

February 27, 2024

Agencies Update #StopRansomware Advisory on ALPHV Blackcat

The Federal Bureau of Investigation, Cybersecurity and Infrastructure Security Agency, and Department of Health and Human Services today issued an updated joint advisory [#StopRansomware: ALPHV Blackcat](#). The updated advisory provides new indicators of compromise and tactics, techniques and procedures associated with the ALPHV Blackcat ransomware as a service. ALPHV Blackcat is alleged to be involved in ongoing attacks impacting the health care field.

Please share the updated joint advisory with your IT and/or cybersecurity teams.

ACTIONS TO TAKE TODAY

Organizations should take action immediately to mitigate against the threat of ransomware.

- Network defenders should enter their indicators of compromise into their network defenses and threat hunting tools as soon as possible.
- Routinely take inventory of assets and data to identify authorized and unauthorized devices and software.
- Prioritize remediation of known exploited vulnerabilities.
- Enable and enforce multifactor authentication with strong passwords.
- Close unused ports and remove applications not deemed necessary for day-to-day operations.

FURTHER QUESTIONS

If you have further questions, please contact Riggi at riggi@aha.org. For the latest cyber threat intelligence and resources, visit www.aha.org/cybersecurity.