**Ataque de ransomware do Colonial Pipeline**

Em 7 de maio de 2021, Colonial Pipeline, um sistema de oleoduto americano que se origina em Houston, Texas, e carrega gasolina e combustível de aviação principalmente para o Sudeste dos Estados Unidos, sofreu um ataque cibernético ransomware que afligia equipamentos informatizados que gerenciavam o oleoduto. A Colonial Pipeline Company interrompeu todas as operações do oleoduto para conter o ataque. Supervisionada pelo FBI, a empresa pagou o valor solicitado pelo grupo hacker (75 bitcoin ou US$ 4,4 milhões) em poucas horas; após o recebimento do resgate, uma ferramenta de TI foi fornecida à Colonial Pipeline Company por DarkSide para restaurar o sistema. No entanto, a ferramenta exigiu um tempo de processamento muito longo para restaurar o sistema ao estado de funcionamento.

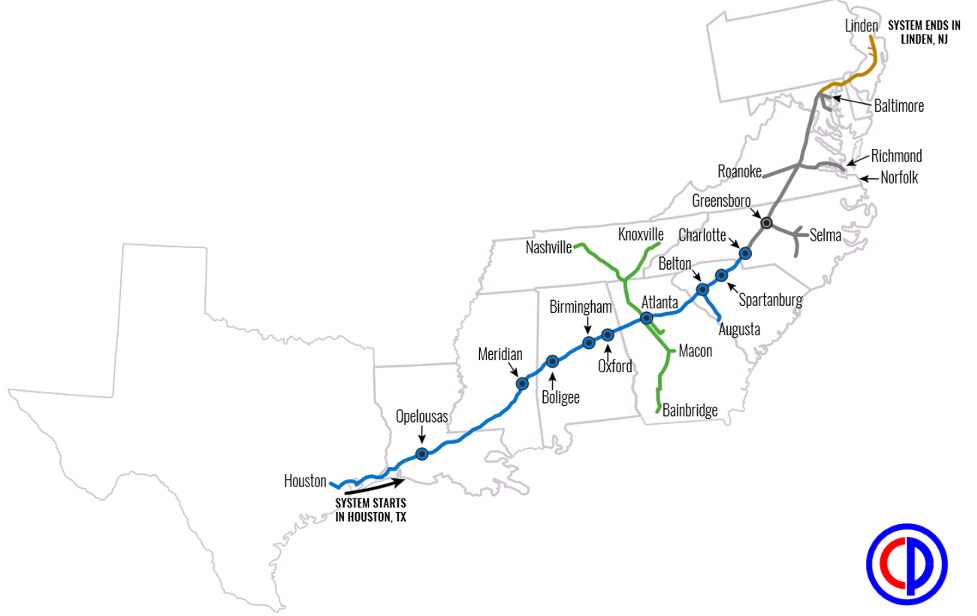
A Administração Federal de Segurança de Transportadoras Rodoviárias emitiu um relatório regional declaração de emergência para 17 estados e Washington, manterem as linhas de abastecimento de combustível abertas em 9 de maio. Foi o maior ataque cibernético a um alvo de infraestrutura petrolífera na história dos Estados Unidos. O FBI e várias fontes da mídia identificaram o grupo criminoso de hackers DarkSide como parte responsável. Acredita-se que o mesmo grupo tenha roubado 100 gigabytes de dados dos servidores da empresa um dia antes do ataque de malware.

**Tipo de ataque:** Ransomware (DarkSide group).

**Vulnerabilidade explorada:** não foi um CVE específico, mas sim uso de credenciais comprometidas em VPN sem MFA (Multi-Factor Authentication).

**Impactos:** a empresa parou o fornecimento de combustível por quase uma semana, gerando escassez e filas em postos de gasolina na costa leste dos EUA. O prejuízo total estimado superou US$ 4,4 milhões pagos de resgate (parte depois recuperada pelo FBI).

**Proteção possível:** uso de MFA (Multi-Factor Authentication), gestão adequada de credenciais, segmentação de rede e monitoramento avançado contra movimentação lateral.



Ataque à cadeia de suprimentos da Kaseya

Em julho de 2021, o grupo de ransomware REvil realizou um dos maiores ataques de cadeia de suprimentos já registrados, explorando uma falha crítica no software Kaseya VSA. Esse programa era amplamente usado por empresas de TI para gerenciar remotamente redes e computadores de seus clientes. Os atacantes conseguiram explorar uma vulnerabilidade zero-day no sistema e, a partir dela, distribuíram uma atualização maliciosa que implantava ransomware diretamente nos computadores administrados pelos provedores de serviços.

Com isso, o ataque não atingiu apenas a Kaseya, mas também se espalhou para centenas de empresas no mundo todo, incluindo supermercados, escolas, órgãos públicos e outras organizações que dependiam de prestadores de serviços de TI. Estima-se que mais de 1.000 empresas clientes tenham sido impactadas. Os criminosos exigiram um resgate coletivo de cerca de US$ 70 milhões para liberar todas as máquinas afetadas, tornando o caso um dos maiores incidentes de ransomware em larga escala já registrados.

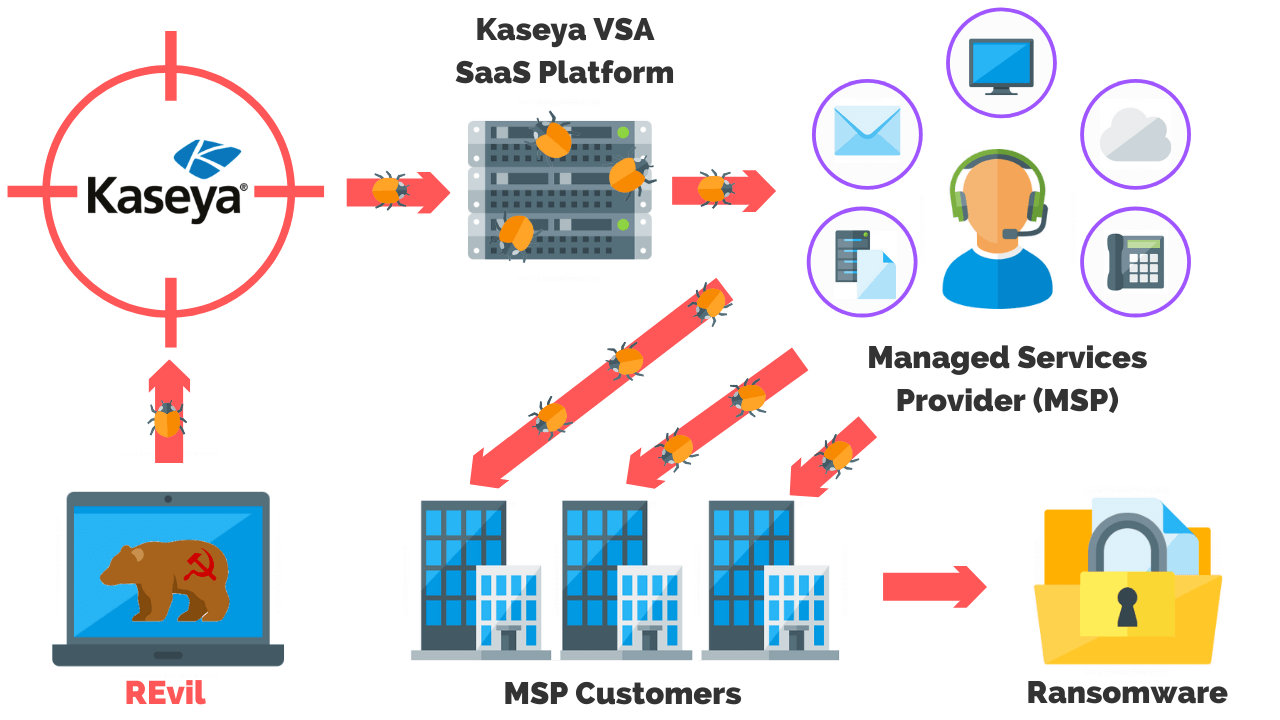
O impacto foi tão grande que a Kaseya precisou desligar seus servidores VSA para conter a propagação, enquanto especialistas em cibersegurança e agências governamentais trabalhavam para mitigar os danos. O ataque destacou a vulnerabilidade de depender de softwares de gerenciamento centralizado e chamou atenção para os riscos de ataques à cadeia de suprimentos, onde comprometer um único fornecedor pode abrir caminho para atingir milhares de organizações ao mesmo tempo.

**Tipo de ataque:** Supply Chain Attack com ransomware (REvil group).

**Vulnerabilidade explorada:** falha de zero-day na Kaseya VSA (CVE-2021-30116).

**Impactos:** bloqueio em massa de sistemas de clientes, pedidos de resgate totalizando até US$ 70 milhões; afetou redes de supermercados, escolas, órgãos governamentais e empresas de TI.

**Proteção possível:** aplicar Zero Trust, monitorar cadeias de suprimentos de software, limitar permissões de atualizações automáticas, além de usar patching rápido e segmentação de sistemas críticos.



***INTEGRANTES***

Rodolfo Regis de Souza – RA 825113514

Sergio Rycbzak Junior – RA 825154823

Pietro Oliveira Silva – RA 825113483

Gabriel Souza Santos – RA 825113168