Published on *The National Law Review* https://natlawreview.com

CISA Issues Advisory on Black Basta Ransomware

Article By:

Linn F. Freedman

On May 10, 2024, CISA, along with the FBI, HHS, and MS-ISAC, issued a joint Cybersecurity Advisory relating to Black Basta ransomware affiliates "that have targeted over 500 private industry and critical infrastructure entities, including healthcare organizations, in North America, Europe, and Australia."

The Black Basta Advisory provides information on how the threat actors gain initial access to victims' systems, which primarily use spearphishing tactics. In addition, "starting in February 2024, Black Basta affiliates began exploiting ConnectWise vulnerability (CVE-2024-1709). In some instances, affiliates have been observed abusing valid credentials."

The affiliates use different tools for lateral movement, including Remote Desktop Protocol, Splashtop, Screen Connect, and Cobalt Strike. In addition, they use credential scraping tools like Mimikatz to escalate privileges and have exploited prior zero-day vulnerabilities for local and Windows Active Domain privilege escalation.

The Advisory lists indicators of compromise, file indicators, and suspected domains used by Black Basta, which are helpful for IT professionals to compare against company systems. Mitigations listed by the Advisory include current patching, MFA, training, securing remote access software, backups, and other mitigation techniques. This Advisory is an important read for IT professionals in all industries.

National Law Review, Volume XIV, Number 137