Issued 7/6/17

Windows 10 Will Use Protected Folders to Thwart Crypto Ransomware

Windows 10 Fall Creators Update (the next major update of Microsoft's popular OS) is scheduled to be released in September, and will come with major new end-to-end security features. As announced last week, the Enhanced Mitigation Experience Toolkit (EMET) is making a partial comeback, along with new vulnerability mitigations, in a new feature called Windows Defender Exploit Guard. "Using intelligence from the Microsoft Intelligent Security Graph (ISG), Exploit Guard comes with a rich set of intrusion rules and policies to protect organizations from advanced threats, including zero day exploits. The inclusion of these built-in rules and policies addresses one of the key challenges with host intrusion prevention solutions which often takes significant expertise and development efforts to make effective," the company explained. Windows Defender Application Guard is designed to isolate threats like downloaded malware from the rest of the corporate network, and Windows Defender Device Guard, integrated with Windows Defender Advanced Threat Protection will allow the automated management of the safe application lists The latest Windows 10 build (16232) for PC has also brought improvements aimed at stopping ransomware from encrypting users' important files. Controlled folder access in Windows

Defender Antivirus can be switched on easily, and it will monitor the changes apps make to files in certain protected folders. “If an app attempts to make a change to these files, and the app is blacklisted by the feature, you’ll get a notification about the attempt,” Microsoft explains. “You can add additional folders to the list of protected folders, but you cannot alter the default list, which includes folders such as Documents, Pictures, Movies, and Desktop. Adding other folders to Controlled folder access can be handy, for example, if you don’t store files in the default Windows libraries or you’ve changed the location of the libraries away from the defaults.” Users will also be able to enter network shares and mapped drives to the protected folders list, but environment variables and wildcards will not be supported for the time being.