FOR IMMEDIATE RELEASE

BY LIGHT RESEARCHER DISCOVERS TECHNIQUE TO BYPASS MICROSOFT APPLICATION TOOL

(ARLINGTON, VA, February 1, 2019) A By Light Professional IT Services LLC security researcher, Jimmy Bayne, has determined a procedure for bypassing Microsoft Application Control solutions using Component Object Model (COM). The technique executes unsigned code to bypass Windows Defender Application Control (WDAC)/Device Guard, including PowerShell Constrained Language Mode (CLM) with an Extensible Stylesheet Transformation (XSLT). Microsoft issued a patch for this bypass vulnerability in October 2018 (CVE-2018-8492).

“With WDAC, the Windows attack surface is greatly reduced,” said Jimmy. “After discovering accessible COM object methods, I used a PowerShell snippet to test for unsigned code execution. The payload executed under the context of CLM and an enforced code integrity policy.”

The full post containing example screenshots can be found here: https://bohops.com/2019/01/10/com-xsl-transformation-bypassing-microsoft-application-control-solutions-cve-2018-8492/.

About By Light
By Light Professional IT Services LLC is an ISO 9001, 20000-1, and 27001 registered and CMMI Level 3 certified systems integrator that provides secure, turn-key systems by incorporating exceptional engineering, project management, telecommunications and cyber capabilities to safeguard mission success. Founded by industry professionals with extensive knowledge in the DoD and other US Government Agencies, By Light successful implements technical solutions that integrate the best commercial practices to meet all government requirements. For more information, visit www.bylight.com.

Contact
Katie Accame
Marketing Specialist
marketing@bylight.com