Ученые из Технологического института Джорджии разработали инструмент ECHO, который автоматически удаляет ботнеты — сети устройств, зараженных вредоносным ПО. Система использует собственные механизмы обновления malware против него самого, блокируя повторное заражение. Эффективность достигает 75%, а процесс, раньше занимавший недели, теперь решается за минуты.

ECHO действует в три этапа. Сначала анализирует, как вирус распространяет код. Затем перехватывает эти каналы, чтобы доставить «противоядие». Наконец, внедряет очищающий скрипт, который отключает вредоносные функции. Тесты на 702 образцах Android-вирусов показали успех в 523 случаях.

Инструмент стал прорывом после ручных методов вроде борьбы с Retadup в 2019 году. Тогда Avast и власти Франции потратили месяцы на обратную разработку, создав разовое решение. ECHO автоматизирует процесс, делая его доступным для массового использования. Код системы открыт на GitHub.

Ботнеты, существующие с 1980-х, сегодня опаснее чем когда-либо. Они крадут данные, парализуют инфраструктуру и обходятся компаниям в миллионы долларов. ECHO позволяет обезвреживать угрозы до масштабных последствий.

Следующая цель команды — адаптировать инструмент для iOS и Windows. Пока ECHO сосредоточен на Android, но принципы универсальны.