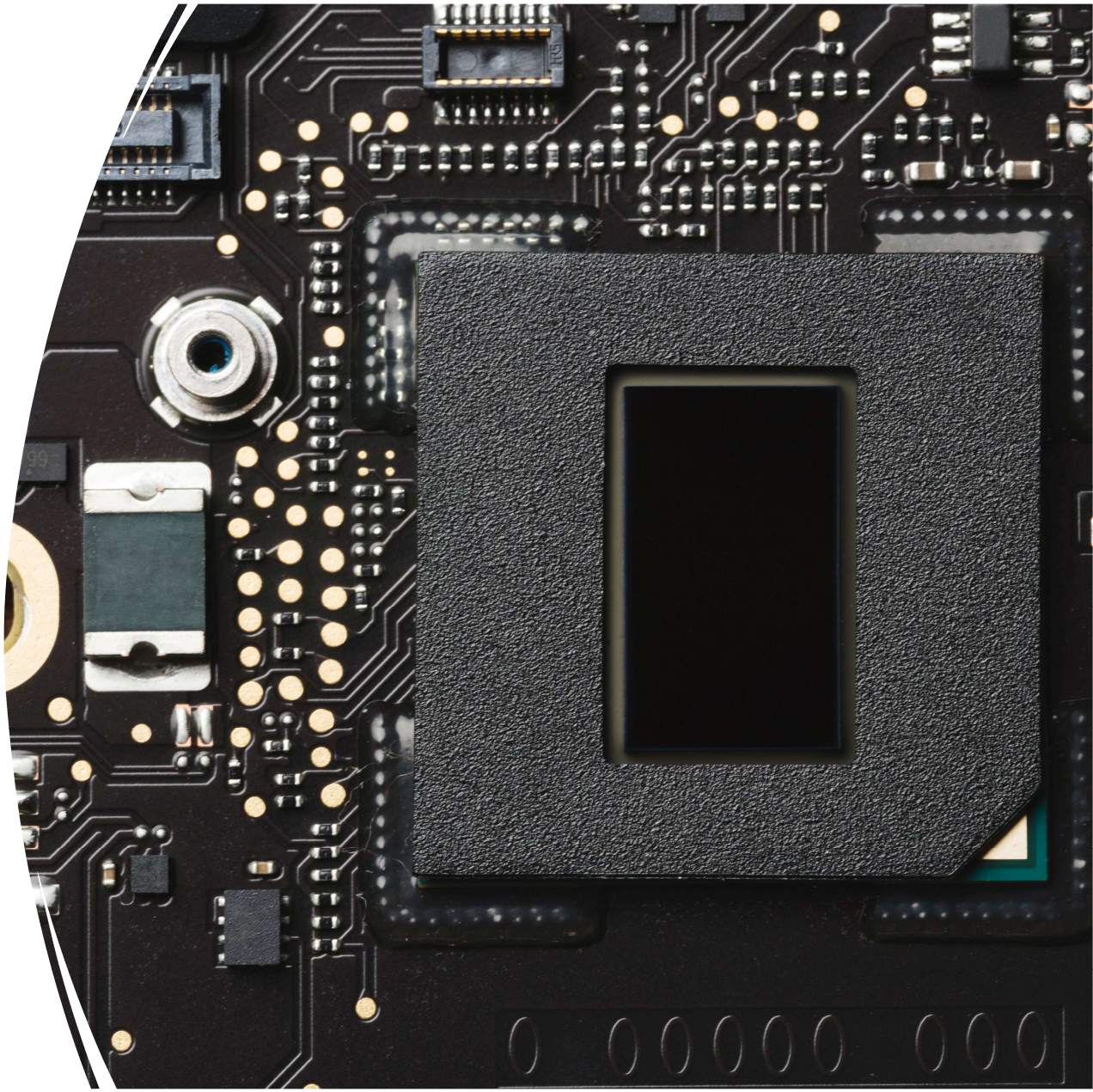
Attacco ransomware a Colonial Pipeline

Santambrogio Lorenzo – Puggioni Riccardo

Chi è Colonial Pipeline

Colonial Pipeline è una delle principali reti di condotte di trasporto di carburanti negli Stati Uniti. Gestisce circa 8.850 chilometri (5.500 miglia) di tubazioni che trasportano prodotti petroliferi raffinati



L’attacco ransomware

Nel maggio 2021, Colonial Pipeline è stata colpita da un attacco ransomware, che ha paralizzato temporaneamente le operazioni dell'azienda.

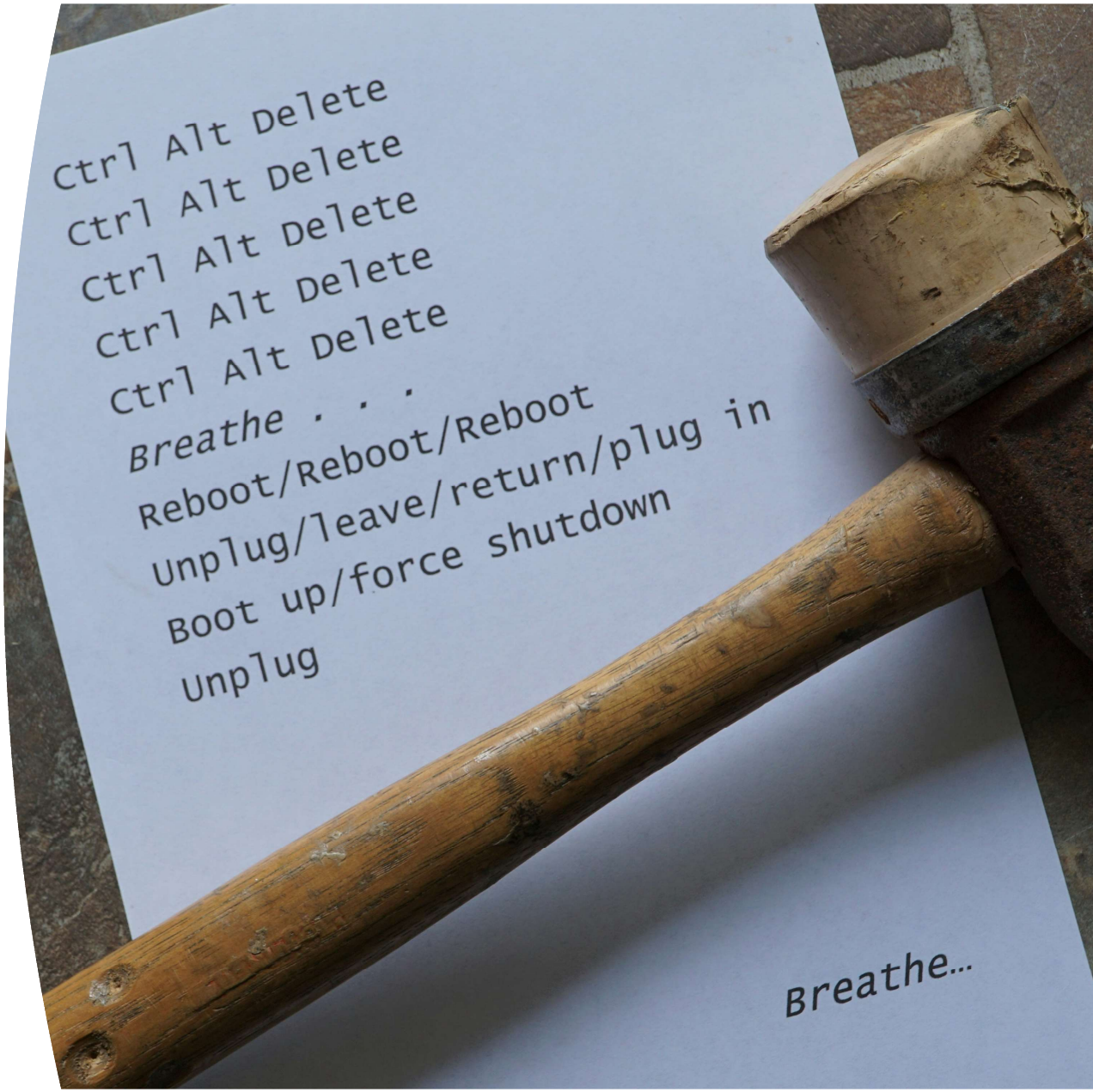
I criminali informatici, detti “Darkside”, hanno utilizzato un ransomware per bloccare l'accesso ai sistemi informatici dell'azienda e hanno richiesto un riscatto in bitcoin per ripristinare l'accesso.

Impatto sull'approvvigionamento di carburante

Colonial Pipeline ha dovuto chiudere temporaneamente l'intera rete di condotte, interrompendo il flusso di carburante lungo la costa orientale degli Stati Uniti. Ciò ha portato a preoccupazioni riguardo alla disponibilità di benzina, diesel e altri prodotti petroliferi, con code ai distributori di benzina e aumenti dei prezzi del carburante.

Conseguenze e implicazioni

L'attacco ransomware alla Colonial Pipeline ha sollevato preoccupazioni sulla sicurezza delle infrastrutture critiche e ha evidenziato la crescente minaccia che i cybercriminali rappresentano per le aziende e i servizi fondamentali. Ha anche portato a un maggiore interesse da parte dei governi e delle organizzazioni per migliorare la sicurezza informatica e prevenire futuri attacchi.



Fase di infezione

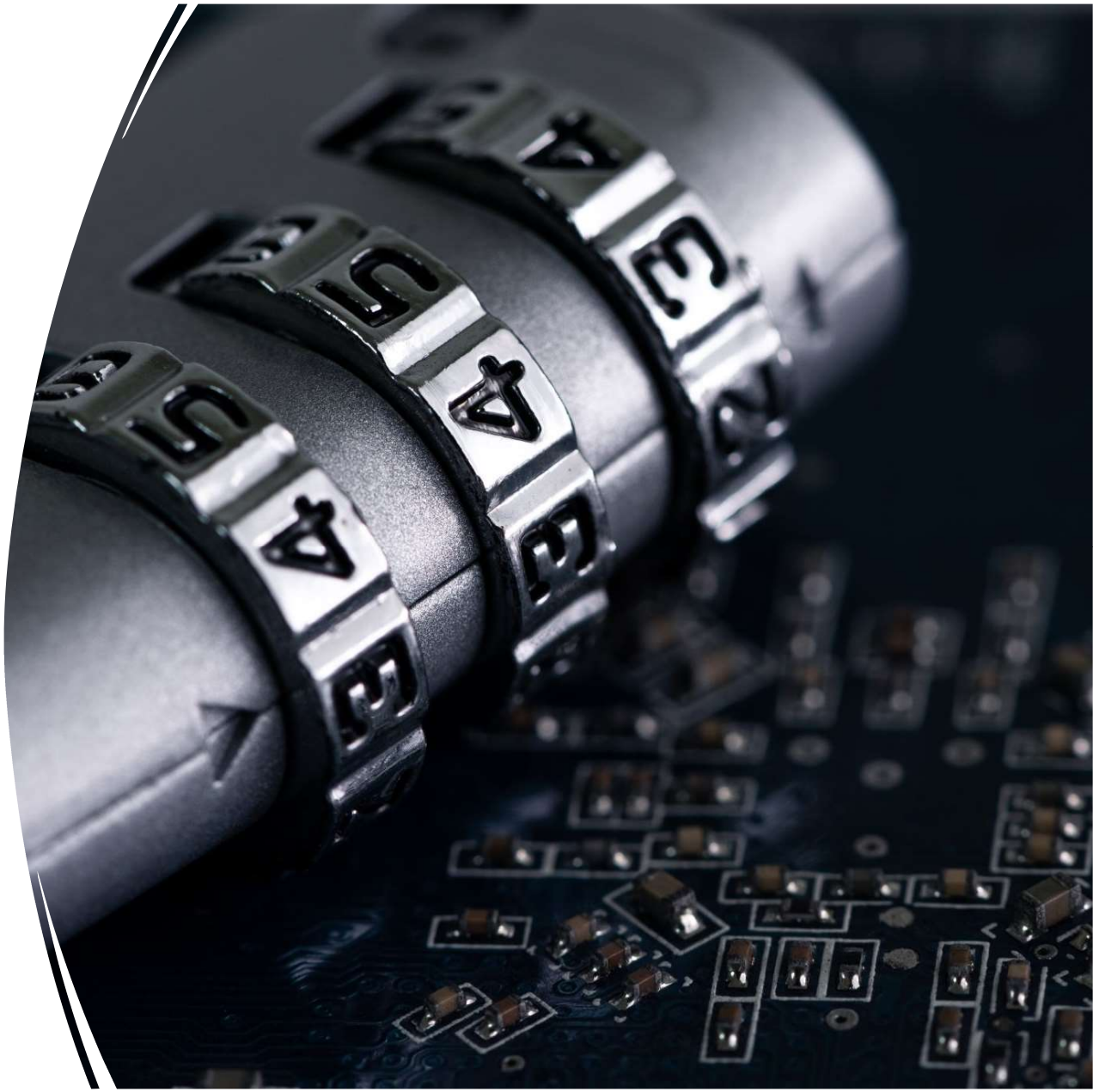
Gli attaccanti hanno verosimilmente utilizzato una varietà di tecniche per infiltrarsi nella rete informatica di Colonial Pipeline. Queste tecniche includono phishing, exploit di vulnerabilità del software o l'uso di credenziali rubate.

Distribuzione del Ransomware

Una volta all'interno del sistema, i cybercriminali hanno rilasciato il ransomware, che è un tipo di malware progettato per crittografare i dati. Il ransomware utilizzato potrebbe essere stato personalizzato per Colonial Pipeline o potrebbe essere stato un malware preesistente, adattato alle specifiche dell'azienda.

Crittaggio dei Dati

Il ransomware crittografa i file e le cartelle rilevanti per rendere i dati inaccessibili senza la chiave di decrittazione corretta. In questo modo, l'azienda non può più accedere ai propri file senza pagare il riscatto o ripristinare i dati da backup sicuri, se disponibili.



Richiesta di Riscatto

Dopo aver crittografato i dati, gli aggressori hanno inviato una richiesta di riscatto a Colonial Pipeline. Questa richiesta può essere stata accompagnata da istruzioni su come effettuare il pagamento del riscatto e ottenere la chiave di decrittazione necessaria per ripristinare i dati.

Pagamento del Riscatto e Ripristino

Colonial Pipelina ha pagato il riscatto richiesto di 4.4 milioni di dollari, il pagamento è avvenuto tramite bitcoin. Tuttavia, pagare il riscatto non è sempre garanzia di ripristino completo dei dati e potrebbe incoraggiare ulteriori attacchi.

Analisi Forense e Miglioramenti della Sicurezza

In seguito all'attacco, l'azienda ha condotto un'analisi forense approfondita per comprendere come gli aggressori sono riusciti a penetrare nella loro rete e identificare eventuali vulnerabilità da correggere. Sono stati implementati miglioramenti alla sicurezza informatica per ridurre il rischio di futuri attacchi.

Sitografia:

https://en.wikipedia.org/wiki/Colonial_Pipeline_ransomware_attack

https://www.cdscultura.com/2021/05/attacco-ransomware-alla-colonial-pipeline-in-usa/

https://chat.openai.com/

https://www.agendadigitale.eu/sicurezza/ransomware-e-riscatti-in-cryptovalute-la-lezione-dellattacco-a-colonial-pipeline/#:~:text=E%20va%20chiarito%20che%20DarkSide,spenta%20a%20solo%20titolo%20precauzionale.