is only 1.04 (on a 0–5.99 scale), whereas finance measured at 1.84 and technology at 1.64 points. Since K–12 schools tend to be less equipped with cybersecurity resources than universities, they are more vulnerable to hacks.

More robust cybersecurity for education is crucial for the next generation to keep learning in a safe and secure environment. The industry is encouraged to take proactive measures to update and patch their IT resources. As remote desktop protocol (RDP) has become a popular tool in education during the pandemic, the Federal Bureau of Investigation warned in June 2020 that ransomware attackers were increasingly targeting vulnerabilities in RDP. Also, it's important to encrypt stored data, including students' personal information, to protect it from information thefts or double-extortion ransomware attacks.

Furthermore, the cybersecurity community needs to offer support to education when the industry is struggling during the pandemic and recession. It would be beneficial to provide industry-specific cyberthreat intelligence updates and cybersecurity best practices without using technical terminologies. NTT Ltd. Australia hosted a cybersecurity webinar on higher education in August 2020 and published a follow-up blog afterward. This type of grass-root activity could be indispensable to build trust and understanding of ongoing problems, as well as to start sharing tailored information helpful for the industry.

The cybersecurity community needs to offer support to educational organizations by providing industry-specific cyberthreat intelligence updates and cybersecurity best practices.

President Biden signs Executive Order focused on strengthening cybersecurity defenses

Lead Analyst: Danika Blessman, Senior Threat Intelligence Analyst, Global Threat Intelligence Center, US

Coming on the heels of several supply chain and infrastructure attacks, US President Biden signed the 'Executive Order on Improving the Nation's Cybersecurity'[1] on 12 May 2021, to address 'persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector and ultimately the American people's security and privacy.'

This Executive Order (EO) was prompted by a string of attacks on national and international critical infrastructure – including Microsoft Exchange Servers, the Colonial Pipeline and the SolarWinds attacks – and seeks to improve the nation's cybersecurity and protect federal government networks.

The EO focuses on the following key areas:

- removing barriers to share threat information between the public and private industries
- modernizing and implementing stronger cybersecurity standards in the federal government
- enhancing software supply chain security, including establishing baseline security standards in software development for software sold to the government
- establishing a cybersecurity safety review board
- creating a standard playbook for responding to cyber-incidents
- improving detection of cybersecurity incidents on federal government networks
- improving investigative and remediation capabilities

The EO also requires federal government agencies to improve their vulnerability and intrusion detection capabilities, along with their investigative and remediation capabilities.

John Petrie, from the NTT Global CISO Team, recommends that readers review this EO in conjunction with the US National Defense Authorization Act (NDAA) for Fiscal Year 2021.[2] The EO builds on changes introduced by the NDAA to expand public/private partnerships, accomplished by changing the way US Government agencies share information and integrate with the capabilities of the private cybersecurity industry.

Petrie suggests that, as part of the greater cybersecurity industry, collaboration must occur between the public and private sectors; neither can win alone. There are distinct advantages for cybersecurity companies in various functional areas of cybersecurity to participate in supporting the intent of this EO. The EO looks to expand this long-time partnership between the two entities.

And they're not just organizations in the cybersecurity sector. Petrie says this continued public and private sector alliance also requires the integration of telecom and ICT services from a global reach perspective. He further states that 'companies like NTT who have a global reach across the entire suite of cyberservices are positioned to join the ecosystem along with other similar companies, and provide the support capabilities for the common good.'

We believe that implementation of the EO, as well as true security across industries, will require extensive public/private partnerships to be successful. This will require organizations in both sectors to innovate, update and refresh their cybersecurity practices to meet the new requirements.

Many breaches – across all industries – occur due to failure to comply with, at a minimum, good security practices. This EO seeks to ensure organizations apply at least 'good practices.' Such practices include encouraging security awareness within organizations, along with implementing further security measures such as a zero-trust model, to prevent potentially catastrophic attacks with far-reaching global effects.

The new Executive Order is available here for review.

[1] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
[2] https://www.congress.gov/bill/116-congress/house-bill/6395

NTT's Global Threat Intelligence Center

The NTT Global Threat Intelligence Center (GTIC) protects, informs and educates NTT Group clients through the following activities:

- threat research
- vulnerability research
- intelligence fusion and analytics
- communication to NTT Group clients

The GTIC goes above and beyond the traditional pure research organization, by taking their threat and vulnerability research and combining it with their detective technologies development to produce applied threat intelligence. The GTIC's mission is to protect clients by providing advanced threat research and security intelligence to enable NTT to prevent, detect and respond to cyberthreats.

Leveraging intelligence capabilities and resources from around the world, NTT's threat research is focused on gaining understanding and insight into the various threat actors, exploit tools and malware – and the techniques, tactics and procedures (TTP) used by attackers.

Vulnerability research pre-emptively uncovers zero-day vulnerabilities that are likely to become the newest attack vector, while maintaining a deep understanding of published vulnerabilities.

With this knowledge, NTT's security monitoring services can more accurately identify malicious activity that is 'on-target' to NTT Group clients' infrastructure.

Intelligence fusion and analytics is where it all comes together. The GTIC continually monitors the global threat landscape for new and emerging threats using our global internet infrastructure, clouds and data centers along with third-party intelligence feeds; and works to understand, analyse, curate and enrich those threats using advanced analysis techniques and proprietary tools; and publishes and curates them using the Global Threat Intelligence Platform (GTIP) for the benefit of NTT Group clients.

Our **Global Threat Intelligence Center** goes beyond a traditional research-only approach by combining focused research with detective technologies. This results in **true applied threat intelligence** to protect our clients with effective tools and services which reduce security risks and threats.

Recent assets

2021 Global Threat Intelligence Report

Our 2021 Global Threat Intelligence Report (GTIR) is the culmination of the data the Global Threat Intelligence Center gathered and analyzed throughout the year. We produce this report by collecting a broad set of global data (log, event, attack, incident and vulnerability) to identify key cybersecurity trends of which businesses need to be aware.

Download report

If you haven't already, **register to receive the Monthly Threat Reports** directly to your inbox each month.


NTT