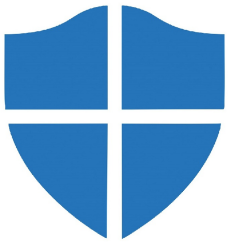
Microsoft Defender ATP считает вредоносным обновление для Chrome

Автор: Administrator
04.02.2021 20:35

{jcomments on}



Платная версия антивирусного продукта Защитник Microsoft, Microsoft Defender Advanced Threat Protection (ATP), принял последнее обновление Google Chrome за троянское ПО. После выхода Chrome v88.0.4324.146 в среду, 3 февраля, Defender ATP стал детектировать многие файлы пакета обновлений как бэкдор-троян Funvalget (PHP/Funvalget.A).

Оповещения Defender ATP об угрозе вызвали большое беспокойство у ИБ-сотрудников предприятий, учитывая недавние нашумевшие атаки на цепочки поставок, затронувшие организации по всему миру. Однако, по мнению многих системных администраторов, срабатывания антивируса были ложноположительными. И действительно, вскоре Microsoft подтвердила, что Defender ATP принял обновления для Chrome за бэкдор-троян из-за «ошибки автоматизации».

«Мы исправили ошибку автоматизации, из-за которой установочный пакет неверно классифицировался как вредоносное ПО», - сообщили в пресс-службе компании журналистам Bleeping Computer.

Для очистки кешированных обнаружений на используемых на предприятиях конечных точках системным администраторам рекомендуется:

- Открыть директорию Defender ATP с помощью командной строки, открытой под учетной записью администратора:

cd %ProgramFiles%Windows Defender

- Запустить эти две команды для очистки текущего кеша и запуска обновлений:

MpCmdRun.exe -removedefinitions -dynamicsignatures

MpCmdRun.exe -SignatureUpdate

Источник: www.securitylab.ru