UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

# CYBER GUIDANCE ISSUE 00165

## KASEYA VSA USED TO DEPLOY RANSOMWARE ATTACKS

**DATE ISSUED:** 5th July 2021

| | | | |
|---|---|---|---|
| IMPACT | LOW | MEDIUM | **HIGH** |
| EASE OF EXPLOIT | HARD | MEDIUM | **EASY** |

## OVERVIEW

Kaseya VSA Management software is being used by an attack group, suspected to be REvil, to distribute ransomware after its compromise during the weekend.

## BREAKDOWN

Attackers have compromised Kaseya's VSA Management software used by numerous MSPs for infrastructure management and in a supply chain attack has been using it to distribute ransomware to various victims globally. Kaseya was aware of the issue and was actively working towards remediation when the attack took place. In their statement issued on July 4th, Kaseya states that they have managed to head off attackers, limiting victims to a "small number of on-premises customers only." SaaS datacenters should begin coming back online today after they were locked down to be secured.

Some schools (11) in New Zealand are reporting to have been effected by the attack including St Peter's College, Cambridge

## REMEDIATION STEPS

- Take all machines with on-premises instances of Kasey VSA offline until further notice and patches are released.
- Apply patches upon their release from Kaseya.
- If you have received any communications from attackers in relation to Kaseya attacks, do not access any hyperlinks as these are likely to be weaponised.
- Download and use the compromise detection toolkit provided by Kaseya – see Kaseya reference.
- Check Indicators of Compromise (IoC's) provided by Sophos – see Sophos reference.
- Update firewall whitelists with new IP addresses as released by Kaseya.

## REFERENCES & RESOURCES


| | |
|---|---|
| Kaseya | https://helpdesk.kaseya.com/hc/en-gb/articles/4403440684689-Important-Notice-July-2nd-2021 |
| CERT NZ | https://www.cert.govt.nz/it-specialists/advisories/kaseya-management-software-being-used-to-deploy-ransomware |
| Malware Bytes | https://blog.malwarebytes.com/cybercrime/2021/07/shutdown-kaseya-vsa-servers-now-amidst-cascading-revil-attack-against-msps-clients/amp/ |
| NZ Herald | https://www.nzherald.co.nz/nz/worldwide-ransomware-attack-st-peters-college-and-10-other-schools-hit-by-us-cyber-attack |
| Sophos | https://community.sophos.com/b/security-blog/posts/active-ransomware-attack-on-kaseya-customers |