Представлена online-энциклопедия методов выявления виртуальной среды

Специалисты компании Check Point запустили online-энциклопедию Malware Evasion Encyclopedia, в которой собраны способы, используемые вредоносным ПО для выявления виртуальной среды.

Для обхода обнаружения и дальнейшего анализа исследователями безопасности вредоносные программы определяют, не запущены ли они на виртуальной машине, например, в VirtualBox или VMWare. Обнаружив виртуальную среду, вредонос просто не запускается, а в некоторых случаях даже самоудаляется.

В Malware Evasion Encyclopedia собраны используемые вредоносным ПО методы обнаружения виртуальной среды. Хотя Malware Evasion Encyclopedia позволит авторам вредоносных программ узнать новые техники, по мнению специалистов Check Point, ценность для сообщества информационной безопасности значительно превышает любые преимущества для разработчиков вредоносного ПО.

Источник: https://www.securitylab.ru/news/505486.php