# Cybersecurity Quarterly Update

Organization, Personnel & Technology Committee
Item 6c
July 12, 2021

# Agenda

- Colonial Pipeline Attack
- Ransomware Defined
- Threat Actor: Darkside

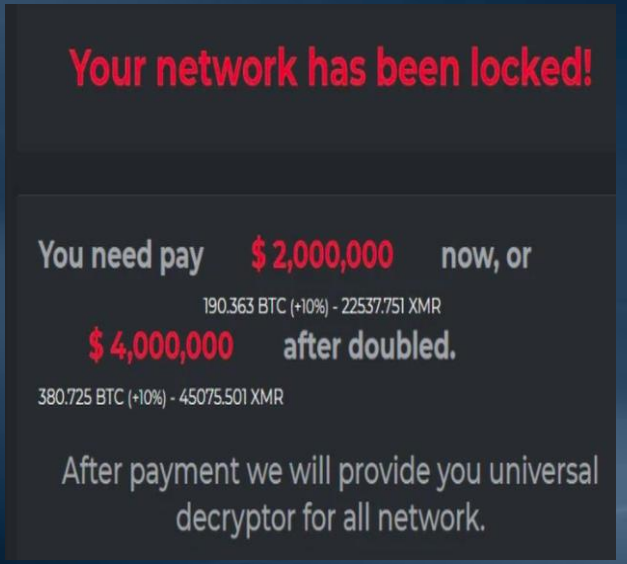
# Who is Colonial Pipeline?

"It is a major transporter of gasoline, diesel and jet fuel delivering critical resources to much of Southern East Coast"

- Ships gasoline and jet fuel from the Gulf Coast through 5,500 miles (8,850 kilometers) of pipeline
  - 2.5 million barrels a day
  - Capable additional 800,000 to NY
  - Texas to North Carolina
  - Over 50 million consumers
  - Supply's fuel to 14 states
  - 6-day operational shutdown
  - Instant supply chain issues
  - Increased fuel costs across U.S. and created havoc at fuel pumps

# Colonial Attack

- May 9, 2021, U.S. declares regional emergency after cyber attack
- May 16, 2021, CP operating @ 100% capacity
- Paid $4.4 million ransom
- Restored main systems from previously maintained backups
- Key-facts
  - Pipeline stretches over 5500 miles Houston, TX – Linden, NJ
  - Remained shutdown > 6 days as precautionary measure
  - Ransomware as a Service (RaaS)
  - Utilized common network admin tools
  - Vast array of indicators of compromise
  - Attack carried out over time



# What is Ransomware?

- Ransomware, TTP (Tactic Techniques, and Procedures):
  - Malware which prevents access by encrypting targeted systems or data until a sum of money is paid
  - Average ransomware payment for Q1 2021 was $220,228 (does not account for downtown cost which are 5 -10 x as much as the Ransom)
    - By far the most expensive cyber incident for organizations to encounter
  - Ransom request is expensive
    - Attacker may negotiate smaller amounts for higher likelihood of payout
  - Ransom demands normally in form of Cryptocurrency
    - Makes tracing funds next to attacker next to impossible
  - Ransom not via email or system generated
  - May delete/encrypt backups
  - Searches for mapped drives/network shares

# Ransomware as a Service (RaaS)

- RaaS TTP (Tactic, Techniques and Procedures):
  - Earliest known approximately May 2015
  - Requests are initiated from a downloaded Tor browser
  - Request is complete and applied instantly
  - Ransom note/keys via email or system generated
  - Typically request high ransom
    - May request large amounts for distribution amongst co-conspirators

# Threat Profile: Darkside

- Colonial Pipeline Breach
  - Ransomware as a Service
  - Darkside criminal organization takes credit
  - MWD Response
    - Validating systems
    - Massive list of Indicators of Compromise (IOC's)
- Country of Origin
  - Russia (Darkside)
    - Cyber criminals (not governmental operatives)

  (May maintain criminal status to obscure Government Ties/Involvement
- Prolific Threat
  - 4 distinct targeted attacks in 1 year
  - Jurisdictional issues across borders
  - Highly sophisticated reconnaissance/tactics

# Ransomware: To Pay or Not to Pay?

- Law Enforcement stance is generally “DO NOT PAY”
  - Once the sum of money is paid, no guarantee of data back
  - Many companies see second round of ransom/repeat attacks
    - Believed to be due to willingness to pay
    - Multiple threat agents (word of mouth)
    - Likely that same attacker will “re-attack” multiple times
  - 46% of those that paid ransom, stated at least some of their data was corrupted
    - 23 days is average downtime when a payment decision is made
  - 58% of extortionist attempt to extort a second ransom after receiving payment

ONCE PAID, CRYPTOCURRENCY RANSOM MONEY IS VIRTUALLY UNTRACEABLE AND SHOULD BE CONSIDERED A COMPLETE LOSS


"Companies that facilitate ransomware payments to cyber actors on behalf of victims, including financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response, not only encourage future ransomware payment demands but also may risk violating OFAC regulations."

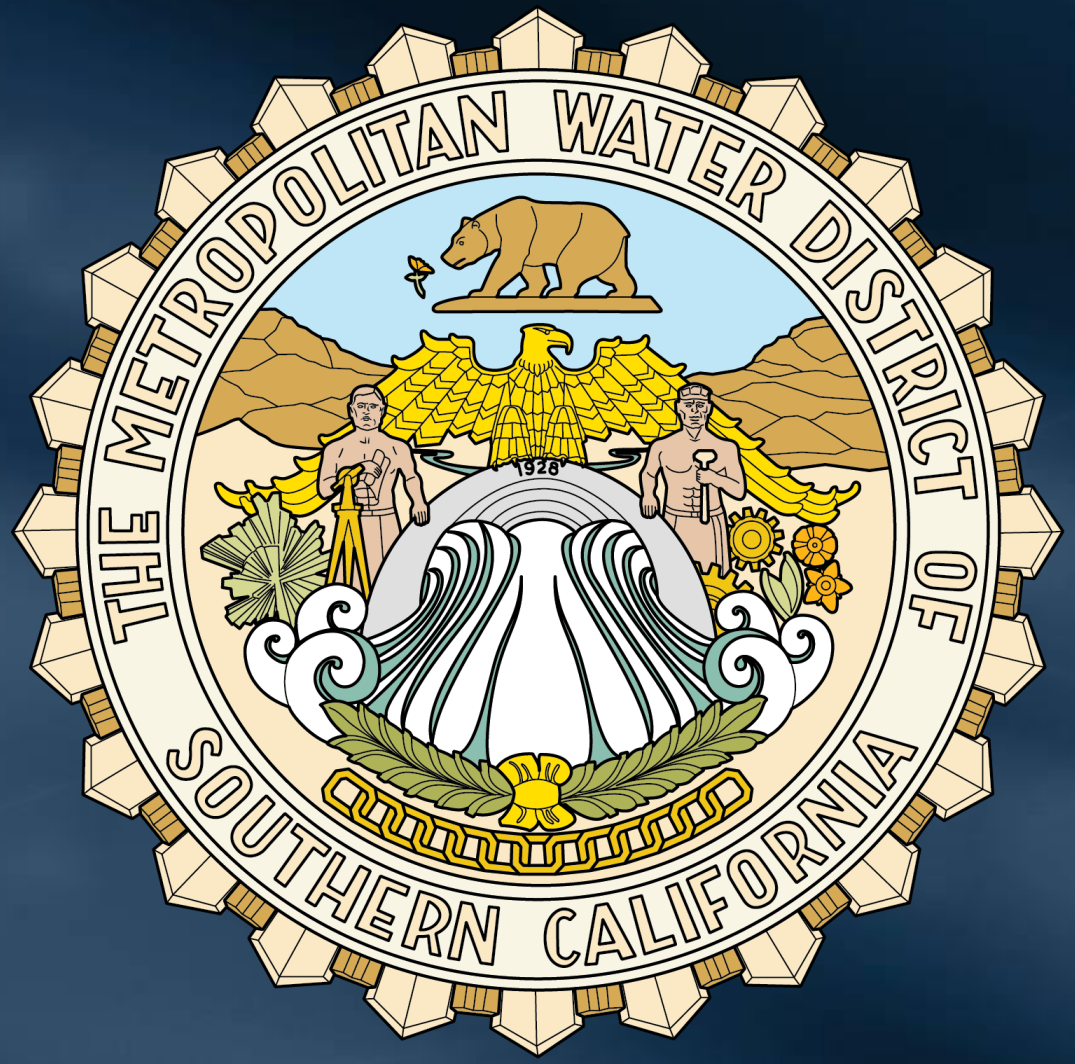
The U.S. Department of the Treasury's Office of Foreign Assets Control, October 1, 2020

# Mitigation Strategy: Ransomware

- Steps to protect:
  - Never open emails or download software from unknown sources
  - Do not disable malware protection on systems
  - Attend user awareness training annually to create a cyber-resilient working culture
  - Update system files and plug-ins from a trusted source, on a regular basis
  - Keep a backup of sensitive data on share drives stored at offsite data centers and limit access to confidential files or the organization’s assets

# Mitigation Strategy: Ransomware

- Steps to protect continued:
  - Administrators should routinely perform account maintenance and routinely scour external sources for leaked confidential information such as:
    - Account usernames and passwords
    - Employee personal information that may have been leaked from company
    - Sensitive documents pertaining to MWD business that are not Public Record
    - Plans, blueprints, GIS or other technically informative types of drawings not authorized for public release
    - ICS/SCADA related diagrams, drawings or other information not authorized for public release


THE METROPOLITAN WATER DISTRICT OF
SOUTHERN CALIFORNIA
1928