Powershell - the gift that keeps on giving

Brett Williams[1]
[1]*Carbon Black*

Over the last 3-4 years powershell's popularity has increased with both responders and attackers. Entire pen testing and attack simulation frameworks have been developed around or heavily using powershell. Powershells' capabilities combined with the efficiency of generated payloads from metasploit or cobalt strike, all of which can then be wrapped into Office macros, provide effective avenues of attack. This talk will highlight some of the more interesting attacks techniques, providing technical details, leveraging powershell that we've observed over the last year. Some of these techniques including targeting specific victim networks, anti-sandbox analysis attempts, as well as using DNS tunneling for C2 communication. The talk will also illustrate how attackers continue to use open source and commercial tools to assist in avoiding detection and analysis techniques.