Member-only story

Kaseya supply chain attack delivers mass ransomware event to US companies

Kevin Beaumont · Follow

Published in DoublePulsar · 8 min read · Jul 2, 2021

Kaseya VSA is a commonly used solution by MSPs — Managed Service Providers — in the United States and United Kingdom, which helps them manage their client systems. Kaseya's website claims they have over 40,000 customers.

Four hours ago, an apparent auto update in the product has delivered REvil ransomware.

By design, it has administrator rights down to client systems — which means that Managed Service Providers who are infected then infect their client's systems.

Infected systems look like this:

How this first unfolded

Initial entry was using a zero day vulnerability in Kaseya VSA. This was CVE-2021–30116 (details have not been entered into CVE database, however it has been allocated for this). More CVEs may be issued.

So even if the latest version is used, at time of attack, attackers could remotely execute commands on the VSA appliance. Technical details of how to exploit the vulnerability are not being provided until the patch is available.

It is not a great sign that a ransomware gang has a zero day in product used widely by Managed Service Providers, and shows the continued escalation of ransomware gangs — which I've written about before.

Written by Kevin Beaumont

17.4K Followers · Editor for DoublePulsar

Everything here is my personal work and opinions.