CYBER DEFENSE INTELLIGENCE

CYBER Defense Briefing

CYBER DEFENCE INTELLIGENCE CENTER

May 10, 2021

Colonial Pipeline Ransomware Attack

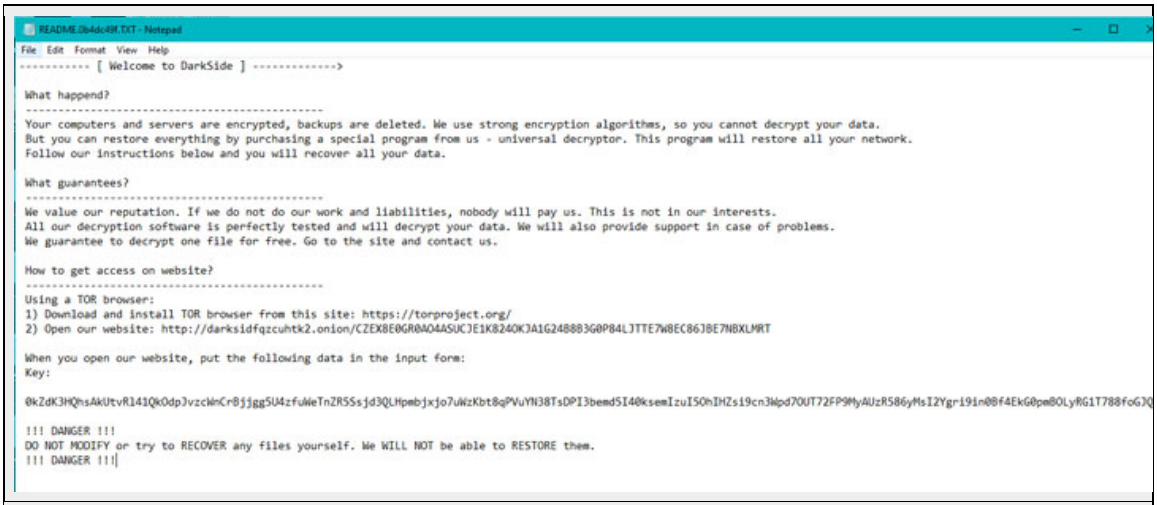
SCOPE: This intelligence briefing affects all Industry Segments and Organizations.

Attack Description and Timeline

Colonial Pipeline, based in Atlanta Georgia, is the largest refined products pipeline in the United States. The Pipeline carries 45% of the fuel consumed on the U.S. East Coast. Colonial halted operations on Saturday due to a ransomware attack.

In a statement posted on their website a Colonial spokesperson stated, "On May 7, the Colonial Pipeline Company learned it was the victim of a cybersecurity attack." The organization further stated "We have since determined that this incident involves ransomware. In response, we proactively took certain systems offline to contain the threat, which has temporarily halted all pipeline operations, and affected some of our IT systems."

Colonial is presently working with multiple US Government agencies and private organizations to assess and remediate the impacts.



Darkside ransom note

Image Source: thehackernews.com

Initial analysis of the attack indicates that the organization was the victim of ransomware. The variant identified in the attack is a variant attributed to Darkside. Darkside is a Ransomware-As-A-Service (RaaS) platform which leverages affiliates to conduct

ransomware campaigns. They are believed to be a Russian Cybercriminal Gang (not believed to be state sponsored).

Attack Methodology

Darkside Summary

- A new variant of Darkside was discovered in August 2020
- Darkside targets English-speaking countries, it also actively avoids impacting former Soviet-bloc countries
- The operators of Darkside state that they do not attack hospitals, hospices, schools, universities, non-profit organizations, or government agencies
- The new variant uses Salsa20 with the custom matrix and RSA-1024 encryption algorithms
- Their typical ransoms range from $200,000 to $2,000,000
- Darkside is a "double-extortion variant that will exfiltrate and publish victim data to increase the pressure on payment.
- The new variant is the fastest encrypting ransomware found to date, allowing it to inflict maximum damage in a short period even when discovered.

Upon infecting a system Darkside attempts to escalate privileges to Admin by bypassing UAC via the COM interface. Unpatched Windows 10 systems will not prompt the user to approve the change and allow the escalation of privilege.

Once the privileges have been escalated the ransomware conducts a local check against 17 former Soviet-bloc countries. This allows them to avoid attacking Russian and Russian allied countries.

Once started the ransomware creates a Log file which dictates the ransomware actions. It also implements numerous actions aimed at minimizing detection. These include emptying the recycle bin, uninstalling services including VSS which disables shadow copies. It then deletes any existing shadow copies by utilizing PowerShell.

Once all shadow copies have been deleted, the ransomware disables other services so that it has full access to users' files. It leaves all files related to TeamViewer to allow for access at a later time.

The ransomware then begins encrypting the users' files using the SALSA20 Algorithm and an RSA-1024 key. Each encrypted file has a unique identifier appended to it. It specifically whitelists specific files and folders, so it doesn't limit its own operations. It appears to then exfiltrate the files and leave a ransom note for the user.

Impacts

Damage from the attack is still being assessed but will have large impacts on the US economy and will result in short-term fuel shortages in the eastern United States. In addition to these impacts, the Ransomware's use of Double-Extortion could result in sensitive Colonial Pipeline data being posted to the Darkweb on the Darkside shame site.

Actions

Protection from attacks like the Colonial Pipeline ransomware attack involve many dimensions of a well-run security program. A strong security program combined with a solid security architecture will increase the likelihood that an attack such as this can be prevented, and at minimum, discovered quickly. This will allow prompt attention by security personnel and reduce the incident's impact without relying solely on an observant employee.

- Implement a strong **vulnerability management** and **patching process** to ensure that inherent weaknesses in systems and devices are identified, analyzed, and closed.
- Maintain all operating systems and software at active and vendor-supported versions.
- Deploy **next-gen Endpoint protection** that not only identifies resident and dormant viruses and malware during system scans, but also stops actions taken by executables when they execute in memory.
- Design a **"Defense-in-depth" architecture** which leverages tools that provide "intelligent overlap" in their detection and protection capabilities including systems that address the monitoring of the SCADA system if you operate an ICS platform.
- Ensure that passwords meet complexity, length and management requirements, especially in systems which do not support multi-factor authentication.
- Isolate the OT Network from the Internet by architecting an **effective "Air-Gap"** between the Internet and the Control Systems that leverages **VPN** (Virtual Private Network) and **Zero-trust Technologies** as well as **multi-factor authentication** technologies. SCADA employees should have to traverse multiple gateways with different credentials prior to OT access.
- **Limit and tightly control Remote Access** by using strong authentication controls and limiting access to the system from specific IP Addresses and locations, and disable RDP (Remote Desktop Protocol) where possible.
- **Utilize advanced cyber tools** that prevent the entry of malware into the OT environment such as **"Content Disarmament and Reconstruction" tools.**
- Implement a strong **monitoring and auditing capability** that gathers telemetry from systems and devices and can correlate events into alerts.
- Ensure that your vendors have a strong security program by implementing a **vendor management process** that assesses and audits vendors' security capabilities and actions.

- Stay engaged with **Threat Intelligence** services to ensure that your team has the "latest and greatest" OSINT (open-source intelligence) information. Ensure that you are active in your industry Information Sharing and Analysis Center (ISAC) to stay abreast of the latest attacker activities and **TTP's (Tactics, Techniques and Procedures).**
- Ensure that you **backup your data regularly**, **keep offline backups, and verify integrity of backup process.**
- **Enable audit logs** for all remote connection protocols and to ensure all new accounts were intentionally created.
- **Scan your network** for open or listening ports and **disable SMBv1**.
- **Implement application whitelisting**. Only allow systems to execute programs known and permitted by security policy.
- **Monitor Active Directory** and local administrators group changes.
- Maintain only the most up-to-date version of PowerShell and uninstall older versions. If possible, **disable or limit PowerShell** on endpoint devices.
- **Enable PowerShell logging** and monitor for unusual commands, especially execution of Base64 encoded PowerShell.
- **Turn off the option to automatically download attachments**. To simplify the process of reading email, many email programs offer the feature to automatically download attachments. Check your settings to see if your software offers the option and disable it.

Prepared by the Cyber Defense Coalition Intelligence Center Analysis Team.