НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Использование файлов типа SettingContent-ms для исполнения произвольного кода в ОС Windows 10

Уровень угрозы: средний

№ 20180801-01 | 1 августа 2018 г.

TLP: WHITE

Цели	Круг потенциальных целей атаки не ограничен.
Время	С 11.06.2018 по н/в
Краткое описание угрозы	Файлы типа SettingContent-ms представляют собой документы в формате XML, содержащие тег DeepLink, который указывает на местоположение страниц настроек ОС Windows 10 на диске ПЭВМ. Используя специальным образом сформированное значение тега DeepLink, злоумышленник может организовать запуск произвольного исполняемого файла (файлов) на ПЭВМ, на которой пользователь попытается запустить файл типа SettingContent-ms. При этом на экране не появляются какие-либо уведомления о запуске стороннего файла. Файлы SettingContent-ms могут быть объединены с другими техниками атак, например, встроены в документы Office при помощи Object Linking and Embedding (OLE), а также дополнены методикой обхода правил ASR (Attack Surface Reduction) в Windows Defender, что позволяет построить цепочки запуска произвольного кода через программное обеспечение, указанное в белом списке OLE Blocks.
Возможные векторы атак	1. Рассылка писем, содержащих во вложении документ Microsoft Office со встроенным модифицированным файлом SettingContent-ms. При получении письма пользователю предлагается открыть присланный файл, в результате чего в фоновом режиме осуществляется запуск произвольного исполняемого файла (файлов) на ПЭВМ. 2. Размещение файла SettingContent-ms на веб-ресурсе и отправка потенциальным жертвам ссылки на него посредством электронной почты. При переходе по вредоносной ссылке браузер атакуемого объекта предложит открыть и исполнить данный файл.
Рекомендации по противодействию	1. Запретить исполнение встроенных объектов в продуктах Microsoft Office. Для этого необходимо выполнить следующие действия: - запустить командную строку (cmd) с правами администратора; - открыть редактор реестра командой regedit;

	- открыть реестр HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\<Office application>\Security\PackagerPrompt, где в атрибуте <Office application> необходимо выбрать один из установленных продуктов Microsoft Office (Word, Excel, PowerPoint, Visio и т.д.); - добавить ключ реестра типа DWORD (32 бита) со значением 2 (запрет исполнения встроенных объектов). 2. Рекомендуется разрешать запуск файлов типа SettingContent-ms только из директории: C:\Windows\ImmersiveControlPanel.
Ссылки на источники	1. https://posts.specterops.io/the-tale-of-settingcontent-ms-files-f1ea253e4d39 2. https://support.microsoft.com/en-us/kb/926530