- ¿Qué tipo de amenaza es?
- ¿Cómo comienza y cómo se propaga esta amenaza?
- ¿Hay más de una amenaza aplicada ?

Aprovechándose de vulnerabilidades de día cero, vulnerabilidades existentes desde el día de creación del software, los hackers ganaron acceso al servidor como un usuario estándar, y luego usaron otro exploit para escalar esa cuenta y darle privilegios de administrador. Lograron crear un "web shell" para tener un "backdoor", un acceso remoto con privilegios de administrador, desde el cual podían ejecutar scripts.
Usaron ese acceso remoto para robar datos de la red de organizaciones. Con estos datos, podían acceder a organizaciones de tamaño bajo-medio, como universidades o firmas de abogados. Estas organizaciones fueron suceptibles a ransomware.