Новый вредонос написан на Golang и имеет легальный сертификат от британского разработчика.

Группа киберпреступников Andariel, связанная с Северной Кореей, в последнее время активно использует новый вирус Dora RAT (созвучный с названием детского ТВ-шоу ), который написан на языке программирования Golang и применяется для атак на образовательные учреждения, производственные компании и строительные фирмы в Южной Корее. Об этом сообщается в отчёте Центра безопасности AhnLab (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), опубликованном на прошлой неделе.

В ходе атак злоумышленники применяют кейлоггеры, программы для кражи данных, различные прокси-инструменты и прочее вредоносное ПО, позволяющее управлять заражёнными системами и похищать с них информацию.

Для распространения вирусов Andariel использует уязвимый сервер Apache Tomcat, работающий на версии 2013 года. Устаревшее программное обеспечение делает системы уязвимыми для множества атак.

Группа Andariel, также известная как Nicket Hyatt, Onyx Sleet и Silent Chollima, действует в интересах Северной Кореи с 2008 года. Это подразделение крупной хакерской группы Lazarus, известной своими фишинговыми атаками и использованием уязвимостей в ПО для проникновения в сети множества частных и правительственных учреждений в разных странах.

Хотя ASEC не раскрывает подробности цепочки атак, упоминается использование модифицированного вируса Nestdoor, который может выполнять команды удалённого сервера, загружать и выгружать файлы, захватывать данные буфера обмена и клавиатуры, а также выполнять функции прокси-сервера.

Новый вирус Dora RAT, использованный в атаках, представляет собой простую вредоносную программу с функциями обратной оболочки и загрузки/выгрузки файлов. Злоумышленники подписали и распространили этот вирус с использованием действительного сертификата, полученного от британского разработчика программного обеспечения.

Другие вредоносные программы, задействованные в атаках, включают кейлоггер,

установленный через упрощённый вариант Nestdoor, а также инструмент для кражи информации и прокси-сервер SOCKS5, аналогичный инструменту, использованному группой Lazarus в кампании ThreatNeedle в 2021 году.

ASEC отмечает, что группа Andariel является одной из наиболее активных северокорейских групп, наряду с Kimsuky и Lazarus. Изначально их атаки были нацелены на получение информации, связанной с национальной безопасностью, но сейчас они также преследуют и финансовые цели.