

REvil's massive ransomware attack

Cybersecurity teams are working to stem the impact of the biggest global ransomware attack on record — a “supply chain” attack infecting thousands of users of Kaseya's VSA software

REvil (aka Sodinokibi) Russian hacker group

1) REvil hacks **Kaseya**, looking for financial records and insurance policies

Computer used by small business or employee of larger firm

2) Malicious **VSA** update file installed on every computer and server it can reach.

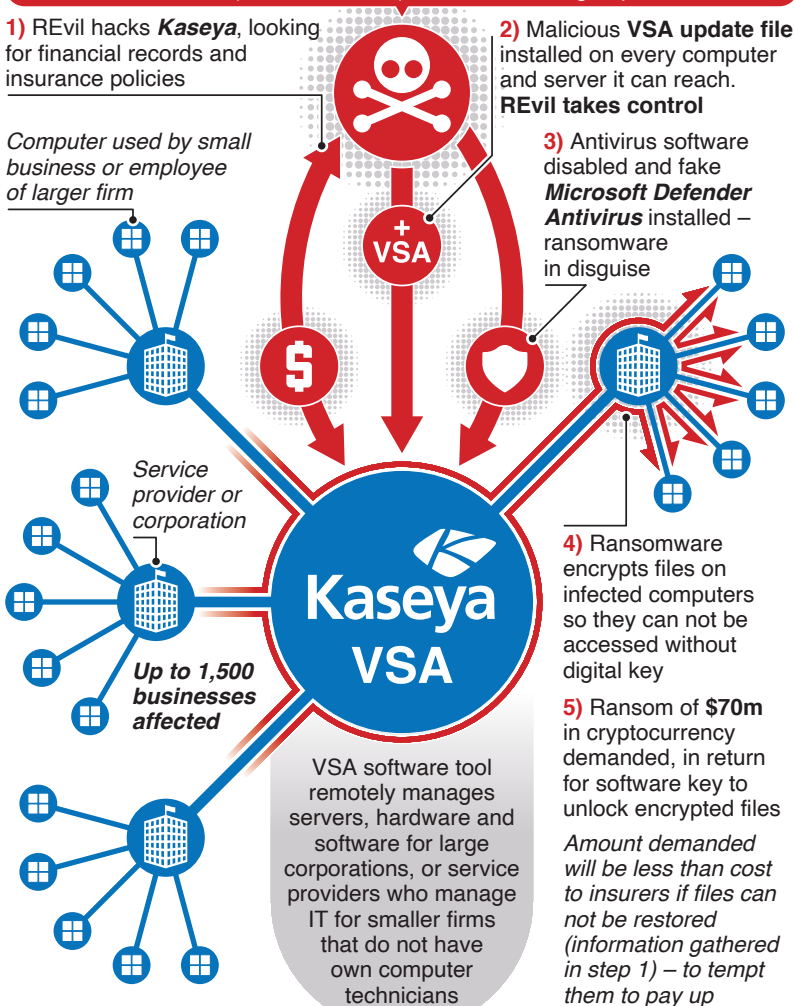
REvil takes control

3) Antivirus software disabled and fake **Microsoft Defender Antivirus** installed — ransomware in disguise

4) Ransomware encrypts files on infected computers so they can not be accessed without digital key

5) Ransom of **\$70m** in cryptocurrency demanded, in return for software key to unlock encrypted files

Amount demanded will be less than cost to insurers if files can not be restored (information gathered in step 1) — to tempt them to pay up



VSA software tool remotely manages servers, hardware and software for large corporations, or service providers who manage IT for smaller firms that do not have own computer technicians