НКЦКИ
НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru
E-mail: threats@cert.gov.ru

Угроза внедрения ВПО при установке обновлений из недостоверных источников

ALRT-20220211 | 11 февраля 2022 г.

Уровень угрозы: КРИТИЧЕСКИЙ

TLP: WHITE

Потенциальные цели внедрения вредоносного программного обеспечения	Серверное и пользовательское программное обеспечение
Описание угрозы	По имеющимся в распоряжении НКЦКИ сведениям в последнее увеличилось количество случаев внедрения вредоносного программного обеспечения посредством подмены или внесения изменений в пакеты обновлений различного популярного программного обеспечения. В целях сокрытия своей деятельности и введения пользователей в заблуждение злоумышленники создают поддельные веб-ресурсы популярных разработчиков программного обеспечения, через которые впоследствии распространяют вредоносные пакеты обновлений. Данная ситуация создает предпосылки к массовой краже пользовательских данных или иной мошеннической деятельности злоумышленников. Ярким примером такой деятельности злоумышленников является использование вредоносных установщиков Windows 11, которые вместо обновления операционной системы производят внедрение вредоносного программного обеспечения RedLine, похищающего данные пользователей. Данная вредоносная программа пытается украсть пароли, данные банковских карт и криптовалютных кошельков. Веб-ресурс, с которого происходит распространение вредоносного пакета обновлений, выглядит как официальный сайт компании Microsoft и имеет доменное имя «windows-upgraded.com», на котором размещена кнопка «Скачать сейчас». Если пользователь нажмёт на эту ссылку, на компьютер загрузится ZIP-архив с именем «Windows11InstallationAssistant.zip». Как только пользователь запустит исполняемый файл из указанного архива, в его операционной системе вместо обновления произойдет внедрение вредоносной программы.
Рекомендации по нейтрализации угрозы	В целях недопущения данной угрозы рекомендуем использовать только лицензионное программное обеспечение и устанавливать обновления только с официальных сайтов производителей, а также проверять доменные имена сайтов на их корректность.