

По словам учёных, они изучили расширения Security-Noteworthy Extensions (SNE) в магазине Chrome. Под SNE понимается расширение, содержащее вредоносное ПО, нарушающее политику Chrome Web Store или содержащее уязвимый код.

В Google признают, что «безопасники» проверяют публикуемые расширения и детектируют уже опубликованные, чтобы выявить огрехи модерации. В связи с этим и было проведено исследование.

Во внимание принимались не только сами расширения, но и «народные» рейтинги, публикуемые пользователями также, как правило, через расширения. При этом оценки пользователей оказались бесполезны — вредоносные или потенциально нежелательные расширения не только публиковались в Chrome Store, но и находились в магазине долгое время, и их регулярно устанавливали.

По информации исследователей, в период с июля 2020 года по февраль 2023 года 346 млн пользователей установили SNES. В то время как 63 млн пользователей нарушали правила Chrome Store и 3 млн установили расширения с уязвимостями, 280 млн человек установили расширения, содержащее вредоносное ПО. В то время в интернет-магазине Chrome было доступно почти 125 000 расширений, и «плохих» среди них, очевидно, не 1%.

Исследователи обнаружили, что безопасные расширения Chrome обычно не задерживаются в магазине надолго: лишь 51,8-62,9% из них остаются доступными через год. SNE, напротив, оставались в магазине дольше: в среднем 380 дней — с вредоносным ПО, 1248 дней — с уязвимым кодом.

«В целом, пользователи не дают SNE более низких оценок, что говорит о том, что пользователи могут не знать, что какие-то расширения опасны. Конечно, не исключено, что боты дают фальшивые отзывы и высокие рейтинги этим расширениям. Однако, учитывая, что половина SNE не имеет отзывов, кажется, что использование фальшивых отзывов не является широко распространённым в данном случае», — отметили авторы исследования.