Россиян предупредили о вредоносных файлах, которые активируются в ночное время

Специалисты «Лаборатории Касперского» заметили новую волну атак группы Librarian Ghouls, которая началась ещё в декабре 2024 года и продолжается до сих пор. В основном злоумышленники работают с часу ночи до пяти утра по местному времени. За это время они пытаются украсть логины и пароли, получить удалённый доступ к компьютерам и заразить их майнером, чтобы тайно добывать криптовалюту. Жертвами стали сотни сотрудников российских предприятий и вузов.

Атаки начинаются с рассылки фишинговых писем, где во вложениях находятся защищённые паролем архивы с вредоносными файлами. Обычно такие письма маскируются под официальные сообщения с документами. Пользователь вводит пароль из письма, распаковывает архив и запускает файлы, среди которых могут быть PDF с фейковым платёжным поручением, утилита curl и скрипт bat.lnk. Вредоносное ПО копируется в папку C:Intel, а для удалённого контроля злоумышленники ставят программу AnyDesk. В ряде случаев фишинговые сайты группы имитируют популярный российский почтовый сервис, чтобы украсть учётные данные.

По данным экспертов, в процессе атаки злоумышленники отключают Защитник Windows и делают так, чтобы программа AnyDesk подключалась без подтверждений, используя заранее заданный пароль. Для скрытия следов заражённый компьютер каждый день выключается ровно в пять утра, а запуск вредоносных скриптов происходит в час ночи. За эти четыре часа злоумышленники успевают собрать данные, включая пароли и ключи криптокошельков, затем загружают майнер и удаляют свои следы. Представитель «Лаборатории Касперского» отметил, что группа не пишет собственное ПО, а пользуется легальными утилитами, постоянно совершенствуя методы атак и используя новые приёмы социальной инженерии.