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

CYBER GUIDANCE ISSUE 00168

FAKE KASEYA VSA UPDATES RELEASE COBALTSTRIKE

DATE ISSUED: 12th July 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

Off the back of the Kaseya VSA breach, attackers have seized the opportunity to deploy fake Microsoft updates which deploys the CobaltStrike malware on execution of SecurityUpdate.exe.

BREAKDOWN

CobaltStrike is being used by attackers to gain persistent remote access to systems when victims access the fake security updates circulating in a recent phishing campaign, preying on user fears created in the aftermath of the Kaseya VSA breach and ransomware attacks last week. CobaltStrike is traditionally a legitimate tool used by security penetration testers but has seen a recent surge in use during cyber-attacks. The beacon software locates vulnerabilities which threat actors can then use to breach systems in an effort to exfiltrate sensitive data and deploy further malware attacks – recently most commonly used as a first step in ransomware attacks. CobaltStrike was also used in the SolarWinds attacks earlier in the year.

REMEDIATION STEPS

- Educate users on social engineering techniques and how to identify phishing emails and what to do if they receive a suspicious email.
- Disable user's ability to run executable files.
- Use Next-Generation Anti-Virus (NGAV) endpoint protection on all devices to detect unusual or malicious activities

REFERENCES & RESOURCES

Threatpost	https://threatpost.com/fake-kaseya-vsa-update-cobalt-strike/167587/ https://threatpost.com/cobalt-strike-cybercrooks/167368/
Bleeping Computer	https://www.bleepingcomputer.com/news/security/fake-kaseya-vsa-security-update-backdoors-networks-with-cobalt-strike/
Heimdal Security	https://heimdalsecurity.com/blog/a-fake-kaseya-security-update-is-backdooring-networks-using-cobalt-strike/