Новый Zero-Click RCE-эксплойт выставлен на продажу за $5 млн.

16 июня злоумышленник под псевдонимом «Sp3ns3r» в своей публикации на киберпреступной площадке BreachForums – онлайн-сообщество, которое специализируется на обсуждении информационной безопасности и кибербезопасности. Участники могут обмениваться информацией о свежих уязвимостях, обнаруженных уязвимостях, техниках и способах защиты, а также обмениваться инструментами и скриптами. На форумах также можно найти информацию о продаже и покупке учетных данных, информационных баз и другой конфиденциальной информации. Некоторые форумы также предоставляют сервисы для проверки на уязвимости и тестирования защиты. Однако, некоторая информация может быть незаконной и неэтичной, и может использоваться для неправомерных действий." data-html="true" data-original-title="BreachForums" >BreachForums объявил о продаже высокоуровневого Уязвимости нулевого дня (Zero-day, 0-day) — это программные недостатки, о которых производитель либо вообще не знает, либо знает, но ещё не успел выпустить патч для их устранения.

 Эти уязвимости представляют особый интерес для хакеров, так как они открывают возможности для скрытного проведения атак с низкой вероятностью обнаружения.

 Обычно такие уязвимости выявляются исследователями безопасности или непосредственно злоумышленниками. В первом случае информация о бреше безопасности обычно сообщается производителю для последующего исправления, во втором — уязвимость может быть эксплуатирована непосредственно в хакерских атаках." data-html="true" data-original-title="Zero-day" >Zero-day Эксплойт (от англ. Exploit – означает «использовать что-то в своих интересах») – компьютерная программа, фрагмент программного кода или последовательность команд, которые используют ошибку или уязвимость для проведения атак на компьютерное ПО, аппаратное обеспечение или электронные устройства. Целью атаки является получение контроля над компьютерной системой, повышения привилегий или атака типа «отказ в обслуживании» (DoS или связанная с ней DDoS).

 Эксплойты обычно классифицируются и называются по: типу уязвимости, которую они используют; являются ли они локальными или удаленными; а также результатом запуска эксплойта (например, EoP, DoS, спуфинг). Одной из схем, предлагающих эксплойты нулевого дня, является Exploit-as-a-Service." data-html="true" data-original-title="Эксплойт" >эксплойта для удалённого выполнения кода (Remote Code Execution (RCE) – это критическая уязвимость, которая позволяет злоумышленнику дистанционно запустить вредоносный код в целевой системе по локальной сети или через Интернет. При этом физический доступ к устройству не требуется.

 В результате эксплуатации RCE-уязвимости киберпреступник может перехватить управление системой или ее отдельными компонентами, а также

похитить конфиденциальные данные." data-html="true" data-original-title="RCE" >RCE).

В объявлении злоумышленник подчёркивает лёгкость атаки, акцентируя внимание на Атаки с нулевым кликом позволяют получить доступ к устройству без каких-либо действий со стороны пользователя, то есть никаких нажатий клавиш или кликов мышью, что может заманить в ловушку даже самых технически подкованных людей.

 Скрытый характер атак с нулевым кликом затрудняет их обнаружение и предотвращение, независимо от того, какое устройство вы используете – iPhone, Android, Mac или ПК на Windows.

 Атаку не не следует путать с атаками нулевого дня, которые представляют собой уязвимости, активно эксплуатируемые и требующие немедленного исправления, но которые требуют действий пользователя для запуска." data-html="true" data-original-title="Zero-Click" >Zero-Click характере эксплойта. Это означает, что для выполнения кода не требуется никаких действий со стороны пользователя.

По утверждениям хакера, эксплойт поддерживает ОС Android – операционная система для мобильных устройств, разработанная компанией Google. Она основана на ядре Linux и предоставляет широкий спектр функций и сервисов для смартфонов, планшетов, умных часов, телевизоров и других устройств.

 Android позволяет пользователям скачивать и устанавливать приложения из магазина Google Play, обеспечивая множество возможностей для индивидуализации и работы с различными приложениями.

 Android является наиболее популярной в мире ОС для мобильных устройств и продолжает активно развиваться и обновляться." data-html="true" data-original-title="Android" >Android версий 11, 12, 13 и 14, показывая работоспособность и эффективность на любых Android-устройствах. Потенциальный масштаб катастрофы стремится к максимуму.

Основным методом распространения указаны MMS (Multimedia Messaging Service) сообщения. Причём сам факт получения подобного сообщения уже приведёт к заражению вашего устройства. RCE-характер эксплойта означает, что удалённый злоумышленник после компрометации сможет выполнять любые команды на заражённом девайсе.

Эксплойт выставлен на продажу за рекордные $5 миллионов. Кроме того, по запросу хакер также предоставляет доказательство концепции (PoC (Proof-of-Concept) (доказательство концепции) – реализация метода и его демонстрация на практике, чтобы доказать, что концепция или теория работает." data-html="true" data-original-title="PoC" >PoC), демонстрирующее возможности эксплойта.

Предыдущий недавний рекорд по стоимости выставленного на продажу эксплойта принадлежал RCE-уязвимости в Microsoft Outlook, эксплойт для которой был выставлен на том же Breachforums за 1,7 миллиона долларов. Теперь же этот рекорд официально побит.

Чтобы защитить свои Android-устройства от новой Zero-Click атаки, можно отключить в настройках сообщений автоматическое скачивание MMS. В Google Сообщениях это делается следующим образом: Нажатие на ваш аватар — Настройки приложения «Сообщения» — ваша SIM-карта — Автоматически скачивать MMS (перевести ползунок в положение «Выкл»).

Появление нового высокоуровневого Zero-Click эксплойта для Android демонстрирует, что киберпреступники постоянно ищут новые способы атак и монетизации уязвимостей. Пользователям необходимо быть бдительными, своевременно обновлять программное обеспечение и следовать рекомендациям по кибербезопасности, чтобы защитить свои устройства и данные.