Trabajo de Investigación: "Explorando Incidentes del Mundo Real"

Objetivo:
Investigar un incidente de ciberseguridad reciente y analizar cómo fue gestionado.

Ataque de ransomware a Colonial Pipeline (2021).

- **¿Qué ocurrió?**

Colonial Pipeline tuvo un ataque de malware el día 6 de mayo de 2021, el ataque detuvo todas las operaciones del oleoducto., el oleoducto mueve el 45% porciento de todo el combustible de la costa este.

- **¿Cuál fue la causa raíz?**

Un ataque hecho por la empresa criminal llamada DarkSide, se dice que también el día antes del ataque el grupo robo 100 gigabytes de datos de los servidores de la empresa. El malware detectado como Trojan-Ransom.Win32.Darkside y Trojan-Ransom.Linux.Darkside utilizaron cifrados potentes por lo que la restauración de los archivos sin la clave correcta es imposible. El grupo utilizo un modelo de ransomware como servicio (RaaS), esto permitió que el grupo proporcionara a sus socios la infraestructura necesaria para realizar el ataque, si bien el grupo declaro que no tenía intención de causar consecuencias tan graves, se dice que el grupo por medio de spear phishing pudo infectar a las victimas en este caso trabajadores y lograron obtener credenciales legitimas para el acceso a VPN de un empleado, al no tener habilitada la doble autenticación , el acceso se obtuvo sin problemas.

- **¿Qué impacto tuvo**

La compañía cerro las operaciones como medida de precaución, esto porque se previo que los piratas hubieran obtenido información que les permitiera llevar a cabo mas ataques. El 9 de mayo la empresa declaro que planea reparar paulatinamente las operaciones. A raíz de la escasez de combustible el aeropuerto internacional de Charlotte-Douglas, American Airlines cambio los horarios de vuelo. También el aeropuerto internacional Hartsfield-Jackson de Atlanta y por lo menos 5 aeropuertos tuvieron la misma suerte. Por otro lado, los empleados tuvieron que desactivar algunos

sistemas de información, puesto que algunos ordenadores habían sido cifrados y en parte para que la infección se extendiera, también disparo en un 4% el costo de la gasolina.

- **¿Cómo fue gestionado?**

Investigadores externos descubrieron donde estaban los datos robados e informaron al FBI el cual procedió a solicitarle al proveedor de servicios de internet propietario del servidor para que fuera asilado, así el grupo DarkSide perdió el acceso a la información, si bien esta acción no restauro los servicios, si evito que los daños hubieran sido mayores.

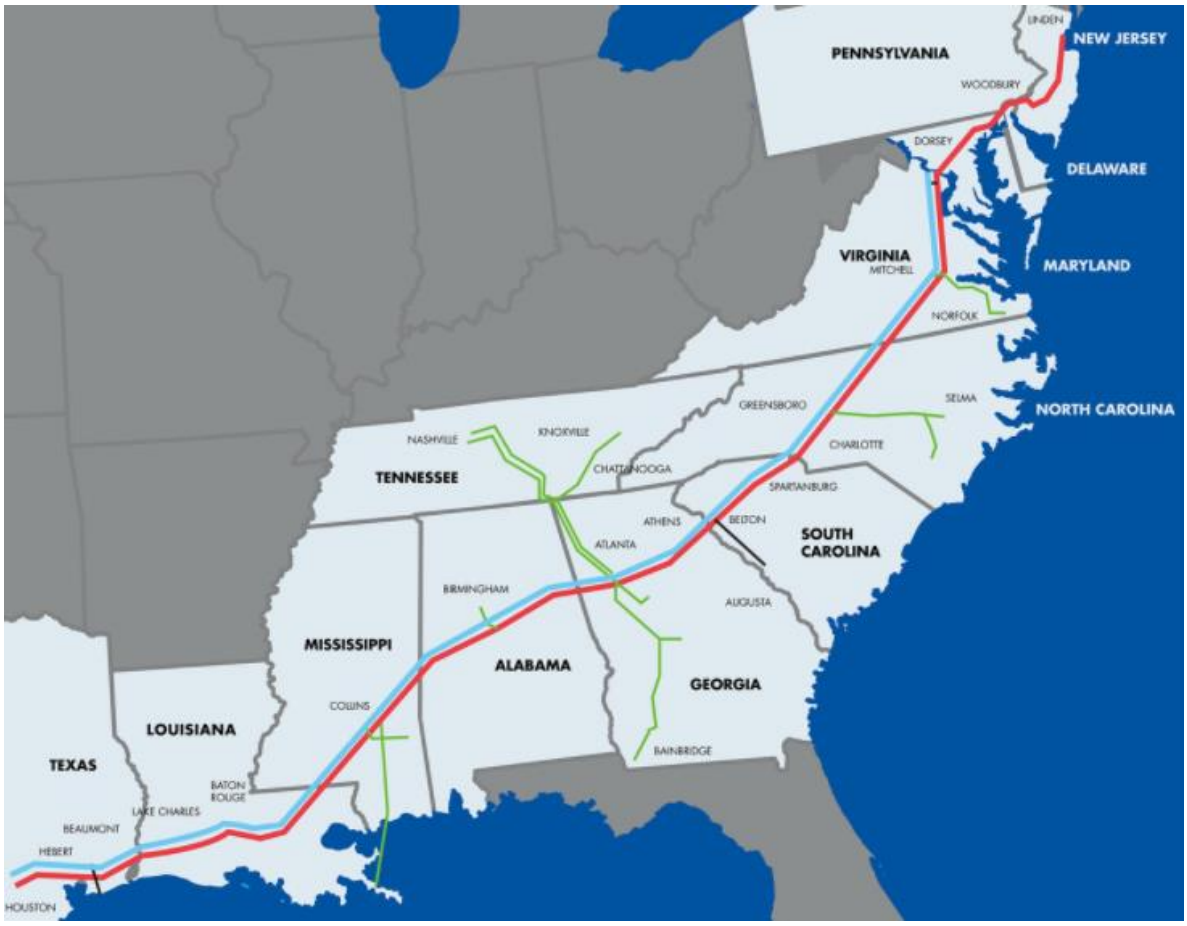
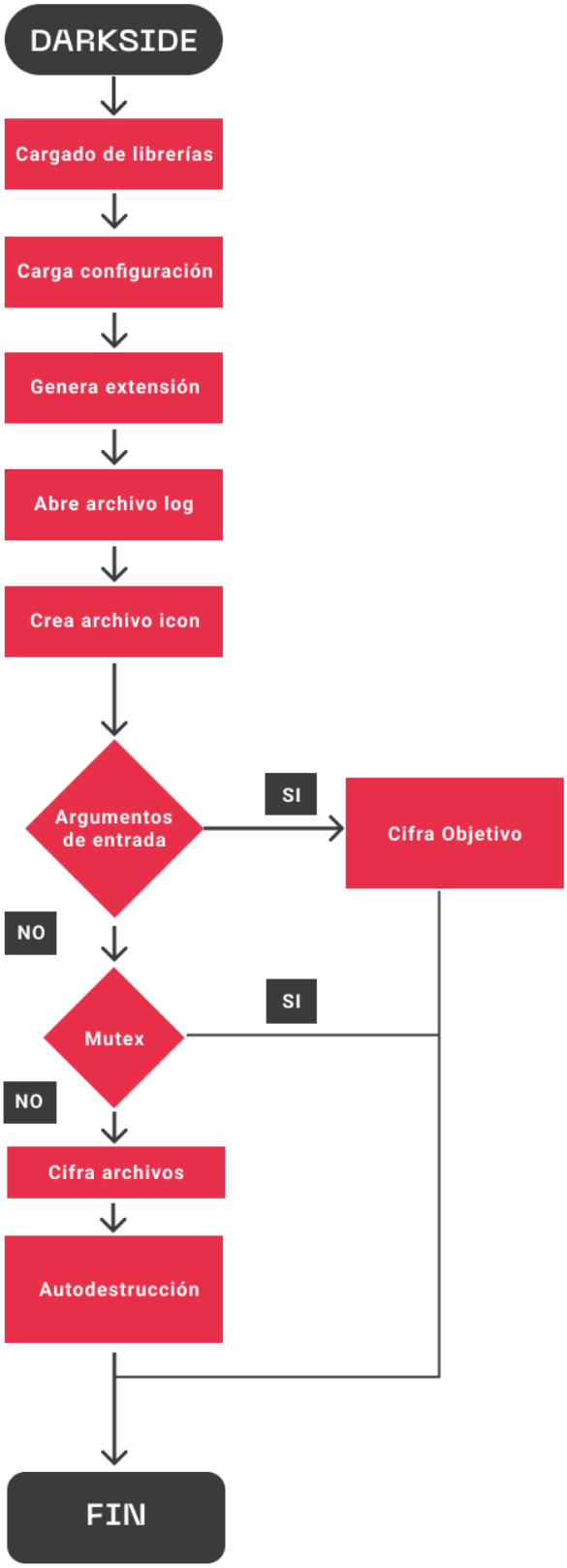
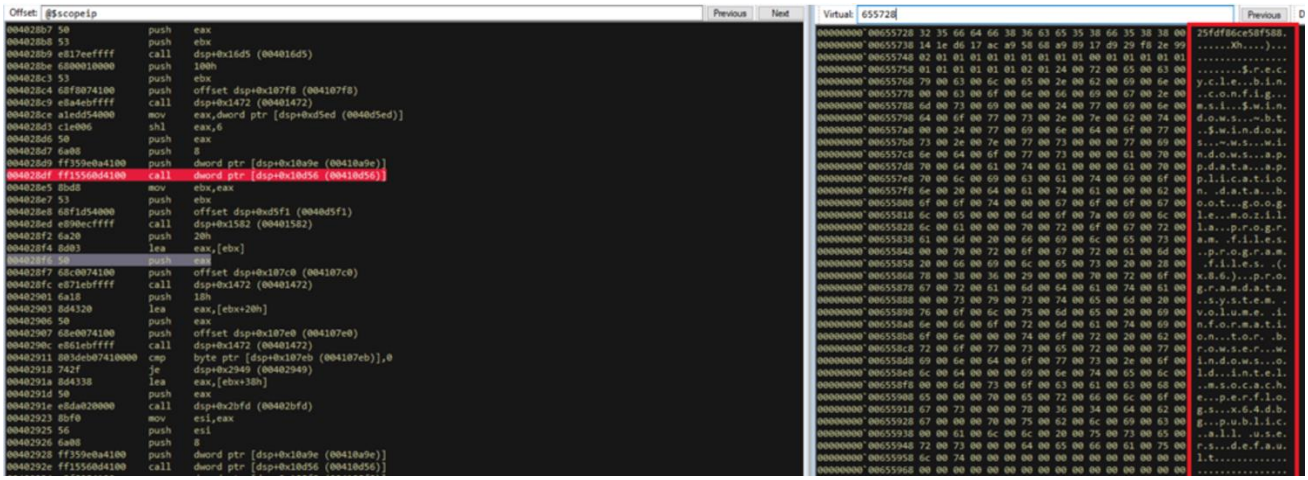
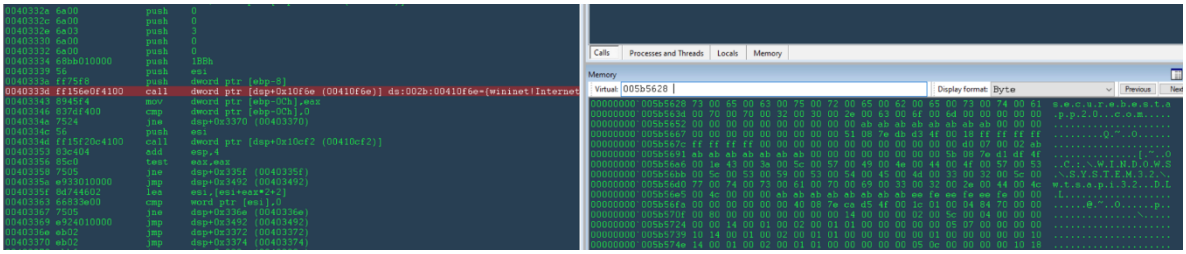


Imagen de la infraestructura del oleoducto afectado.


DARKSIDE
Cargado de librerías
Carga configuración
Genera extensión
Abre archivo log
Crea archivo icon
Argumentos de entrada
SI
Cifra Objetivo
NO
Mutex
SI
NO
Cifra archivos
Autodestrucción
FIN





```
void fun_encrypt_local_drives(void)

{
  uint drives_string_len;
  int drive_type;
  undefined *valid_drives_buff_cpy;
  undefined valid_drives_buffer [256];
  undefined4 local_24;
  undefined4 local_20;
  undefined current_drive [24];

  drives_string_len = (*_GetLogicalDriveStringsW)(0x80,valid_drives_buffer);
  if (drives_string_len != 0) {
    valid_drives_buff_cpy = valid_drives_buffer;
    drives_string_len = drives_string_len >> 2;
    do {
      drive_type = (*_GetDriveTypeW)(valid_drives_buff_cpy);
      if (((drive_type == 3) || (drive_type == 2)) || (drive_type == 4)) {
        local_24 = 0x5c005c;
        local_20 = 0x5c003f;
        (*_wcscpy)(current_drive,valid_drives_buff_cpy);
        f_encrypt_files(&local_24);
      }
      valid_drives_buff_cpy = valid_drives_buff_cpy + 8;
      drives_string_len = drives_string_len - 1;
    } while (drives_string_len != 0);
  }
  return;
}
```