American Hospital Association™
Advancing Health in America

Cybersecurity Advisory

May 10, 2024

Federal Government Issues Joint Advisory as Black Basta Ransomware Group Accelerates Attacks on the Health Care Sector

Security partners are warning of significant risk; share this information and technical mitigation recommendations with IT and cyber infrastructure teams

The Federal Bureau of Investigation, Cybersecurity and Infrastructure Security Agency, Department of Health and Human Services, and Multi-State Information Sharing and Analysis Center today released a joint cybersecurity advisory to provide information on Black Basta, a ransomware variant whose actors have encrypted and stolen data from at least 12 out of 16 critical infrastructure sectors, including the health care and public health sector.

The joint advisory provides tactics, techniques, and procedures and indicators of compromise obtained from FBI investigations and third-party reporting. The federal agencies urge organizations to apply the recommendations in the mitigations section of the advisory to reduce the likelihood of compromise from Black Basta and other ransomware attacks.

Please share this information with your IT and cyber infrastructure teams. A PDF version of the joint federal advisory is available here.

Earlier today, the Health Information Sharing and Analysis Center (Health-ISAC) issued a bulletin warning to hospitals and other health care sector entities of a significant acceleration in cyberattacks by the Black Basta ransomware group.

“Recent actionable cyber threat intelligence provided by our partners at federal agencies and the Health-ISAC indicate that this known Russian-speaking ransomware gang is actively targeting the U.S. and global health care sector with high-impact ransomware attacks designed to disrupt operations,” said John Riggi, AHA’s national advisor for cybersecurity and risk. “It is recommended that this alert be reviewed with high urgency and the identified ransomware signatures be immediately loaded into network defenses and threat hunting tools. It also is recommended that the identified cyber risk mitigation practices be implemented as soon as feasible.”

WHAT YOU CAN DO

- **Share** this AHA Cybersecurity Advisory with your organization’s IT and cyber infrastructure teams.

- **Review** Kroll's Technical Analysis of Black Basta's tactics.
- **Implement** the voluntary consensus-based health care sector cybersecurity performance goals.
- **Review** the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients resources.
- **Update** regularly software and operating systems to patch vulnerabilities.
- **Implement** strong email security measures to prevent phishing attacks.
- **Limit** account access privileges across organizations.
- **Protect** against threats using a combination of antivirus, anti-malware and firewall solutions.
- **Back up** data frequently and ensure backups are isolated and immutable.
- **Conduct** cybersecurity awareness training for employees to recognize and report suspicious activities such as phishing attempts.
- **Monitor** networks for suspicious activity and have an incident response plan in place.
- **Establish** and implement a business continuity plan to ensure minimal operational disruptions in case of a ransomware incident.

Additional details on mitigation strategy can be found on the Cybersecurity and Infrastructure Security Agency's #StopRansomware page.

FURTHER QUESTIONS

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