Несмотря на то, что Microsoft навсегда отключила Internet Explorer, исследователь Check Point Хайфей Ли обнаружил, что его по-прежнему можно использовать во вредоносных целях. Атака использует файлы с расширением .url. При открытии эти файлы могут вызывать Internet Explorer, обходя меры безопасности современных браузеров, таких как Chrome и Edge. Эта уязвимость позволила хакерам получить «преимущества» при эксплуатации компьютеров жертв.

Хакеры используют эту технику в фишинговых письмах, маскируя .url-файлы под PDF. После открытия Internet Explorer загружает вредоносную программу в виде файла .hta, если пользователь нажимает на подсказки. Современные браузеры блокируют такие загрузки, но Internet Explorer лишь выдает предупреждение, которое можно легко проигнорировать.

Исследование Ли показывает, что этот метод используется с января 2023 года. Поскольку Microsoft прекратила выпуск крупных обновлений безопасности для Internet Explorer, браузер остается уязвимым для непропатченных эксплойтов.

Сейчас Microsoft выпустила исправление для устранения этого недостатка, но никто не может гарантировать, что хакеры найдут другие способы.