Как северокорейские хакеры маскируют вредоносный код под обычные уведомления.

Группа ScarCruft из Северной Кореи вновь использовала уязвимость в Windows – это операционная система для персональных компьютеров, разработанная и выпускаемая компанией Microsoft. ОС предоставляет пользователю удобный интерфейс и обширный функционал для работы с компьютером. Первая версия Windows вышла в 1985 году.

 С помощью Windows пользователи могут закрывать целый спектр различных потребностей, будь то работа, учёба, развлечения, разработка программного обеспечения и т.п.

 Windows поддерживает широкий спектр аппаратного обеспечения, что делает её самой популярной и широко используемой настольной ОС в мире, способной, впрочем, работать также и на мобильных устройствах.
" data-html="true" data-original-title="Windows" >Windows для распространения вредоносного программного обеспечения RokRAT. Эксплуатация затрагивает уязвимость CVE-2024-38178 с рейтингом CVSS 7.5, связанную с повреждением памяти в Scripting Engine, что позволяет выполнять удалённый код через Edge в режиме Internet Explorer.

Microsoft выпустила исправление для этой проблемы в рамках обновлений Patch Tuesday в августе 2024 года, однако хакеры не сбавляют темп и активно атакуют необновлённые системы.

Для активации атаки злоумышленникам необходимо убедить жертву перейти по специально подготовленной ссылке. Исследователи из AhnLab Security Emergency response Center (ASEC) – это центр круглосуточной поддержки и реагирования на инциденты безопасности. Он занимается мониторингом, анализом и устранением угроз безопасности, включая вирусы, хакерские атаки и фишинг." data-html="true" data-original-title="ASEC" >ASEC и Национального центра кибербезопасности Южной Кореи (Национальный центр кибербезопасности (National Cyber Security Centre, NCSC) – это государственное учреждение любой конкретно взятой страны, которое занимается защитой критически важных систем от кибератак.

 Центр предоставляют экспертные рекомендации и помощь в вопросах кибербезопасности для государственных органов, частных компаний и обычных граждан." data-html="true" data-original-title="NCSC" >NCSC) назвали кампанию «Операция Code on Toast». В международной среде группа ScarCruft также известна как TA-RedAnt, APT37, InkySquid, Reaper, Ricochet Chollima и Ruby Sleet.

Особенностью этой атаки стало использование рекламной программы «toast» — уведомлений, которые появляются в нижней части экрана. Атакующие взломали сервер неназванного рекламного агентства, предоставляющего контент для таких

уведомлений, и внедрили в скрипт рекламы вредоносный код.

Уязвимость активировалась при загрузке вредоносного содержимого через «toast», использующего устаревший модуль Internet Explorer. Это вызвало ошибку интерпретации типов в JavaScript Engine (jscript9.dll), что позволило атакующим проникнуть в системы с установленной уязвимой программой и получить удалённый доступ.

Обновлённая версия RokRAT способна управлять файлами, завершать процессы, выполнять команды с удалённого сервера и собирать данные из популярных приложений, таких как KakaoTalk и WeChat, а также из браузеров Chrome, Edge, Opera, Firefox и других. Для управления атаками RokRAT использует легитимные облачные сервисы, включая Dropbox, Google Cloud и Yandex Cloud, чтобы маскировать свою активность.

Группа ScarCruft уже не впервые эксплуатирует уязвимости в Internet Explorer. В прошлом ей приписывали атаки с использованием CVE-2020-1380 и CVE-2022-41128. Эксперты подчёркивают, что хакеры из Северной Кореи продолжают совершенствовать свои методы и применять различные уязвимости. Рекомендуется регулярно обновлять операционные системы и программы для защиты от подобных атак.

Узнайте как на нашем канале