# Report on Patient Privacy Volume 23, Number 2. February 09, 2023 Security Checklist: Safeguarding Common Tools

By Jane Anderson

HHS Health Sector Cybersecurity Coordination Center (HC3) is warning health care organizations that several widely used tools—including Cobalt Strike and PowerShell—can be turned against users' own infrastructure and is outlining a series of actions organizations can take to combat these tactics.[1]

These tools represent what HC3 said were "especially challenging security issues" because "mitigating the risk associated with them is not as simple as deploying a patch or reconfiguring an application," and "several of [the security tools] are resident on common systems, making them even more challenging to detect when used maliciously."

Other potentially abused tools cited by HC3 include:

- Sysinternals—an advanced system utilities tool
- AnyDesk—remote desktop software
- Brute Ratel—a customized command and control center for red team and adversary simulation